УДК 341.1:004.8:342.7
DOI: 10.60022/3(5)-64S

Чістякова Ірина Миколаївна
кандидат філософських наук, доцент
завідувачка кафедрою міжнародних відносин та права
Національний університет «Одеська політехніка», Україна
Chistiakova Iryna
PhD in Philosophy, Associate Professor
Head of the Department of International Relations and Law,
National University «Odesa Polytechnic», Ukraine
ORCID: 0000-0002-0182-9334

Кудлай Ірина Володимирівна
старший викладач кафедри міжнародних відносин та права
Національний університет «Одеська політехніка», Україна
Kudlai Iryna
Art. off Department of International Relations and Law
National University "Odesa Polytechnic", Ukraine
ORCID: 0000-0002-6154-5245

ПРАВО НА ПРИВАТНІСТЬ ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ ФОРМУВАННЯ ГЛОБАЛЬНОГО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

Анотація. *У статті досліджується право на приватність як фундаментальний елемент формування глобальної системи регулювання штучного інтелекту. Встановлено, що стрімкий розвиток технологій штучного інтелекту зумовлює трансформацію традиційних підходів до захисту приватного життя, зокрема у зв'язку з поширенням алгоритмічного профілювання, обробки великих масивів персональних даних та використання біометричних технологій.*

Проаналізовано міжнародно-правові стандарти захисту приватності, зокрема положення Загальної декларації прав людини, Європейської конвенції з прав людини та сучасні регуляторні акти, включаючи GDPR і EU AI Act. Доведено, що право на приватність поступово трансформується у центральний принцип формування підходів до регулювання штучного інтелекту на глобальному рівні. Окрему увагу приділено ролі міжнародних організацій, зокрема ООН та Ради Європи, у виробленні універсальних стандартів у сфері цифрових прав. Обґрунтовано наявність фрагментації міжнародного регулювання та конкуренції моделей (європейської, американської, китайської), що ускладнює формування єдиного глобального режиму.

Зроблено висновок, що розвиток штучного інтелекту суттєво трансформує зміст права на приватність у сучасних міжнародних відносинах. Воно виступає не лише об'єктом захисту, а й системоутворюючим принципом регулювання штучного інтелекту, який визначає межі допустимого використання технологій. Ефективний захист права на приватність у цифрову епоху значною мірою залежатиме від здатності міжнародних організацій та держав забезпечити прозорість контролю за обробкою даних і дотримання принципів міжнародного права прав людини. Міжнародне співтовариство постає перед необхідністю формування універсальних міжнародно-правових стандартів регулювання штучного інтелекту, які забезпечували б баланс між технологічним розвитком, національною безпекою та дотриманням фундаментальних прав людини.

Запропоновано напрями гармонізації міжнародних підходів та посилення праволюдинно-орієнтованого регулювання ШІ.

Ключові слова: *право на приватність, штучний інтелект, міжнародне право, GDPR, AI Act, права людини, персональні дані.*

THE RIGHT TO PRIVACY AS A KEY ELEMENT IN FORMING GLOBAL REGULATION OF ARTIFICIAL INTELLIGENCE

Abstract. *This article examines the right to privacy as a fundamental element in shaping the global*

regulatory framework for artificial intelligence (AI). The rapid development of AI technologies has led to significant transformations in traditional approaches to privacy protection, particularly in the context of algorithmic profiling, big data processing, and biometric surveillance.

The study analyzes key international legal instruments, including the Universal Declaration of Human Rights, the European Convention on Human Rights, as well as modern regulatory frameworks such as the General Data Protection Regulation and the Artificial Intelligence Act. It is argued that the right to privacy is evolving into a central principle guiding AI Act at the global level.

Special attention is paid to the role of international organizations, including the United Nations and the Council of Europe, in establishing universal standards in the field of digital rights. The article highlights the fragmentation of global regulation and the competition between different regulatory models. It is concluded that the development of artificial intelligence significantly transforms the content of the right to privacy in modern international relations. It acts not only as an object of protection, but also as a system-forming principle of regulating artificial intelligence, which determines the boundaries of permissible use of technologies. Effective protection of the right to privacy in the digital age will largely depend on the ability of international organizations and states to ensure transparency of control over data processing and compliance with the principles of international human rights law. The international community is faced with the need to form universal international legal standards for regulating artificial intelligence, which would ensure a balance between technological development, national security and observance of fundamental human rights. Directions for harmonizing international approaches and strengthening human rights-oriented regulation of AI are proposed.

Keywords: *right to privacy, artificial intelligence, international law, GDPR, AI Act, human rights, personal data.*

Постановка проблеми. Штучний інтелект (ШІ) стрімко трансформує систему міжнародних відносин, поступово перетворюючись на один із ключових інструментів реалізації державної влади та впливу, що переосмислює традиційні уявлення про геополітичне домінування. Його використання охоплює широкий спектр сфер - від посилення військового та економічного потенціалу держав до формування інформаційних і культурних наративів, а також застосування у гібридних інформаційних операціях і дезінформаційних кампаніях.

У сучасних умовах провідні глобальні актори, зокрема Сполучені Штати Америки та Китайська Народна Республіка, активно інтегрують технології штучного інтелекту у свої стратегії національної безпеки та зовнішньої політики, розглядаючи їх як інструмент зміцнення геополітичної конкурентоспроможності та технологічного суверенітету. Водночас Європейський Союз та держави Глобального Півдня адаптують використання ШІ відповідно до власних стратегічних пріоритетів, зокрема у сферах цифрового врядування, економічного розвитку та підвищення ефективності публічного управління.

