Наукові записки НаУКМА
Юридичні науки 16 (2025)

NaUKMA Research Papers
Law 16 (2025)

СТАТТЯ

ARTICLE

DOI: 10.18523/2617-2607.2025.16.80-87
УДК 342.738:004.056.8

Олександр Кожухар
Аспірант кафедри загальнотеоретичного правознавства та публічного права
факультету правничих наук,
Національний університет «Києво-Могилянська академія», Київ, Україна
https://orcid.org/0009-0006-4183-3289
o.kozhukhar@ukma.edu.ua

ПРАВОВЕ РЕГУЛЮВАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ: ЛІНІЇ ВЗАЄМОЗВ'ЯЗКІВ

У статті досліджено зв'язок між потенційним правовим регулюванням систем штучного інтелекту (ШІ) та режимом захисту персональних даних. Аналіз проведено крізь призму тенденцій у сфері регулювання систем ШІ, зокрема Акта (ЄС) про ШІ та Рамкової конвенції Ради Європи про ШІ, що на сьогодні визначають вектор розвитку політики на міжнародному та національному рівнях. У статті обґрунтовано, що архітектура сучасних систем ШІ на всіх етапах їхнього життєвого циклу — від розроблення до практичного впровадження — пов'язана з обробкою значних масивів персональних даних. Така характеристика систем ШІ зумовлює системні ризики для прав і свобод суб'єктів даних, створюючи певний конфлікт між інноваційним потенціалом ШІ та усталеними гарантіями у сфері захисту персональних даних. Ці ризики є особливо істотними в юрисдикціях із неналежним рівнем захисту персональних даних, що характерно й для України. Тож актуальним є аналіз взаємозв'язків між системами ШІ та захистом персональних даних.

Дослідження демонструє, як основні принципи захисту персональних даних: законність, мінімізація, обмеження мети, прозорість та точність — стикаються з викликами в застосуванні ШІ. Наприклад, принцип мінімізації даних вступає в колізію з потребою алгоритмів машинного навчання у значних наборах даних для цілей розробки систем, а проблема «чорної скриньки» систем ШІ може не узгоджуватися з вимогою прозорості обробки даних. Автор доводить необхідність розроблення підходу, за яким вимоги у сфері захисту персональних даних (оновлені відповідно до чинних стандартів ЄС у цій сфері, включно із Загальним регламентом про захист даних) повинні бути складовою частиною механізму правового регулювання ШІ в Україні. Головними механізмами, що дають змогу реалізувати такий підхід, є прозорість та людський нагляд, що уможливлюють реалізацію інших гарантій як у сфері захисту персональних даних, так і в регулюванні ШІ. Для України це також означає нагальну потребу в імплементації відповідних норм і створення відповідного наглядового органу з належним рівнем інституційної спроможності. Ці висновки є важливими для подальшої роботи над законопроєктом № 8153 та для формування національної стратегії регулювання ШІ.

Ключові слова: права людини, правове регулювання, юридичні гарантії, штучний інтелект, ШІ, приватність, захист персональних даних, Загальний регламент про захист даних, Конвенція про ШІ.

Постановка проблеми

Сучасні підходи до регулювання систем штучного інтелекту (ШІ) ґрунтуються на тому, що існує стійкий зв'язок між функціонуванням технологій ШІ та режимом захисту персональних даних. Наприклад, Європейський Союз запропонував модель співіснування Загального регламенту про захист

даних (далі — Регламент) та Акта про ШІ, за якою спеціальне регулювання ШІ (базоване на ризиковості відповідних систем) не замінює, а доповнює та конкретизує загальні юридичні гарантії, встановлені для будь-якої обробки персональних даних[1].

Цей зв'язок зумовлений самою архітектурою сучасних систем ШІ, життєвий цикл яких (від навчання моделей на масивах даних до їхнього практичного впровадження) передбачає обробку персональних даних. Це породжує певні системні ризики між певними властивостями систем ШІ та усталеними юридичними гарантіями у сфері захисту персональних даних, включно з принципами обробки даних. Зокрема, алгоритмічна непрозорість систем ШІ часто вступає в колізію з принципом прозорості обробки персональних даних, а масштабна та часто непередбачувана зміна цілей обробки даних у системах ШІ не узгоджується з принципом обмеження мети обробки даних. Іншими принципами обробки даних, які можуть певною мірою підважуватися динамічними системами ШІ, є законність обробки даних (наприклад, через складність отримання згоди суб'єкта даних або забезпечення іншої підстави для обробки даних) та точність такої обробки (через схильність моделей ШІ до створення хибної інформації).

