DOI: 10.33498/louu-2025-04-026

Максим Суржинський

кандидат юридичних наук,
науковий співробітник відділу міжнародного права
та права Європейського Союзу
Інституту держави і права імені В. М. Корецького НАН України
(Київ, Україна)
ORCID ID: https://orcid.org/0000-0003-1697-1816
maksym.surzhynskyi@gmail.com

УДК 346.7:342.721:614.2

# ВИКЛИКИ ТА МОЖЛИВОСТІ АДАПТАЦІЇ ЗАКОНОДАВСТВА УКРАЇНИ ДО ЄВРОПЕЙСЬКИХ СТАНДАРТІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ШТУЧНОГО ІНТЕЛЕКТУ

Анотація. Дослідження адаптації законодавства України до європейських стандартів захисту персональних даних у сфері штучного інтелекту (далі – ШІ) зумовлене низкою питань, що виникають із швидкого розвитку технологій, а також необхідністю забезпечення прав людини, прозорості й підзвітності при автоматизованій обробці персональних даних. Особливу складність становить регулювання специфічних правовідносин, що виникають під час використання ШІ, зокрема профілювання, автоматизованого прийняття рішень, етичного та недискримінаційного застосування алгоритмів, а також забезпечення належних гарантій для суб'єктів даних.

Метою цієї статті є комплексний аналіз європейських правових актів (GDPR та AI Act), чинного українського законодавства і перспективних його змін, зокрема проєкту Закону № 8153 "Про захист персональних даних", для вироблення цілісного бачення викликів і можливостей у гармонізації українського права з європейськими стандартами. Також метою є визначення напрямів подальшого удосконалення національного законодавства, здатного забезпечити належний захист персональних даних при використанні технологій ШІ.

Встановлено, що чинні норми українського права потребують значного доопрацювання з метою ефективного врахування специфіки технологій ШІ, особливо у питаннях прозорості алгоритмів, захисту від автоматизованих рішень, а також гарантій щодо етики і недискримінації. Виявлено необхідність підтримки малого і середнього підприємництва (далі – МСП) при адаптації до нових вимог GDPR та AI Act, а також вирішення складних питань транскордонної передачі даних. Сформульовано рекомендації щодо запровадження спеціалізованих правових інструментів (етичні кодекси, регуляторні пісочниці), які забезпечать баланс між захистом прав суб'єктів даних та інноваційною діяльністю у сфері ШІ.

Ключові слова: персональні дані; штучний інтелект; GDPR; AI Act; автоматизоване прийняття рішень; прозорість алгоритмів; етика штучного інтелекту; гармонізація законодавства; штучний інтелект; Fully Homomorphic Encryption.



У сучасну епоху цифрової трансформації обсяг і цінність персональних даних зросли до безпрецедентного рівня. За прогнозами, до 2028 р. світовий обсяг даних досягне 394 зетабайтів[1], що відображає стрімке зростання циф-

[1] P Taylor, 'Amount of data created, consumed, and stored 2010-2023, with forecasts to 2028' (Nov 21, 2024) <https://www.statista.com/statistics/871513/worldwide-data-created> (accessed 14.04.2025).

ровізації, накопичення інформації. Стрімкий розвиток технологій штучного інтелекту (далі – ШІ) та масове використання великих даних загострюють питання захисту персональної інформації. Практично кожна сфера суспільного життя пов'язана з обробкою цифрової інформації про осіб, що висуває нові вимоги до правового забезпечення права на приватність та захисту персональних даних. Традиційні підходи і законодавчі інструменти нерідко виявляються застарілими перед стрімким технологічним прогресом, створюючи правові прогалини та ризики зловживань. Подібні проблеми актуальні й для України: чинні норми не враховують сучасних технологічних реалій і фактично гальмують впровадження інноваційних рішень у сфері обробки даних. Це зумовлює нагальну потребу в модернізації нормативної бази для належної охорони персональних даних та адаптації до викликів цифрової доби.