Особливого значення набуває подвійна природа штучного інтелекту, який одночасно виступає як інструмент демократизації доступу до інформації та технологічних ресурсів, так і як фактор загострення етичних дилем, посилення інформаційної асиметрії та виникнення нових ризиків дестабілізації міжнародної безпеки. Мають місце проблеми алгоритмічного маніпулювання, поширення дезінформації, а також використання ШІ в операціях когнітивного впливу. Також, сучасний розвиток штучного інтелекту створює якісно нові виклики для реалізації права на приватність. Масове використання алгоритмів, здатних до автономного аналізу поведінки особи, формує ризики прихованого втручання у приватне життя, що не завжди охоплюється традиційними правовими механізмами.

Проблема полягає у тому, що існуючі норми не встигають за технологіями, що зумовлює необхідність переосмислення ролі приватності у системі глобального регулювання ШІ, відсутній єдиний глобальний стандарт, приватність стає вразливою через data-driven models of AI.

Метою статті є дослідження права на приватність як системоутворюючого принципу формування глобального регулювання штучного інтелекту та визначення основних напрямів його розвитку.

Аналіз останніх досліджень і публікацій. Проблематика взаємодії ШІ та права на приватність активно досліджується у сучасній науці. Значна увага приділяється співвідношенню норм захисту персональних даних та нових регуляторних актів у сфері ШІ. Зокрема, дослідники підкреслюють, що регулювання ШІ та захист персональних даних мають взаємодоповнюючий характер: якщо перше спрямоване на контроль технологій, то друге - на захист прав особи. Водночас у наукових працях наголошується на тому, що ШІ створює новий рівень складності обробки даних, який не був передбачений традиційними правовими моделями .

Теоретико-правова природа права на приватність формувалася протягом тривалого історичного

періоду як відповідь на зміну соціальних, технологічних і політичних умов існування людини, що зумовило поступову еволюцію цього права від індивідуально-особистісного феномена до складної багатовимірної правової категорії. У класичному розумінні право на приватність виникло наприкінці XIX століття як реакція на розвиток засобів масової комунікації та втручання у приватне життя через пресу, що було концептуалізовано у відомій статті Samuel Warren та Louis Brandeis «The Right to Privacy» (1890), де приватність визначалась як «право бути залишеним у спокої» [33]. У цьому контексті приватність розглядалася передусім як негативне право, спрямоване на обмеження втручання з боку держави або третіх осіб у сферу особистого життя.

Подальший розвиток концепції приватності відбувався у межах європейської правової традиції, де вона отримала закріплення у міжнародно-правових актах, зокрема у Загальній декларації прав людини (ст. 12) [12] та Європейській конвенції з прав людини (ст. 8) [7], що значно розширило її зміст, включивши не лише захист від фізичного втручання, а й інформаційний аспект приватності. Як зазначає Alan Westin, приватність у сучасному розумінні слід тлумачити як здатність особи самостійно визначати межі доступу до інформації про себе [34]. Таким чином, концепція приватності еволюціонувала від пасивного захисту до активного контролю над персональними даними.

У другій половині XX століття розвиток інформаційних технологій сприяв формуванню так званого інформаційного підходу до приватності, який акцентує увагу на обробці персональних даних. У цьому контексті значний внесок зробив Daniel Solove, який запропонував класифікацію порушень приватності, включаючи збір, обробку, поширення інформації та втручання у приватне життя [29; 30]. Водночас Helen Nissenbaum розробила концепцію «контекстуальної цілісності», відповідно до якої приватність порушується не лише через сам факт збору інформації, а й через невідповідність контексту її використання [25].

З розвитком цифрових технологій і, особливо, штучного інтелекту, класичні підходи до приватності зазнали суттєвої трансформації. У цифрову епоху приватність перестає бути лише просторовою або фізичною категорією та набуває характеру динамічного процесу, пов'язаного з постійним обігом даних. Як зазначає Shoshana Zuboff, сучасна економіка ґрунтується на так званому «капіталізмі спостереження», де персональні дані стають основним ресурсом [35]. Це призводить до ситуації, коли втручання у приватність відбувається не явно, а через алгоритмічні процеси, які є непрозорими для суб'єкта даних.

У цьому контексті виникає протиставлення класичних і цифрових підходів до приватності. Класичний підхід базується на ідеї територіальності та недоторканності приватного простору, де ключовим є обмеження фізичного або прямого інформаційного втручання. Натомість цифровий підхід орієнтується на управління потоками даних, прозорість алгоритмів і забезпечення контролю суб'єкта над інформацією про себе. Як підкреслює Paul De Hert, сучасне право на приватність трансформується у право на захист даних, яке включає такі елементи: згода, мінімізація даних та відповідальність операторів [20].

Особливого значення набуває інтеграція принципів «privacy by design» та «privacy by default», закріплених у GDPR, що відображає перехід від реактивної до превентивної моделі захисту приватності. У цьому випадку приватність розглядається не як зовнішнє обмеження, а як внутрішня характеристика технологічних систем. Водночас прийняття EU AI Act [11] демонструє подальший розвиток цієї концепції, оскільки приватність інтегрується у ширший контекст оцінки ризиків, пов'язаних із використанням штучного інтелекту.

У науковій літературі також відзначається зміщення акценту з індивідуальної приватності до колективних вимірів цього права. Зокрема, дослідники наголошують, що алгоритмічні системи можуть впливати не лише на окремих осіб, але й на соціальні групи, формуючи нові ризики дискримінації та соціального контролю [30]. Це зумовлює необхідність переосмислення приватності як елемента ширшої системи цифрових прав людини.