Станом на сьогодні законодавство України щодо захисту персональних даних є певною мірою застарілим та не узгоджується зі стандартами в цій сфері, які існують у ЄС, включно з Регламентом. Одним із наслідків цього є те, що Україна не входить до переліку європейських держав, які забезпечують належний (адекватний) рівень захисту персональних даних, що ускладнює процес транскордонної передачі даних з ЄС до України. У зв'язку з цим для правової системи України, що перебуває в процесі гармонізації з правом ЄС (зокрема в межах роботи над законопроєктом № 8153)[2], наведені вище питання взаємозв'язків мають важливе значення. Належне (у розумінні ЄС) регулювання сфери захисту персональних даних не обмежується лише впровадженням Регламенту. Потрібно забезпечити узгоджене співіснування режиму захисту персональних даних та регулювання систем ШІ з наданням реальних юридичних гарантій для суб'єктів даних. Першим кроком для такого узгодженого співіснування є розуміння основних взаємозв'язків між регулюванням ШІ та регулюванням у сфері захисту персональних даних, що найкраще можна простежити крізь призму принципів захисту персональних даних[3].

Аналіз досліджень

На формування сучасного дискурсу щодо правового регулювання ШІ та суміжних питань захисту персональних даних значний вплив мали Акт про ШІ та Рамкова конвенція Ради Європи про ШІ та права людини (далі — Конвенція). Дослідження переважно концентруються на аналізі викликів для розробників і постачальників систем ШІ, а також на проблематиці співвідношення нового, спеціального законодавства про ШІ із загальним режимом захисту персональних даних, втіленим у Регламенті. Зокрема, у посібниках Оксфордського та Кембриджського університетів питання приватності та захисту даних входять до переліку основних етико-правових викликів, породжених технологічними можливостями ШІ[4].

Паралельно з академічним дискурсом із 2024 року спостерігається перехід до етапу, коли державні органи також формують власне бачення співіснування обох режимів та практичного застосування відповідних норм. Роз'яснення французького регулятора у сфері захисту даних (CNIL) щодо використання «легітимного інтересу» як правової підстави для обробки даних під час навчання моделей ШІ, а також документ Європейської ради із захисту даних (EDPB) щодо аспектів обробки даних у ШІ є прикладами такої діяльності, спрямованої на зменшення правової невизначеності[5].

В українському контексті також з'являються перші напрацювання щодо цих питань, зокрема урядові матеріали (рекомендації Міністерства цифрової трансформації)[6] та наукові публікації з аналізом загальних ризиків для суб'єктів даних (праці М. та Д. Бєлових та інших)[7]. Проте науковому дискурсу

---

1 Див. ст. 2(7) Акта про ШІ.

2 Проєкт Закону про захист персональних даних № 8153 від 25 жовтня 2022 року, який має імплементувати Загальний регламент про захист даних в Україні, https://itd.rada.gov.ua/billinfo/Bills/Card/40707.

3 Для завдань цієї статті ми будемо використовувати термінологію щодо питань захисту персональних даних, передбачену Регламентом і законопроєктом № 8153.

4 Markus Dirk Dubber, Frank Pasquale, and Sunit Das, *The Oxford Handbook of Ethics of AI* (Oxford University Press, 2021); Nathalie A. Smuha, *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (Cambridge University Press, 2025).

5 CNIL, *Relying on the Legal Basis of Legitimate Interests to Develop an AI System*, 2024, https://www.cnil.fr/en/relying-legal-basis-legitimate-interests-develop-ai-system; European Data Protection Board, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, December 2024, https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf.

6 Міністерство цифрової трансформації, *Рекомендації з відповідальної розробки систем із використанням технологій штучного інтелекту* (червень 2025), https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs/ШІ%20для%20розробників.pdf.

7 Бєлова М. В., Бєлов Д. М., «Виклики та загрози захисту персональних даних у роботі зі штучним інтелектом», *Науковий вісник Ужгородського національного університету. Серія: Право* 79, ч. 2 (2023): 17–22, https://doi.org/10.24144/2307-3322.2023.79.2.2.