Тому метою цього дослідження й стало визначення, яких змін потребує законодавство України задля відповідності європейським стандартам захисту персональних даних у сфері ШІ, а також які виклики й можливості виникають у цьому процесі. Так, на міжнародному рівні вже сформовані уніфіковані стандарти захисту даних, зокрема, Європейський Загальний регламент із захисту даних (General Data Protection Regulation, GDPR) встановив суворі вимоги до організацій, які обробляють персональні дані резидентів ЄС[2], і фактично став глобальним еталоном приватності. Прийнятий 14 квітня 2016 р., він набув чинності 25 травня 2018 р., замінивши Директиву 95/46/ЄС про захист даних від 1995 р.[3], яка до того часу становила основу правового режиму ЄС у цій сфері[4].

GDPR встановлює єдиний для всіх держав – членів ЄС правовий режим, який значно полегшує транснаціональну діяльність організацій завдяки усуненню нормативної фрагментації. Окрім того, він істотно посилює права суб'єктів даних, запровадивши нові інструменти контролю, зокрема право на перенесення даних, право на стирання ("право бути забутим") та посилені вимоги до згоди на використання особистих даних.

Регламент GDPR визначає три фундаментальні цілі:

1) зміцнення контролю фізичних осіб над своїми персональними даними, зокрема, шляхом надання прозорої інформації про обробку даних і забезпечення прав на заперечення та обмеження обробки;

[2] 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) <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (accessed 14.04.2025).

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data <https://eur-lex.europa.eu/eli/dir/1995/46/oj> (accessed 14.04.2025).

[4] General Data Protection Regulation (n 2).

2) гармонізація законодавства держав – членів ЄС, що створює передумови для уніфікованого правозастосування й зменшення адміністративного навантаження на бізнес;

3) адаптація до викликів цифрової трансформації, включаючи технології хмарних обчислень, інтернет-банкінг, великі дані та алгоритмічне прийняття рішень.

Сфера застосування GDPR є надзвичайно широкою: вона охоплює як суб'єктів, що здійснюють обробку персональних даних на території ЄС, так і ті організації, які, перебуваючи за межами ЄС, пропонують товари або послуги резидентам ЄС чи здійснюють моніторинг їхньої діяльності в мережі Інтернет (ст. 3 GDPR).

Ключовим поняттям у регламенті є "персональні дані", що визначаються як будь-яка інформація, яка прямо або опосередковано дає змогу ідентифікувати фізичну особу. До них належать, зокрема, ім'я, адреса електронної пошти, геолокаційні дані, IP-адреси, біометричні й генетичні дані (ст. 4 GDPR). Водночас окремі категорії діяльності, такі як обробка для виключно особистих чи побутових потреб, діяльність органів національної безпеки або правоохоронних органів, не підпадають під дію GDPR (ст. 2).

Попри значний позитивний вплив GDPR на розвиток культури захисту даних, практика його застосування супроводжується низкою викликів. Серед них:

– складність упровадження для малого і середнього підприємництва (далі – МСП), який часто не має ресурсів для повноцінної відповідності вимогам GDPR;

– юридична неоднозначність окремих положень, таких як псевдонімізація або автоматизоване прийняття рішень (ст. 22 GDPR), що викликає суперечки як серед правників, так і серед науковців[5];

– потенційний стримуючий ефект для інновацій, особливо у сфері ШІ та аналізу великих даних, де суворі обмеження на обробку персональної інформації можуть перешкоджати розвитку нових технологій[6]. У контексті ШІ особливо важливими є положення GDPR щодо автоматизованого прийняття рішень і профілювання. Стаття 22 GDPR надає особі право не підпадати під рішення, що базується виключно на автоматизованій обробці (включно з профілюванням), якщо таке рішення має значні наслідки. Відповідно контролери зобов'язані впроваджувати запобіжні заходи, зокрема людське втручання та можливість оскарження рішення. Також GDPR встановлює вимогу інформувати суб'єкта про логіку та наслідки автоматизованої обробки його даних, а у випадку систематичного профілювання – проводити оцінку впливу на права та свободи (Data Protection Impact Assessment, DPIA). Отже,

[5] C Kuner, L A Bygrave, C Docksey (eds), *The EU General Data Protection Regulation (GDPR): A commentary* (Oxford University Press 2017).