У вітчизняній правовій науці право на приватність традиційно розглядається як складова системи особистих немайнових прав людини, що забезпечує автономію особи та недоторканність її приватного життя. Так, у працях українських дослідників підкреслюється, що приватність є не лише індивідуальним благом, а й важливим елементом демократичного суспільства, який гарантує свободу особистості від надмірного контролю [2]. Водночас науковці наголошують на тому, що в умовах інформаційного суспільства право на приватність набуває нових змістовних характеристик, пов'язаних із цифровими технологіями та обробкою даних [5]. Окремий напрям присвячений співвідношенню права на приватність та захисту персональних даних. Зокрема, зазначається, що право на захист персональних даних є сучасною формою реалізації права на приватність, адаптованою до умов цифрового середовища [4]. У цьому контексті підкреслюється, що традиційні правові механізми вже не забезпечують належного рівня захисту у зв'язку з використанням великих масивів даних та

автоматизованих систем обробки інформації.

Важливий внесок у розвиток концепції інформаційної приватності зроблено українськими науковцями, які досліджують проблеми інформаційного права. Так, акцентується увага на тому, що сучасне право на приватність тісно пов'язане з інформаційною безпекою та кібербезпекою, оскільки витоки даних, несанкціонований доступ та кіберзагрози безпосередньо впливають на реалізацію цього права [6]. У цьому аспекті приватність розглядається як елемент ширшої системи інформаційних прав людини.

Сучасні українські дослідження також приділяють увагу впливу штучного інтелекту на право на приватність. Зокрема, підкреслюється, що використання алгоритмічних систем створює нові ризики порушення приватності, які пов'язані з непрозорістю алгоритмів та складністю контролю за обробкою даних [1]. Дослідники наголошують, що штучний інтелект змінює саму природу втручання у приватне життя, оскільки таке втручання часто є непрямим і відбувається без усвідомлення особи. Також, українські науковці звертають увагу на необхідність гармонізації національного законодавства з європейськими стандартами, зокрема із GDPR, що розглядається як базовий орієнтир у сфері захисту персональних даних [3] й підкреслюють, що імплементація європейських підходів сприятиме формуванню ефективної системи захисту приватності в Україні.

Загалом огляд української наукової думки дозволяє зробити висновок, що вітчизняні дослідники підтримують тенденцію трансформації права на приватність від класичного розуміння до цифрового, акцентуючи увагу на необхідності забезпечення контролю над персональними даними, прозорості алгоритмічних процесів та підвищення рівня правового регулювання у сфері штучного інтелекту. При цьому українська доктрина поступово інтегрується у глобальний науковий дискурс, поєднуючи традиційні підходи з сучасними концепціями інформаційного суспільства та цифрових прав людини.

Таким чином, теоретико-правова природа права на приватність характеризується складною еволюцією від класичного розуміння як права на недоторканність приватного життя до сучасного багатовимірного концепту, що охоплює контроль над персональними даними, алгоритмічну прозорість і захист від непрямих форм втручання. Сучасні наукові підходи демонструють, що приватність вже не може розглядатися ізольовано, а повинна аналізуватися у контексті цифрових технологій, глобалізації та розвитку штучного інтелекту, що обумовлює її ключову роль у формуванні нової моделі правового регулювання.

Виклад основного матеріалу дослідження. Вплив штучного інтелекту на право на приватність у сучасних умовах набуває системного та багатовимірного характеру, що обумовлено передусім специфікою функціонування самих алгоритмічних систем. Штучний інтелект, на відміну від традиційних інформаційних технологій, базується на обробці великих масивів даних, включаючи персональні, що створює структурну напругу між технологічною ефективністю та правовими гарантіями приватності. Як зазначається у сучасних дослідженнях, ефективність систем ШІ прямо залежить від обсягу та якості даних, які використовуються для навчання моделей, що ускладнює дотримання принципів мінімізації та цільового використання даних [22; 10].

Одним із ключових аспектів впливу ШІ на приватність є феномен так званого «надмірного використання даних», коли інформація, зібрана для однієї мети, використовується для інших, часто без відома суб'єкта даних. Це прямо суперечить базовим принципам захисту персональних даних і створює ризики несанкціонованого втручання у приватне життя [27; 32]. У зв'язку з цим, особливої актуальності набуває проблема алгоритмічного профілювання, коли на основі великих масивів даних формуються поведінкові або соціальні характеристики особи, що можуть використовуватися для прийняття рішень у сфері працевлаштування, кредитування або соціального забезпечення [32]. Такі процеси часто є непрозорими і не піддаються ефективному контролю з боку особи, що посилює ризики порушення її прав.

Іншою важливою проблемою є так званий ефект «чорної скриньки», притаманний багатьом системам ШІ, коли логіка прийняття рішень є незрозумілою навіть для розробників. Відсутність прозорості у функціонуванні алгоритмів унеможливлює перевірку їх законності, справедливості та пропорційності, що прямо впливає на реалізацію права на приватність та інших прав людини [35]. У цьому контексті right to explanation, яке закріплене у законодавстві Європейського Союзу, набуває особливого значення як інструмент забезпечення підзвітності алгоритмічних систем. Крім того, використання ШІ значно розширює можливості спостереження та контролю за поведінкою людини. Технології розпізнавання облич, аналізу емоцій, поведінкового моніторингу та прогнозування створюють передумови для формування систем масового спостереження, які можуть використовуватися як державними органами, так і приватними компаніями. Такі практики становлять серйозну загрозу для приватності, оскільки втручання відбувається постійно і часто непомітно для особи [26]. ШІ трансформує саме розуміння втручання у приватність - воно стає не епізодичним, а системним і безперервним. Водночас важливим

аспектом є ризик дискримінації, який виникає унаслідок використання упереджених даних для навчання алгоритмів. Ці системи можуть відтворювати або навіть посилювати існуючі соціальні нерівності, що має безпосередній вплив на права людини, включаючи приватність, оскільки рішення приймаються на основі аналізу персональних характеристик [15], що зумовлює необхідність інтеграції принципів недискримінації та справедливості у процес розробки та використання ШІ.