бракує системного аналізу взаємозв'язків між фундаментальними принципами захисту персональних даних та основними властивостями функціонування систем ШІ. Саме дослідження цього рівня потенційних конфліктів є важливою передумовою для розроблення обґрунтованого підходу до регулювання ШІ, що забезпечує належне співіснування із законодавством у сфері захисту персональних даних.

Регулювання ШІ та захист персональних даних: основні взаємозв'язки

Належний підхід до регулювання ШІ повинен враховувати взаємозв'язки між системами ШІ на різних етапах життєвого циклу та режимом захисту персональних даних. Ці взаємозв'язки виникають під час навчання систем ШІ на тренувальних даних та під час операційної діяльності, коли кінцевий споживач взаємодіє з системою. Зокрема, тренувальні набори даних (дані, які використовуються для навчання систем ШІ) часто містять персональні дані. Одним із прикладів є навчання системи ШІ для виявлення податкового шахрайства на основі баз даних платників податків[8]. Схожих випадків (коли під час функціонування системи ШІ виникнуть питання щодо персональних даних) є чимало, особливо якщо взяти до уваги широкий обсяг терміна «персональні дані». Цей термін традиційно охоплює будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано або може бути ідентифіковано[9], зокрема, коли це може бути зроблено з огляду на наявні технології та інші об'єктивні фактори[10].

Відповідні взаємозв'язки закріплені (як і потенційний негативний вплив) на рівні розроблених сьогодні міжнародно-правових документів. Конвенція містить згадку, що системи ШІ можуть мати негативний вплив на людську гідність та індивідуальну автономію, права людини, демократію та верховенство права[11]. До практик, які можуть мати негативний вплив, Конвенція зараховує незаконне спостереження, що суперечить праву людини на повагу до приватного життя[12]. З огляду на потенційний негативний вплив систем ШІ, Конвенція прямо згадує питання захисту персональних даних. Преамбула Конвенції містить посилання на Конвенцію 108[13], а стаття 11 присвячена питанням приватності та обробки персональних даних і вимагає, щоб держави вживали належних заходів для того, щоб на всіх етапах життєвого циклу систем ШІ захищалися право на приватність та персональні дані, а також забезпечувалися належні гарантії відповідно до національного законодавства та міжнародного права.

Автори Оксфордського посібника з етики ШІ наголошують, що дедалі більше занепокоєння викликають питання приватності суб'єктів даних (споживачів), а відповідні виклики, пов'язані з системами ШІ, зростатимуть у міру того, як відповідні системи діятимуть без прямого нагляду з боку людини[14]. Системи ШІ часто передбачають обробку значної кількості тренувальних даних для вдосконалення (оптимізації) системи. До складу тренувальних даних можуть входити також персональні дані, отримані з різних джерел (не безпосередньо в суб'єкта даних)[15]. Обробка персональних даних можлива також на пізнішому етапі, коли систему ШІ використовують кінцеві споживачі, які можуть передавати власні персональні дані. У кожному з цих випадків особливістю систем ШІ може бути те, що мета, спосіб та обсяг обробки персональних даних можуть змінюватися в процесі функціонування системи, а розробник чи постачальник такої системи не завжди може надати повну інформацію кінцевому споживачу (суб'єкту даних) про порядок обробки персональних даних.

Через широку сферу дії законодавства щодо захисту персональних даних, наявні технологічні можливості (зокрема систем ШІ) та фактичне використання значної кількості персональних даних для систем ШІ перетин між питаннями регулювання систем ШІ та захисту персональних даних є неминучим. З одного боку, беручи до уваги цей перетин, складно заперечити переваги для суб'єктів даних від систем ШІ. Наприклад, у цьому випадку створюється можливість задовольняти більш чітко запити конкретної особи. Водночас така «персоналізована» обробка даних пов'язана з уже традиційними для ШІ ризиками: ризики упередженості алгоритмів та дискримінації конкретних осіб, репутаційної шкоди, втрати (зокрема крадіжки) персональних даних тощо[16].