[6] M Brkan, 'Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond' [2019] 27(2) International Journal of Law and Information Technology 91–121.

GDPR уже заклав базові гарантії проти непрозорих або дискримінаційних рішень ШІ, хоча й не містить детальних правил саме для технологій штучного інтелекту.

GDPR виступає не лише як інструмент регулювання, а й як еталон для законодавчих ініціатив у сфері конфіденційності в усьому світі. Широке застосування GDPR також спричинило так званий феномен "брюссельського ефекту", який продемонстрував здатність ЄС де-факто експортувати свої регуляторні стандарти за межі власної юрисдикції[7]. Його принципи прозорості, мінімізації даних і відповідальності активно впливають на формування глобальної практики обробки персональної інформації. Незважаючи на існуючі складнощі, GDPR залишається зразком для країн, що прагнуть модернізувати своє законодавство про захист даних відповідно до викликів XXI ст.

Однак через критику щодо надмірного регуляторного навантаження на МСП Європейська Комісія вже почала розроблення планів спрощення GDPR, які мають бути впроваджені до середини 2025 р.[8] Загалом прийняття GDPR стало потужним каталізатором процесів гармонізації національних законодавств у сфері персональних даних навіть поза межами ЄС, закріпивши тенденцію до світового підвищення вимог щодо приватності.

Усвідомлюючи обмеженість загальних норм GDPR для специфіки ШІ, ЄС розробив окремий правовий акт для всеосяжного регулювання штучного інтелекту. Регламент ЄС 2024/1689 (AI Act)[9] ухвалений у червні 2024 р. і набув чинності 1 серпня 2024 р., ставши першою комплексною спробою врегулювати ШІ на рівні широкої юрисдикції ЄС.

AI Act запроваджує ризик-орієнтований підхід: всі системи ШІ поділяються на категорії за рівнем ризику. Системи ШІ з неприйнятним рівнем ризиків заборонені до використання – зокрема, заборонено алгоритми, що маніпулюють поведінкою людей таким чином, щоб суттєво спотворити їхні рішення, а також системи "соціального рейтингування", які класифікують осіб за поведінкою чи характеристиками з метою присвоєння їм соціальної оцінки. Під пряму заборону також підпали деякі практики, пов'язані з біометричними технологіями (як біометрична класифікація осіб за певними ознаками) та оцінка емоцій у чутливих сферах на кшталт працевлаштування чи освіти. Для високоризикованих систем ШІ (High-risk AI) AI Act встановлює суворі вимоги: розробники мають здійснювати належне управління даними та ризиками, забезпечувати якість і релевантність датасетів, документува-

[7] A Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).

[8] K Van Quathem, 'European Commission Confirms Plans to Simplify GDPR' (March 17, 2025) <https://www.insideprivacy.com/gdpr/european-commission-confirms-plans-to-simplify-gdpr> (accessed 14.04.2025).

[9] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (accessed 14.04.2025).

ти роботу систем, проводити оцінку відповідності тощо. Окремо регламент закріплює обов'язок забезпечити людський нагляд за функціонуванням ШІ всюди, де це потрібно для захисту основоположних прав. Також закон вимагає певної прозорості: наприклад, розробники повинні інформувати людей про те, що вони взаємодіють із системою ШІ (це стосується, зокрема, чатботів чи систем розпізнавання облич).

Важливо, що AI Act не скасовує дію GDPR (прямо передбачено в ст. 2 Регламенту); навпаки, він доповнює його, створюючи "гармонізовані правила" для використання ШІ при обробці даних з метою краще гарантувати права суб'єктів. Новий закон накладає обов'язки не тільки на класичних володільців і розпорядників даних, а й на інших пов'язаних суб'єктів – розробників, постачальників, користувачів ШІ-систем. Таким чином, у ЄС сформовано дворівневу систему регулювання: загальні вимоги захисту даних за GDPR, а також спеціальні вимоги та обмеження для ШІ за AI Act. Експерти відзначають, що GDPR містить певні розмиті норми й відкриті стандарти, застосування яких потребує балансу інтересів, через що їх може бути недостатньо для унікальних ризиків ШІ. Прийняття AI Act заповнює цю прогалину, запроваджуючи більш чіткі та специфічні правила саме для технологій ШІ – орієнтовані на оцінку рівнів ризику, управління життєвим циклом систем і недопущення порушень прав людини.