З огляду на зазначені виклики, міжнародне співтовариство поступово формує систему правових стандартів, спрямованих на забезпечення захисту приватності в умовах розвитку штучного інтелекту. Базовими актами у цій сфері залишаються Загальна декларація прав людини та Європейська конвенція з прав людини, які закріплюють загальні гарантії недоторканності приватного життя. Однак ці акти були прийняті в доцифрову епоху, що обумовлює необхідність їх сучасного тлумачення та розвитку.

Суттєвий прорив у сфері міжнародно-правового регулювання приватності пов'язаний із прийняттям GDPR, який встановлює комплексну систему захисту персональних даних. GDPR закріплює ключові принципи обробки даних, зокрема законність, прозорість, обмеження мети та мінімізацію даних, а також надає суб'єктам даних широкі права, включаючи право доступу, виправлення та видалення інформації. Особливе значення має стаття 22 GDPR, яка передбачає право особи не підлягати виключно автоматизованому прийняттю рішень, що має суттєвий вплив на її права [10].

Подальший розвиток міжнародних стандартів пов'язаний із прийняттям EU AI Act [11], який став першим комплексним актом, спрямованим безпосередньо на регулювання штучного інтелекту. Цей акт запроваджує ризик-орієнтований підхід, відповідно до якого системи ШІ класифікуються залежно від рівня потенційної шкоди, яку вони можуть завдати. Зокрема, забороняються системи, що становлять неприйнятний ризик, включаючи деякі види масового спостереження, тоді як для високоризикових систем встановлюються жорсткі вимоги щодо прозорості, підзвітності та людського контролю [11].

Важливо підкреслити, що GDPR і AI Act функціонують у взаємодії, формуючи комплексну систему регулювання, в якій приватність виступає центральним елементом. Якщо GDPR забезпечує захист персональних даних, то AI Act [11] доповнює його, встановлюючи вимоги до безпеки та етичності самих алгоритмічних систем [8; 31]. Така модель свідчить про перехід від ізольованого регулювання даних до інтегрованого підходу, що охоплює весь життєвий цикл ШІ. На глобальному рівні також спостерігається тенденція до розширення правового регулювання у сфері приватності та ШІ, зокрема через розвиток національних законодавств та міжнародних ініціатив. Водночас відсутність єдиного універсального підходу призводить до фрагментації регулювання, що ускладнює забезпечення ефективного захисту прав людини у глобальному цифровому середовищі [18; 24]

Таким чином, вплив штучного інтелекту на приватність характеризується зростанням масштабів та складності втручання у приватне життя, що зумовлює необхідність трансформації міжнародно-правових стандартів. Сучасні регуляторні підходи демонструють тенденцію до інтеграції принципів захисту приватності у саму архітектуру технологій, що свідчить про становлення нової парадигми правового регулювання, в якій приватність виступає не лише об'єктом захисту, а й фундаментальним принципом розвитку ШІ.

Сучасні підходи до регулювання формують три різні нормативно-ціннісні моделі регулювання ШІ, які відображають не лише юридичні особливості, а й різні філософії співвідношення держави, технологій і прав людини.

Європейська модель є праволюдинно-орієнтованою та базується на поєднанні GDPR та AI Act, що забезпечує інтеграцію приватності у регуляторну систему [11]. Європейський Союз формує модель, у якій ключовим є пріоритет фундаментальних прав, насамперед права на приватність та захист персональних даних. Європейська модель є найбільш комплексною та нормативно деталізованою. Вона базується на ризик-орієнтованому підході, відповідно до якого рівень правового регулювання залежить від ступеня потенційної небезпеки систем штучного інтелекту для прав людини та де технологія оцінюється ще до її впровадження. Центральним елементом цієї моделі виступають GDPR та EU AI Act [11], які запроваджують багаторівневу класифікацію систем ШІ (від мінімального до неприйнятного ризику), формують єдину систему цифрового врядування та встановлюють жорсткі вимоги до високоризикових систем, включаючи прозорість, людський контроль і оцінку впливу на основні права. У науковій літературі зазначається, що європейський підхід є «праволюдинно-орієнтованим», оскільки інтегрує принципи захисту приватності та персональних даних у саму архітектуру регулювання ШІ [31; 8].

Американська модель, на відміну від європейської, характеризується фрагментарністю та інноваційною орієнтацією. Сполучені Штати Америки застосовують переважно ринково-орієнтовану та фрагментарну модель регулювання, де відсутній єдиний комплексний федеральний акт щодо ШІ. Регулювання здійснюється через окремі галузеві норми, судову практику та рекомендації регуляторних органів, без наявності єдиного федерального закону. У наукових дослідженнях підкреслюється, що

така модель відображає пріоритет ринку та технологічного розвитку над централізованим правовим контролем [17; 23]. Водночас окремі штати, зокрема Каліфорнія, запроваджують власні підходи до регулювання ШІ, що створює додаткову правову фрагментацію [31; 8]. Це забезпечує гнучкість інновацій, однак створює ризики слабшого захисту приватності та нормативної непослідовності на загальнонаціональному рівні. Отже, Американська модель є фрагментарною і базується на секторному регулюванні та рекомендаціях регуляторних органів, без єдиного федерального закону про ШІ (U.S. National AI Initiative Act, 2020) [13].