---

8 Smuha, *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, 133.
9 Див. ст. 2 проєкту Закону про захист персональних даних № 8153 від 25.10.2022.
10 Smuha, *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, 138.
11 Ibid.
12 Ibid.
13 Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Strasbourg: Council of Europe, 1981), https://rm.coe.int/1680078b37.
14 Dubber, Pasquale, and Das, *The Oxford Handbook of Ethics of AI*, 27.
15 Міністерство цифрової трансформації, *Рекомендації з відповідальної розробки систем із використанням технологій штучного інтелекту* (червень 2025), 46, https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs/ШІ%20для%20розробників.pdf.
16 Там само, 133; Бєлова М. В., Бєлов Д. М., «Виклики та загрози захисту персональних даних у роботі зі штучним інтелектом», 20.

Для детальнішого дослідження суміжних ризиків доцільно звернути увагу на питання т. зв. «темних патернів» (*dark patterns* або *deceptive design patterns*). З урахуванням Настанов 03/2022, виданих Європейською радою із захисту даних, до таких патернів належать приховані і часто маніпулятивні дизайнерські або маркетингові тактики, що експлуатують певні упередження, вразливості та уподобання споживачів з метою отримання вигоди бізнесом, який подає певну інформацію, що може не відповідати справжнім інтересам або вподобанням самого споживача[17]. Класичними прикладами є створення хибної ієрархії (коли потрібне для бізнесу рішення, яке може прийняти споживач, є одразу візуально помітнішим чи привабливішим) або створення хибного для споживача відчуття терміновості[18]. Поєднання темних патернів, персональних даних та ШІ створює нові істотні ризики для зловживань, оскільки «ШІ є інструментом, що дозволяє модифікувати темні патерни для досягнення більшого впливу на поведінку споживачів прихованим способом, досліджуючи, які патерни працюють найефективніше, та адаптувати їх відповідним чином»[19].

Зазначене вище підтверджує, що ефективне регулювання ШІ вимагає гармонійного співіснування двох режимів. Юридичні гарантії суб'єкта даних не можна розглядати як певне зовнішнє обмеження. Натомість принципи обробки персональних даних (законність, прозорість, обмеження мети, мінімізація, точність та підзвітність)[20] як важлива частина юридичних гарантій суб'єктів даних повинні бути важливою складовою будь-якого законодавства у сфері ШІ. Для практичної реалізації цього співіснування (регулювання ШІ та захист персональних даних) потрібно впровадити конкретні механізми, як-от ефективний людський нагляд і прозорість систем ШІ, які є інструментами для забезпечення дотримання цих принципів у сфері захисту персональних даних. Ця теза підкріплюється аналізом взаємозв'язків між вказаними принципами та особливостями функціонування систем ШІ, які розглянуто в цій статті.

Законність, мінімізація даних та обмеження мети обробки персональних даних і системи ШІ

Головною вимогою законодавства у сфері захисту персональних даних є вимога законності, що передбачає наявність законної підстави для обробки персональних даних. Контролер самостійно вирішує застосовність тієї чи іншої підстави в кожному випадку обробки персональних даних з урахуванням застосовного законодавства. Найпоширенішими підставами для обробки персональних даних є згода суб'єкта персональних даних, необхідність укладення або виконання правочину із суб'єктом персональних даних (договірна необхідність) та необхідність для цілей легітимного інтересу контролера або третьої особи[21].

Водночас функціонування систем ШІ створює системний конфлікт із наведеним принципом обробки даних. Традиційні підстави для обробки даних, зокрема згода суб'єкта даних чи договірна необхідність, є нежиттєздатними в умовах обробки значних масивів тренувальних даних. Це змушує розробників покладатися на власний легітимний інтерес. Застосування цієї підстави вимагає проведення складного тесту на баланс інтересів: потрібно довести, що права та свободи суб'єктів даних не переважають інтереси розробника.

Складність цього тесту також зростає через те, що стандартні практики розробки ШІ можуть суперечити двом іншим принципам — обмеження мети обробки та мінімізації даних. Навчання моделей часто передбачає вторинне використання даних (наприклад, використання публічно доступної інформації), які первинно збиралися для інших, несумісних цілей. Постає питання, чи є таке використання «подальшою обробкою», чи новим збором, що вимагає окремої правової підстави[22]. Прагнення до точності моделей ШІ спонукає до невибіркового збору значних обсягів даних, що прямо суперечить одному з принципів захисту персональних даних: дозволено обробляти лише ту інформацію, яка є об'єктивно необхідною для досягнення мети. Внаслідок цього виникає суперечність: як розробник системи може довести, що його законний інтерес переважає, якщо сам процес зазвичай побудований на порушенні принципів у сфері захисту персональних даних?