Водночас стрімкий розвиток технологій ШІ спричиняє виникнення й нових технічних рішень для забезпечення приватності, безпечної обробки даних системами та більш повної реалізації прав суб'єктів даних. У цьому контексті повністю гомоморфне шифрування (Fully Homomorphic Encryption, FHE) постає як трансформаційна криптографічна технологія підвищення конфіденційності, яка дає змогу обробляти зашифровані дані без їх розшифрування, забезпечуючи безпеку протягом усього циклу використання таких даних. Це означає, що сторонній обчислювальний ресурс може оперувати з даними, не маючи до них доступу у відкритому вигляді, що суттєво підвищує рівень безпеки і знижує ризики витоку[10].

Концепція FHE була вперше реалізована в докторській дисертації К. Джентрі у 2009 р., де він запропонував криптографічну систему, що уможливлює обмежене (а згодом – повне) гомоморфне обчислення на зашифрованих даних[11]. Подальший розвиток технології відбувався шляхом створення більш ефективних схем, таких як BGV (Brakerski–Gentry–Vaikuntanathan)[12] і FV

[10] V Vaikuntanathan, 'Computing Blindfolded: New Developments in Fully Homomorphic Encryption' *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science* (Palm Springs, 2011) 5–16.
[11] C Gentry, 'A Fully Homomorphic Encryption Scheme' (Doctoral dissertation, Stanford University 2009) <https://crypto.stanford.edu/craig/craig-thesis.pdf> (accessed 14.04.2025).
[12] Z Brakerski, C Gentry, V Vaikuntanathan, 'Fully Homomorphic Encryption without Bootstrapping' [2014] 6 ACM Transactions on Computation Theory 13.

(Fan–Vercauteren)[13], що суттєво зменшили обчислювальні витрати й зробили FHE придатним для практичного застосування.

Ця інновація пропонує безпрецедентні переваги безпеки, особливо в таких секторах, як ШІ, інтернет-банкінг, блокчейн і хмарні обчислення, де кіберзагрози та витоки даних стають дедалі масштабнішими. Останні розробки новітніх обчислювальних чипів, напрям інвестицій венчурного капіталу та діяльність міжгалузевих консорціумів, таких як FHETCH, свідчать про те, що FHE наближається до широкого впровадження[14].

GDPR проголошує захист персональних даних як фундаментальне право (ст. 1(2)), і встановлює низку принципів, зокрема мінімізації даних, обмеження цілі, прозорості й безпеки обробки (ст. 5)[15]. У цьому контексті FHE набуває особливої ваги, оскільки дає змогу реалізувати обробку даних відповідно до принципу "конфіденційності за замовчуванням" (data protection by default), зберігаючи змістовність обробки при повному збереженні шифрування. Крім того, згідно з Recital 78 GDPR контролери повинні впроваджувати "технології, що забезпечують конфіденційність за проєктом" (data protection by design), і FHE є одним із небагатьох сучасних рішень, які можуть відповідати цим вимогам навіть у хмарному середовищі, де ризики доступу сторонніх осіб до персональних даних особливо високі.

У правовому аспекті перспективним є також використання FHE у контексті забезпечення згоди на обробку даних (ст. 7 GDPR), коли обробка здійснюється автоматизовано без прямого доступу до інформації. Це відкриває нові горизонти для етичного використання ШІ в медицині, фінансах та науці.