Китайська модель характеризується державоцентричним підходом, де ШІ розглядається як інструмент соціального управління та державного контролю [19]. Китайська Народна Республіка реалізує державоцентричну модель, у якій штучний інтелект розглядається як інструмент державного управління та соціального контролю над розробкою та використанням алгоритмів, а також інтеграцію технологічної політики у систему державного управління. Науковці відзначають, що китайський підхід розглядає штучний інтелект як елемент національної інфраструктури та інструмент соціального управління [14; 8: 28]. Регулювання має адміністративний характер і базується на принципах цифрового суверенітету, пріоритету національної безпеки та централізованого контролю над даними. Це відрізняє його як від європейської правлюдинної, так і від американської ринкової моделей. Так, Китайська модель є найбільш централізованою та державоорієнтованою.

Отже, сучасні моделі регулювання штучного інтелекту формуються як відповідь на необхідність балансування між інноваційним розвитком технологій та захистом фундаментальних прав людини, зокрема права на приватність. Підкреслені у сучасній доктрині три базові регуляторні моделі відображають різні філософські підходи до ролі держави у сфері цифрового врядування. Особливу роль у процесах глобального регулювання відіграє європейська модель, яка завдяки екстериторіальній дії GDPR та AI Act [11] фактично формує так званий «ефект Брюсселя», коли європейські нормативні стандарти стають орієнтиром для глобальних міжнародних компаній та інших юрисдикцій [16].

Таким чином, глобальний простір регулювання ШІ характеризується системною правовою асиметрією, яка ускладнює формування єдиного міжнародного стандарту.

Для більш наочного відображення відмінностей між провідними підходами до правового регулювання штучного інтелекту доцільно здійснити порівняльний аналіз ключових моделей, що сформувалися у Європейському Союзі, США та КНР (табл. 1). Узагальнення їх основних характеристик дозволяє простежити специфіку співвідношення між інноваційним розвитком, державним контролем та захистом прав людини у сучасному цифровому середовищі.

Таблиця 1

Порівняльна характеристика основних моделей регулювання штучного інтелекту у глобальному ШІ крізь призму права на приватність

Критерій прівнання	Європейська модель (ЄС)	Американська модель (США)	Китайська модель (КНР)
Загальна характеристика моделі	Праволюдинно-орієнтована та ризик-орієнтована модель	Ринково-інноваційна та децентралізована модель	Державоцентрична та адміністративно-контрольна модель
Основна мета регулювання	Захист фундаментальних прав людини та безпечне використання ШІ	Стимулювання інновацій та технологічного розвитку	Забезпечення державного контролю, національної безпеки та соціальної стабільності
Ключові нормативні акти	GDPR; EU AI Act	Sectoral AI regulation; Executive Orders; State AI laws	Interim Measures for Generative AI; New Generation AI Development Plan
Тип регулювання	Комплексне та превентивне	Секторальне та фрагментарне	Централізоване адміністративне
Рівень централізації	Високий (наднаціональний рівень ЄС)	Низький (федеральний + штатний рівень)	Дуже високий (централізований державний контроль)
Підхід до приватності	Приватність як фундаментальне право	Приватність як елемент ринкового регулювання	Приватність підпорядковується державним інтересам
Принцип регулювання ШІ	Risk-based approach	Innovation-first approach	Security-first approach
Регулювання високоризикових систем	Жорсткі вимоги щодо прозорості, аудиту та людського контролю	Часткове та галузеве регулювання	Контроль через державний нагляд
Алгоритмічна прозорість	Високий рівень вимог	Обмежене регулювання	Часткова прозорість під контролем держави

Продовження таблиці 1

Автоматизоване прийняття рішень	Право на оскарження та людський перегляд	Обмежені гарантії	Переважно державний контроль
Використання біометричних технологій	Суттєво обмежене	Частково регульоване	Широко використовується
Роль держави	Регулятор і гарант прав людини	Координатор інноваційного розвитку	Центральний суб'єкт цифрового контролю
Роль приватного сектору	Висока, але під регуляторним наглядом	Домінуюча	Підконтрольна державі
Міжнародний вплив моделі	Формування глобальних стандартів («ефект Брюсселя»)	Технологічне та корпоративне домінування	Розширення цифрового впливу через інфраструктурні проєкти
Основні переваги	Високий рівень захисту прав людини та приватності	Гнучкість та швидкий розвиток інновацій	Висока швидкість централізованого впровадження технологій
Основні недоліки	Надмірна зарегульованість та ризик уповільнення інновацій	Фрагментація та нерівномірний захист прав	Ризики масового спостереження та обмеження прав людини

Джерело: складено автором за даними [8; 11; 13-18]

Порівняльний аналіз зазначених моделей свідчить про існування нормативної конкуренції моделей ШІ, що ускладнює формування єдиного глобального правового режиму у сфері регулювання штучного інтелекту. Як підкреслюється у сучасних дослідженнях, різні правові системи фактично формують «несумісні регуляторні архітектури», навіть якщо використовують подібну термінологію таку як «ризик», «безпека», «прозорість» [31; 21]. Це ускладнює формування універсальних стандартів та підвищує значення міжнародної координації.