---

17 Smuha, *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, 205; European Data Protection Board, *Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces*, February 2023, 9, https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf.

18 Smuha, *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, 205.

19 Ibid.

20 Див. ст. 4 проєкту Закону про захист персональних даних № 8153 від 25.10.2022 та ст. 5 Загального регламенту про захист даних.

21 Див. ст. 5 проєкту Закону про захист персональних даних № 8153 від 25.10.2022.

22 Smuha, *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, 133.

Наведене вище ставить юридичні гарантії у сфері захисту персональних даних на важливе місце в регулюванні ШІ. Пошук підходу до належного врахування зазначених вимог є складним завданням, оскільки, по-перше, немає єдиних правил для розроблення систем ШІ, а по-друге, розробники не можуть повністю передбачити всі наслідки функціонування систем ШІ та повідомити про них користувачу (проблема «чорної скриньки»). Однак уже на цьому етапі простежується напрям, у якому розробники систем ШІ повинні рухатися для врахування прав та інтересів суб'єктів даних і стандартів ЄС у цій сфері (зокрема забезпечення таких стандартів, як захист персональних даних за проєктуванням та за замовчуванням)[23]. Таким напрямом є потреба в імплементації юридичних гарантій суб'єктів даних на всіх етапах життєвого циклу системи, включно з її розробленням. Замість того щоб намагатися виправдати надмірну обробку персональних даних після етапу розміщення системи ШІ на ринку, розробники повинні заздалегідь впроваджувати технічні та організаційні заходи для мінімізації ризиків, наприклад, відсіювати непотрібну інформацію та проводити оцінювання впливу системи ШІ на права суб'єктів даних. Такі заходи для мінімізації ризиків є практичним втіленням вимог, які на сьогодні впроваджуються в ЄС щодо систем ШІ, — вимог, які забезпечують прозорість систем ШІ та ефективний контроль людини за їхнім функціонуванням.

Прозорість і точність обробки персональних даних, а також обмеження їхнього зберігання в системах ШІ

У попередніх публікаціях ми розглядати важливість принципу прозорості в контексті регулювання систем ШІ[24]. Так, кінцевому користувачу важливо розуміти, як функціонує система ШІ та які наслідки її використання може мати для його прав та інтересів.

Традиційно законодавство у сфері захисту персональних даних відводить питанню прозорості обробки персональних даних важливе місце, покладаючи на контролерів обов'язок надати значний обсяг інформації про відповідну обробку, що охоплює, зокрема, обсяг обробки персональних даних та застосовну мету, а також осіб, залучених до обробки персональних даних (операторів)[25].

Якщо ми говоримо про «традиційну» обробку персональних даних (за межами контексту, пов'язаного із ШІ), ми розуміємо, що контролер спроможний комплексно визначити, які саме персональні дані будуть йому потрібні та з якою метою (наприклад, контролеру відомо, яка інформація йому потрібна для здійснення прямого маркетингу). Проте коли обробка персональних даних здійснюється з використанням систем ШІ — враховуючи саму логіку функціонування технології, особливо якщо вона базується на глибокому навчанні, — розробники систем не завжди можуть оцінити, як система оброблятиме такі дані, для яких цілей та в якому обсязі. Виникає певний парадокс: ставиться вимога прозорості процесів, які за своєю архітектурою є непрозорими навіть для розробників. Це створює перешкоду, що істотно ускладнює повноцінне виконання обов'язку з інформування суб'єктів даних.

Цей конфлікт загострюється також через те, що законодавство у сфері захисту персональних даних ґрунтується на принципі пропорційності, що охоплює мінімізацію та точність обробки персональних даних, які ми згадували вище, та передбачає, що дані підлягають видаленню після досягнення мети[26]. Натомість логіка розроблення ШІ часто виходить із принципу максималізму («що більше даних, то краще»), розглядаючи дані як постійний актив для навчання моделей. Внаслідок цього системи накопичують значні обсяги персональних даних, які згодом втрачають точність та актуальність, але зберігаються та обробляються, порушуючи тим самим весь комплекс взаємопов'язаних принципів.