Особливо цінним може бути внесок FHE у забезпечення безпечного транскордонного обміну даними. Стаття 44 GDPR вимагає еквівалентного рівня захисту при передачі даних до третіх країн. FHE усуває потребу в розшифруванні, знижуючи ризик витоків під час таких операцій. Це набуває актуальності в контексті спрощення GDPR для МСП, де зменшення адміністративного навантаження має поєднуватися з високими стандартами безпеки. Крім того, FHE посилює суверенітет даних, дозволяючи організаціям зберігати контроль над інформацією навіть при використанні зовнішніх ресурсів, що відповідає принципам прозорості та підзвітності GDPR. Зазначена технологія здатна докорінно змінити підхід до дотримання суворих норм захисту персональних даних, зокрема GDPR.

Для України проблематика захисту персональних даних у контексті ШІ систем набуває особливої гостроти в умовах війни та водночас курсу на європейську інтеграцію. Повномасштабна російська агресія, що триває з 2022 р., не лише створила безпрецедентні виклики безпеці, а й прискорила

[13] J Fan, F Vercauteren, 'Somewhat Practical Fully Homomorphic Encryption' [2012] IACR Cryptol. ePrint Arch 144 <https://eprint.iacr.org/2012/144> (accessed 14.04.2025).
[14] J Myszne, '3 Homomorphic Encryption Trends for 2025' (December 19, 2024) <https://www.itprotoday.com/data-privacy/three-homomorphic-encryption-trends-for-2025> (accessed 14.04.2025).
[15] General Data Protection Regulation (n 2).

цифровізацію суспільства та державного управління. Під час війни держава швидко розширила перелік електронних послуг: лише з 2019 р. впроваджено понад 250 цифрових сервісів, і натепер близько 19 мільйонів громадян (половина населення) користуються мобільним застосунком "Дія" для отримання цифрових документів та послуг[16]. Водночас зростає значення належного захисту цих масивів даних і гарантій приватності, особливо з огляду на посилені кіберзагрози та широкого залучення ШІ в кампанії по дезінформації населення. Війна змусила адаптувати й регуляторні підходи: з міркувань збереження інформації в умовах атак на ІТ-інфраструктуру необхідністю стала обробка персональних даних на хмарних серверах за кордоном, хоча раніше пріоритет надавався локальному зберіганню. Крім того, набуття Україною статусу кандидата в члени ЄС надало додаткового імпульсу реформам, спрямованим на гармонізацію національного законодавства із правом ЄС у сфері захисту даних[17]. Відповідність європейським стандартам приватності розглядається як необхідна передумова євроінтеграції та зміцнення суспільної довіри до цифрових сервісів.

У межах євроінтеграційних зусиль держава розпочала перегляд законодавства про персональні дані з урахуванням європейських вимог. Вагомим кроком стало ухвалення Верховною Радою у першому читанні законопроєкту № 8153 "Про захист персональних даних", що має замінити застарілий закон 2010 р.[18] Цей проєкт спрямований на гармонізацію національних правил із європейськими стандартами, зокрема імплементацію підходів GDPR[19] та положень модернізованої Конвенції 108+ Ради Європи[20]. Новий законопроєкт передбачає якісно інший підхід до приватності: встановлення чітких принципів обробки даних за сучасними міжнародними вимогами та розширення прав суб'єктів даних (право на забуття, обмеження обробки, переносимість даних, заперечення проти обробки, захист від автоматизованого прийняття рішень). Також запроваджено принципи "захист даних за замовчуванням" і "захист даних за проєктуванням", що гарантують високий рівень конфіденційності з самого початку і у всіх процесах обробки. Проєкт вимагає обов'язкового повідомлення контролюючих органів про витоки даних протягом 72 годин, чітко регулює транскордонну передачу пер-

[16] Звіти про роботу Міністерства цифрової трансформації <https://thedigital.gov.ua/community/reports> (дата звернення 14.04.2025).

[17] Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025–2027 роках: розпорядження Кабінету Міністрів України від 31 грудня 2024 р. № 1351-р <https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text> (дата звернення 14.04.2025).

[18] Проект Закону про захист персональних даних № 8153 від 25.10.2022 <https://itd.rada.gov.ua/billInfo/Bills/Card/40707> (дата звернення 14.04.2025).