Глобальне регулювання ШІ перебуває на етапі становлення і характеризується одночасно процесами конвергенції та фрагментації. З одного боку, спостерігається поступове зближення базових принципів регулювання, таких як безпека, прозорість, підзвітність і захист прав людини. З іншого боку, механізми їх реалізації суттєво відрізняються залежно від правової системи держави, що формує проблему відсутності єдиного глобального стандарту. Так, однією з ключових проблем є нормативна фрагментація. Різноманітність підходів призводить до того, що одна й та сама технологія може одночасно підпадати під різні, інколи суперечливі вимоги залежно від юрисдикції.

Другою проблемою є так званий «регуляторний розрив» між швидкістю розвитку технологій і повільністю правового реагування. Штучний інтелект розвивається експоненційно, тоді як міжнародно-правові механізми залишаються інерційними. Це створює ситуацію, коли правове регулювання постійно запізнюється щодо технологічних інновацій, що особливо критично у сфері захисту приватності та персональних даних.

Третьою проблемою є відсутність єдиного міжнародного органу або універсального договору, який би встановлював обов'язкові стандарти для всіх держав. Хоча існують різні ініціативи, зокрема в рамках міжнародних організацій, вони здебільшого мають рекомендаційний характер і не створюють юридично обов'язкових норм. У науковій літературі це визначається як «інституційна фрагментація глобального AI governance» [18; 14].

Водночас перспективи розвитку глобального регулювання пов'язані з поступовою гармонізацією принципів та формуванням мінімального консенсусу щодо базових етичних і правових стандартів. Перспективним напрямом також є розвиток концепції ризик-орієнтованого регулювання, яка поступово стає загальновизнаною у різних правових системах. Як показують порівняльні дослідження, навіть за умов різних політичних моделей, більшість країн визнають необхідність класифікації систем ШІ за рівнем ризику та запровадження пропорційного контролю [31; 21].

У довгостроковій перспективі можливе формування гібридної моделі глобального регулювання, яка поєднуватиме елементи національного суверенітету з мінімальними міжнародними стандартами. Така модель дозволила б зберегти інноваційний потенціал технологій, одночасно забезпечуючи базовий рівень захисту прав людини, включаючи право на приватність.

Сучасна концепція ШІ формується як система правових, етичних та інституційних механізмів управління розвитком і використанням штучного інтелекту, у центрі якої дедалі частіше знаходиться право на приватність як базовий принцип регулювання цифрових технологій. У сучасній доктрині підкреслюється, що саме обробка персональних даних є ключовим елементом функціонування систем штучного інтелекту, що зумовлює необхідність інтеграції приватності у всі етапи життєвого циклу

алгоритмів [35].

Трансформація ролі приватності в цифрову епоху пов'язана з переходом від класичного розуміння цього права як «права на недоторканність приватного життя» до сучасної концепції інформаційної автономії особи. У класичній теорії, сформованій ще у працях S. Warren та L. Brandeis, приватність визначалася як право «бути залишеним у спокої» [33]. Однак у сучасних умовах цей підхід є недостатнім, оскільки цифрові технології створюють постійні, а не епізодичні форми збору та аналізу інформації. Значний внесок у розвиток сучасної теорії приватності зробив A. Westin, який визначив її як контроль особи над інформацією про себе [34]. Ця концепція стала основою для подальшого розвитку інформаційного підходу до приватності, який сьогодні лежить в основі регулювання персональних даних у Європейському Союзі.

Штучний інтелект суттєво змінює характер реалізації права на приватність, оскільки він базується на обробці великих масивів даних, включаючи персональні, біометричні та поведінкові дані. Згідно з D. Solove, сучасні загрози приватності є системними і включають не лише збір інформації, але й її агрегування, аналіз та вторинне використання [29]. Особливу проблему становить алгоритмічне профілювання, яке дозволяє формувати детальні соціальні та поведінкові портрети осіб. Це створює ризики непрозорого прийняття рішень у сферах працевлаштування, кредитування та державного управління. H. Nissenbaum вводить концепцію «контекстуальної цілісності», відповідно до якої порушення приватності відбувається тоді, коли інформація використовується поза межами її первинного контексту [25]. Базовими міжнародно-правовими актами у сфері приватності є Загальна декларація прав людини (ст. 12) [12] та Європейська конвенція з прав людини (ст. 8) [7], які закріплюють загальний принцип недоторканності приватного життя(UDHR, 194)

Сучасний етап розвитку правового регулювання представлений Загальним регламентом про захист даних (GDPR), який встановлює комплексний підхід до обробки персональних даних виконує системоутворюючу функцію, оскільки більшість ризиків штучного інтелекту пов'язані саме з обробкою персональних даних. Зокрема, ст. 25 GDPR закріплює принцип «privacy by design», який фактично трансформує приватність у елемент архітектури цифрових систем, а не лише у правову гарантію. Ст. 22 - надає право особи не підлягати виключно автоматизованому прийняттю рішень (Regulation (EU) 2016/679, ст. 22, 25) [10].

Подальшим розвитком є AI, який запроваджує ризик-орієнтовану модель регулювання штучного інтелекту та інтегрує захист фундаментальних прав у класифікацію систем ШІ (Regulation (EU) 2024/1689, ст. 5–14) [11].

Як зазначається у звітах Європейської комісії, приватність є ключовим критерієм оцінки допустимості використання систем ШІ [9].

Висновки. Узагальнюючи, можна констатувати, що глобальна система ШІ перебуває у стані нормативної конкуренції моделей, де відсутній єдиний універсальний стандарт, а приватність виконує різні функції залежно від правової системи - від фундаментального права (ЄС) до інструменту регуляції (США) та елемента державного управління (Китай).