В умовах такого системного конфлікту механізмом, здатним узгодити співіснування систем ШІ та захисту персональних даних, є ефективний людський нагляд і прозорість систем ШІ. Саме ці інструменти дають змогу поєднати юридичні гарантії суб'єкта даних (насамперед основні принципи обробки даних) із життєвим циклом ШІ. Інакше є ризик неконтрольованого, непрозорого та безстрокового накопичення персональних даних для будь-яких цілей. Такий підхід дасть змогу, по-перше, оцінювати пропорційність обробки даних і точність персональних даних,

---

[23] Див. ст. 29 проєкту Закону про захист персональних даних № 8153 від 25.10.2022.

[24] Олександр Кожухар, «Принцип прозорості в контексті правового регулювання систем штучного інтелекту», *Наукові записки НаУКМА. Юридичні науки* 15 (2025): 78–85, https://doi.org/10.18523/2617-2607.2025.15.78-85.

[25] Див. ст. 6 проєкту Закону про захист персональних даних № 8153 від 25.10.2022.

[26] Див. ст. 4 проєкту Закону про захист персональних даних № 8153 від 25.10.2022.

які обробляються в певний момент, як розробнику чи постачальнику, так і суб'єкту даних; по-друге, забезпечувати ефективну взаємодію між суб'єктом даних та розробником і постачальником даних щодо всіх питань обробки персональних даних (і таким чином гарантувати підзвітність останніх). У регулюванні ШІ це наближатиме досягнення мети, яку на сьогодні задекларовано в підході ЄС до цього питання, — забезпечення співіснування регулювання систем ШІ та законодавства у сфері захисту персональних даних.

Висновки та перспективи подальшого розроблення тематики ШІ

Проведене дослідження демонструє стійкий зв'язок між правовим регулюванням систем ШІ та режимом захисту персональних даних. Обґрунтовано, що архітектура та логіка функціонування систем ШІ, які базуються на обробці великих масивів даних та містять елемент алгоритмічної непрозорості, вступають у системний конфлікт із принципами захисту даних, зокрема з принципами законності, мінімізації, прозорості та точності. Це підтверджує тезу нашого дослідження проблематики ШІ: розроблення ефективного регулювання ШІ потребує належної імплементації юридичних гарантій, передбачених законодавством про захист персональних даних.

Важливим висновком є також те, що для подолання цього системного конфлікту недостатньо лише імплементації Регламенту. З огляду на Акт про ШІ та Конвенцію, потрібно впроваджувати додаткові інструменти, які будуть забезпечувати баланс між регулюванням ШІ та захистом персональних даних. На нашу думку, такими інструментами є прозорість систем ШІ та ефективний людський контроль. Для України як держави, де (у розумінні ЄС) не забезпечено належний захист персональних даних, це означає нагальну потребу в гармонізації національного законодавства з європейським підходом до регулювання ШІ та захисту персональних даних (Регламент, Конвенція та Акт про ШІ) та розбудові інституційної спроможності, насамперед через створення компетентного наглядового органу.

Матеріали цієї статті як частина нашого аналізу проблематики ШІ увійдуть до відповідного розділу дисертаційного дослідження. Проведений аналіз, зосереджений на принципах обробки даних, створює підґрунтя для подальшого вивчення впливу ШІ на реалізацію конкретних прав суб'єктів даних. Перспективи подальших досліджень полягатимуть у детальному аналізі викликів, які системи ШІ створюють для таких прав, як «право на забуття» та права суб'єкта даних у зв'язку з автоматизованою обробкою даних. Зокрема, буде досліджено, наскільки технічно можливо реалізувати «забуття» даних у системах ШІ та як забезпечити право людини на прозорість (пояснюваність) рішення, ухваленого системою ШІ.

Список використаної літератури

Бєлова, М. В., Бєлов Д. М. «Виклики та загрози захисту персональних даних у роботі зі штучним інтелектом». *Науковий вісник Ужгородського Національного Університету. Серія: Право* 79, ч. 2 (2023): 17–22. https://doi.org/10.24144/2307-3322.2023.79.2.2.