[19] General Data Protection Regulation (n 2).

[20] Convention for the protection of individuals with regard to the processing of personal data. Convention 108 + <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1> (accessed 14.04.2025).

сональної інформації за умови належного рівня захисту, а також вводить ефективні фінансові санкції за порушення.

Також варто зазначити, що, хоча законопроєкт має на меті імплементувати багато ключових стандартів GDPR щодо автоматизованої обробки даних, деякі його положення залишаються занадто загальними для особливостей ШІ. По суті, документ зосереджується на універсальних нормах захисту даних і прямо не регламентує специфічні ризики, що їх несуть складні алгоритми штучного інтелекту. У ЄС таку специфіку покликаний покрити окремий AI Act, а український підхід натепер – використовувати наявні акти (як Закон про персональні дані) та м'яке регулювання. Урядова "Біла книга з регулювання ШІ"[21] передбачає на найближчі 2–3 роки переважно саморегуляцію галузі замість ухвалення спеціального закону. Це означає, що індустрія ШІ має керуватися чинними нормами (у т. ч. законодавством про дані) та добровільними рекомендаціями до моменту імплементації європейського AI Act в Україні. Такий гнучкий підхід допомагає не гальмувати інновації, але водночас створює регуляторні прогалини. Отже, аналіз законопроєкту № 8153 показує, що він є необхідною базою для адаптації до GDPR і дає змогу частково охопити проблематику ШІ, але для комплексного врегулювання штучного інтелекту в майбутньому знадобляться додаткові спеціальні норми.

Процес гармонізації з правом ЄС ускладнюється також низкою інших пов'язаних з ШІ викликів, зокрема щодо правозастосування, інституційної спроможності, транскордонного обміну даними та економічного навантаження на МСП у зв'язку з необхідністю адаптації до вимог GDPR. Далі пропонуємо розглянути ці виклики докладніше.

*Транскордонна передача даних:* GDPR дозволяє передачу персональних даних до третіх країн лише за умови забезпечення адекватного рівня захисту. Україна натепер не отримала рішення про адекватність від Європейської Комісії, що ускладнює обмін даними з європейськими суб'єктами. Українським організаціям доводиться використовувати стандартні договірні умови (SCC) або обов'язкові корпоративні правила (BCR), які є складними та ресурсозатратними. Відсутність рішення про адекватність створює юридичну невизначеність, особливо для IT-сектору та аутсорсингових компаній. Впровадження FHE може допомогти Україні продемонструвати відповідність стандартам GDPR, що є ключовим для отримання рішення про адекватність від Європейської Комісії. Безпечна обробка та обмін зашифрованими даними знижує ризики порушення конфіденційності, що є важливим для транскордонних потоків даних (Data protection adequacy).

*Баланс між національною безпекою та приватністю.* У контексті геополітичної напруженості Україна приділяє значну увагу кібербезпеці та національній обороні, що іноді суперечить принципам конфіденційності

[21] Біла книга з регулювання ШІ в Україні: бачення Мінцифри <https://thedigital.gov.ua/storage/uploads/files/page/community/docs/Регулювання%20ШІ.pdf> (дата звернення 14.04.2025).

GDPR. Наприклад, практики спостереження чи зберігання даних для протидії кіберзагрозам або з метою використання у війні можуть порушувати права на приватність. Для вирішення цієї дилеми необхідний збалансований підхід, який включає незалежний нагляд за діяльністю спецслужб і прозорість процедур збору інформації. Для вирішення цієї колізії Україна має сформувати збалансований підхід, який забезпечить як національну безпеку, так і дотримання принципів GDPR. Це може включати впровадження незалежного нагляду за діяльністю спецслужб, прозорість процедур збору інформації та наявність судового контролю над діяльністю, пов'язаною із захистом національної безпеки. Крім того, технічні інструменти, зокрема FHE, можуть сприяти дотриманню прав на конфіденційність навіть у контексті розширених заходів безпеки.