Порівняльний аналіз демонструє наявність трьох принципово різних моделей регулювання штучного інтелекту, які формують глобальну правову асиметрію та кожна з яких відображає різні підходи до співвідношення технологічного розвитку, державного контролю та захисту прав людини.

Європейський Союз формує найбільш розвинену модель інтеграції права на приватність у систему ШІ, де приватність виступає не лише як захищене право, а як регуляторний критерій допустимості технологій. Це створює модель «правового превентивного контролю». США забезпечують максимальну інноваційну свободу, однак за рахунок фрагментації регулювання, що призводить до нерівномірного захисту приватності та залежності від секторних правил. Китайська модель забезпечує високий рівень державного контролю, однак обмежує індивідуальну автономію у сфері приватності, підпорядковуючи її інтересам державної політики.

Таким чином, визначимо, що:

по-перше, приватність під впливом штучного інтелекту зазнає фундаментальної трансформації: від класичного права на недоторканність приватного життя вона переходить до концепції цифрової та алгоритмічної приватності, що охоплює контроль над даними та процесами їх обробки;

по-друге, приватність поступово стає центральним елементом ШІ, оскільки саме через неї визначаються межі допустимого використання технологій штучного інтелекту та оцінюються їхні ризики для прав людини;

по-третє, глобальне регулювання штучного інтелекту є фрагментованим через різні моделі правового регулювання (європейську, американську та китайську), що ускладнює формування єдиного міжнародного стандарту;

по-четверте, існує об'єктивна необхідність гармонізації міжнародного регулювання шляхом

формування універсальних принципів ШІ, у центрі яких має бути право на приватність як базове фундаментальне право людини.

Література

1. Баранов О. А. Штучний інтелект і захист персональних даних: правові виклики. *Право і суспільство*. 2021. № 4. С. 98–104.
2. Гриценко І. С. Право на приватність у системі прав людини. *Право України*. 2012. № 3. С. 45–52.
3. Костецька Т. А. Адаптація законодавства України до стандартів GDPR. *Європейське право*. 2020. № 2. С. 67–73.
4. Кохановська О. В. Захист персональних даних як елемент права на приватність. *Юридична наука*. 2017. № 2. С. 112–118.
5. Рабінович П. М. Основи загальної теорії права та держави. Львів: Край, 2015. 320 с.
6. Ткачук Т. Ю. Інформаційна безпека та право на приватність у цифрову епоху. *Інформаційне право*. 2019. № 1. С. 25–31.
7. Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights). Rome, 1950. URL: https://www.echr.coe.int (дата звернення: 06.04.2026).
8. European Commission. Proposal for a Regulation laying down harmonised rules on artificial intelligence. Brussels, 2021. URL: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence (дата звернення: 05.04.2026).
9. European Commission. AI Ethics Guidelines for Trustworthy AI. Brussels, 2019. P. 1–36.
10. 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 (General Data Protection Regulation (GDPR)). *Official Journal of the European Union*. 2016. L 119. P. 1–88.
11. Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act (AI Act)). *Official Journal of the European Union*. 2024. P. 3-10.
12. Universal Declaration of Human Rights: adopted and proclaimed by the United Nations General Assembly on 10 December 1948. Art. 12. URL: https://www.un.org/ en/about-us/universal-declaration-of-human-rights (дата звернення: 06.04.2026).
13. U.S. National AI Initiative Act, 2020. URL: https://www.congress.gov/ bill/116th-congress/house-bill/6216 (дата звернення: 05.04.2026).
14. Abbott K., Snidal D. The Governance Triangle: Regulatory Standards Institutions. Harvard International Law Journal. 2020. P. 45–52.
15. Barocas S., Selbst A. Big Data's Disparate Impact. California Law Review. 2016. Vol. 104. P. 671–732.
16. Bradford A. The Brussels Effect: How the European Union Rules the World. Oxford University Press, 2020. P. 15-22.
17. Calo R. Artificial Intelligence Policy: A Primer and Roadmap. U.C. Davis Law Review. 2017. Vol. 51. P. 399–435.
18. Cath C. Governing Artificial Intelligence: Ethical, Legal and Technical Opportunities. Phil. Trans. R. Soc. A. 2018. P. 5-9.
19. Creemers R. China's Approach to AI Governance. Journal of Cyber Policy. 2021. P. 112–118.
20. De Hert P., Papakonstantinou V. The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals? *Computer Law & Security Review*. 2016. Vol. 32. № 2. P. 179–194.
21. Floridi L. et al. AI4People-An Ethical Framework for a Good AI Society. Minds and Machines. 2018. Vol. 28. P. 689–707.
22. Goodfellow I., Bengio Y., Courville A. Deep Learning. Cambridge: MIT Press, 2016. 775 p.
23. Marchant G., Wallach W. Coordinating Technology Governance. Issues in Science and Technology. 2015. Vol. 31. P. 37–46, 380-385.
24. Nemitz P., Pfeffer M. Principles and Limits of AI Ethics. Oxford University Press, 2020. P. 145–150.
25. Nissenbaum H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press, 2010. 288 p.
26. O'Neil C. Weapons of Math Destruction. New York: Crown, 2016. 259 p.
27. Pasquale F. The Black Box Society. Harvard University Press, 2015. 320 p.
28. Roberts H., Cowls J., Morley J. et al. The Chinese Approach to AI Governance. AI & Society. 2021. P. 1–18.