Кожухар, Олександр. «Принцип прозорості в контексті правового регулювання систем штучного інтелекту». *Наукові записки НаУКМА. Юридичні науки* 15 (2025): 78–85. https://doi.org/10.18523/2617-2607.2025.15.78-85.

CNIL. *Relying on the Legal Basis of Legitimate Interests to Develop an AI System.* 2024. https://www.cnil.fr/en/relying-legal-basis-legitimate-interests-develop-ai-system.

Dubber, Markus Dirk, Frank Pasquale, and Sunit Das. *The Oxford Handbook of Ethics of AI.* Oxford University Press, 2021.

European Data Protection Board. *Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces.* February 2023. https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf.

European Data Protection Board. *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models.* December 2024. https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf.

Smuha, Nathalie A. *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence.* Cambridge University Press, 2025.

Bibliography

Bielova, M., and D. Byelov. "Challenges and Threats of Personal Data Protection in Working with Artificial Intelligence." *Uzhhorod National University Herald. Series: Law* 79, part 2 (2023): 17–22. https://doi.org/10.24144/2307-3322.2023.79.2.2 [in Ukrainian].

CNIL. *Relying on the Legal Basis of Legitimate Interests to Develop an AI System.* 2024. https://www.cnil.fr/en/relying-legal-basis-legitimate-interests-develop-ai-system.

Dubber, Markus Dirk, Frank Pasquale, and Sunit Das. *The Oxford Handbook of Ethics of AI.* Oxford University Press, 2021.

European Data Protection Board. *Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces.* February 2023. https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf.

European Data Protection Board. *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models.* December 2024. https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf.

Kozhukhar, Oleksandr. "The Principle of Transparency in the Context of Legal Regulation of Artificial Intelligence Systems." *NaUKMA Research Papers. Law* 15 (2025): 78–85. https://doi.org/10.18523/2617-2607.2025.15.78-85 [in Ukrainian].

Smuha, Nathalie A. *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence.* Cambridge University Press, 2025.

Oleksandr Kozhukhar
Doctoral student,
Department of General Legal Theory and Public Law, Faculty of Law,
National University of Kyiv-Mohyla Academy, Kyiv, Ukraine
https://orcid.org/0009-0006-4183-3289
o.kozhukhar@ukma.edu.ua

LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE SYSTEMS AND PERSONAL DATA PROTECTION: LINES OF INTERCONNECTION

Abstract

The article explores the interplay between the potential legal regulation of artificial intelligence (AI) systems and the personal data protection regime. The analysis is conducted with due regard to the relevant trends in AI regulation, particularly the (EU) AI Act and the Council of Europe Framework Convention on AI, which currently define the vector for policy development at the international and national levels. The article substantiates that the architecture of modern AI systems, at all stages of their lifecycle (from development to practical implementation), is associated with significant personal data processing operations. This creates systemic risks to the rights and freedoms of data subjects, causing a certain conflict between the innovative potential of AI and the established guarantees in the sphere of personal data protection. These risks are especially significant in jurisdictions with an inadequate level of personal data protection, which includes Ukraine, making the analysis of the interconnections between AI systems and personal data protection particularly relevant.

The research demonstrates how key principles of personal data protection (such as lawfulness, data minimisation, purpose limitation, transparency, and accuracy) face challenges in the AI context. For example, the principle of data minimisation conflicts with the need for AI systems to use large datasets for system development purposes, and the "black box" problem of AI systems may be inconsistent with the requirement of data processing transparency. The author argues for the necessity of developing an approach where data protection requirements (updated in line with current EU standards, including the General Data Protection Regulation) must be an integral part of the legal regulation of AI in Ukraine. The key mechanisms that allow for the implementation of such an approach are AI transparency and human oversight, which enable the realisation of other guarantees both in the sphere of personal data protection and in the context of AI regulation. For Ukraine, this also signifies an urgent need to implement the relevant norms and to create a corresponding supervisory authority with a sufficient level of institutional capacity. These conclusions are important for further work on draft data protection law No. 8153 and for the formation of a national strategy for regulating AI.

Keywords: human rights, legal regulation, legal guarantees, artificial intelligence, AI, privacy, personal data protection, General Data Protection Regulation, Convention on AI.

Матеріал надійшов 11.06.2025
Схвалено до публікації 23.09.2025
Оприлюднено 31.12.2025