29. Solove D. J. A Taxonomy of Privacy. *University of Pennsylvania Law Review*. 2006. Vol. 154. №. 3. P. 477–564.
30. Solove D. J. The Myth of the Privacy Paradox. *George Washington Law Review*. 2021. Vol. 89. P. 1–51.
31. Veale M., Borgesius F. Z. Demystifying the Draft EU Artificial Intelligence Act. Computer Law Review International. 2021. P. 97–112.
32. Wachter S., Mittelstadt B., Floridi L. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR. International Data Privacy Law. 2017. Vol. 7. P. 76–99.
33. Warren S., Brandeis L. The Right to Privacy. *Harvard Law Review*. 1890. Vol. 4. №. 5. P. 193–220.
34. Westin A. F. *Privacy and Freedom*. New York: Atheneum, 1967. 487 p.
35. Zuboff S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs, 2019. 704 p.

References

1. Baranov, O. A. (2021) Artificial intelligence and personal data protection: legal challenges. *Law and society.* № 4. P. 98–104.
2. Hrytsenko, I. S. (2012) The right to privacy in the human rights system. *Law of Ukraine.* № 3. P. 45–52.
3. Kostecka, T. A. (2020) Adaptation of Ukrainian legislation to GDPR standards. *European law.* № 2. P. 67–73.
4. Kokhanovs'ka, O. V. (2017) Protection of personal data as an element of the right to privacy. *Legal Science*. № 2. P. 112–118.
5. Rabinovych, P. M. (2015) Fundamentals of the General Theory of Law and State. Lviv: Kray. 320 p.
6. Tkachuk, T. Yu. (2019) Information security and the right to privacy in the digital age. *Information Law.* № 1. P. 25–31.
7. Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights). (1950). Rome. URL: https://www.echr.coe.int (access date: 06.04.2026).
8. European Commission. Proposal for a Regulation laying down harmonised rules on artificial intelligence. (2021), Brussels. URL: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence (access date: 05.04.2026).
9. European Commission. (2019) AI Ethics Guidelines for Trustworthy AI. Brussels. P. 1–36.
10. 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 (General Data Protection Regulation (GDPR)). *Official Journal of the European Union*. 2016. L 119. P. 1–88.
11. Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act (AI Act)). *Official Journal of the European Union*. 2024. P. 3-10.
12. Universal Declaration of Human Rights: adopted and proclaimed by the United Nations General Assembly on 10 December 1948. Art. 12. URL: https://www.un.org/ en/about-us/universal-declaration-of-human-rights (access date: 06.04.2026).
13. U.S. National AI Initiative Act, 2020. URL: https://www.congress.gov/ bill/116th-congress/house-bill/6216 (access date: 05.04.2026).
14. Abbott, K., Snidal, D. (2020) The Governance Triangle: Regulatory Standards Institutions. Harvard International Law Journal. P. 45–52.
15. Barocas, S., Selbst, A. (2016) Big Data's Disparate Impact. California Law Review. Vol. 104. P. 671–732.
16. Bradford, A. (2020) The Brussels Effect: How the European Union Rules the World. Oxford University Press. P. 15-22.
17. Calo, R. (2017) Artificial Intelligence Policy: A Primer and Roadmap. U.C. Davis Law Review. Vol. 51. P. 399–435.
18. Cath, C. (2018) Governing Artificial Intelligence: Ethical, Legal and Technical Opportunities. Phil. Trans. R. Soc. A. P. 5-9.
19. Creemers, R. (2021) China's Approach to AI Governance. Journal of Cyber Policy. P. 112–118.
20. De Hert, P., Papakonstantinou, V. (2016) The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals? *Computer Law & Security Review*. Vol. 32. P. 179–194.
21. Floridi, L. et al. (2018) AI4People-An Ethical Framework for a Good AI Society. Minds and Machines. Vol. 28. P. 689–707.

22. Goodfellow, I., Bengio, Y., Courville, A. (2016) Deep Learning. Cambridge: MIT Press. 775 p.
23. Marchant, G., Wallach, W. (2015) Coordinating Technology Governance. Issues in Science and Technology. Vol. 31. P. 37–46, 380-385.
24. Nemitz, P., Pfeffer, M. (2020) Principles and Limits of AI Ethics. Oxford University Press. P. 145–150.
25. Nissenbaum, H. (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press. 288 p.
26. O'Neil, C. (2016) Weapons of Math Destruction. New York: Crown. 259 p.
27. Pasquale, F. (2015) The Black Box Society. Harvard University Press. 320 p.
28. Roberts, H., Cowls, J., Morley, J. et al. (2021) The Chinese Approach to AI Governance. AI & Society. P. 1–18.
29. Solove, D. J. (2006) A Taxonomy of Privacy. *University of Pennsylvania Law Review*. Vol. 154. № 3. P. 477–564.
30. Solove, D. J. (2021) The Myth of the Privacy Paradox. *George Washington Law Review*. Vol. 89. P. 1–51.
31. Veale, M., Borgesius, F. Z. (2021) Demystifying the Draft EU Artificial Intelligence Act. Computer Law Review International. P. 97–112.
32. Wachter S., Mittelstadt B., Floridi L. (2017) Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR. International Data Privacy Law. Vol. 7. P. 76–99.
33. Warren, S., Brandeis, L. (1890) The Right to Privacy. *Harvard Law Review*. Vol. 4. № 5. P. 193–220.
34. Westin, A. F. (1967) *Privacy and Freedom*. New York: Atheneum. 487 p.
35. Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs. 704 p.

Отримано: 11.04.2026
Прийнято до публікації: 11.05.2026
Опубліковано: 15.05.2026