*Економічні та адміністративні навантаження на МСП.* GDPR накладає суворі обов'язки на контролерів і операторів, включаючи проведення оцінок впливу на захист даних (DPIA), призначення уповноважених із захисту даних (DPO) та ведення обліку операцій обробки. Для МСП із обмеженими ресурсами ці вимоги можуть бути надмірно обтяжливими. Досвід ЄС показує, що МСП з чисельністю працівників менше 250 осіб можуть бути звільнені від деяких зобов'язань, якщо обробка даних не становить загрози правам суб'єктів. Європейська Комісія також планує спростити GDPR для МСП до кінця 2025 р., що може слугувати орієнтиром для України після внесення відповідних змін до законопроєкту. Зокрема, розглядається запровадження пільг, таких як спрощення вимог до документації чи розробка шаблонів для оцінки відповідності – за допомогою FHE держава може полегшити дотримання GDPR для малого бізнесу без шкоди для загального рівня захисту персональних даних. Це також відповідатиме стратегічним економічним пріоритетам України, зокрема стимулюванню підприємництва й залученню інвестицій.

*Інституційні та правозастосовчі прогалини.* GDPR потребує наявності незалежних наглядових органів, таких як Європейська рада із захисту даних (EDPB), які забезпечують узгоджене застосування регламенту GDPR. В Україні цю функцію виконує Уповноважений Верховної Ради України з прав людини (омбудсмен), який є обмеженим у ресурсах і технічній експертизі. Так офіс омбудсмена зазнає особливих труднощів з ефективним правозастосуванням чинного Закону України "Про захист персональних даних" 2010 р.[22], особливо у справах, пов'язаних із транснаціональними корпораціями чи транскордонними потоками даних. Посилення інституційної спроможності офісу Омбудсмена або визначення іншого уповноваженого органу державної влади, збільшення фінансування та підвищення кваліфікації є необхідним для відповідності стандартам GDPR.

[22] Про захист персональних даних: Закон України від 1 червня 2010 р. № 2297-VI <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення 14.04.2025).

*Громадська обізнаність і культурні бар'єри.* Низька обізнаність громадян України про їхні права щодо захисту персональних даних знижує ефективність законодавства. GDPR надає суб'єктам даних права на доступ, виправлення та видалення даних, але багато українців не знають, як ними скористатися. Освітні ініціативи, підтримувані Радою Європи, такі як заходи до "Дня захисту даних", є важливими для формування культури конфіденційності. На тлі численних інцидентів витоку даних і зловживань приватною інформацією, які підривають довіру споживачів по всьому світу, надійне законодавство про захист даних може стати суттєвою конкурентною перевагою. Гармонізація з GDPR дасть Україні змогу запевнити своїх громадян і міжнародних партнерів у тому, що персональні дані обробляються відповідально й безпечно, що особливо важливо в умовах ведення повномасштабних військових дій. Крім того, узгодження із GDPR здатне стимулювати цифрові інновації, створюючи стабільне й передбачуване нормативне середовище, а впровадження технологій, таких як FHE, дасть змогу здійснювати захищену обробку даних, відкриваючи нові можливості для інновацій у галузях охорони здоров'я, фінансів та штучного інтелекту. Ці досягнення принесуть вигоди не лише бізнесу, а й суспільству загалом – шляхом покращення якості медичних послуг, державного управління та освітніх ініціатив.

Висновки. Адаптація законодавства України до європейських стандартів захисту персональних даних у сфері ШІ є складним, але необхідним процесом на шляху цифрової трансформації та євроінтеграції України. Проведений аналіз показав, що законопроєкт № 8153 закладає міцну основу, імплементуючи основоположні принципи GDPR і значно підвищуючи рівень захисту даних в Україні. Це створює можливості для тіснішої співпраці з ЄС, зокрема перспективи визнання належного рівня захисту (адекватності) та інтеграції до єдиного європейського ринку даних. Нове законодавство зміцнить права громадян на приватність, підвищить довіру до цифрових послуг і відкриє українському бізнесу двері до глобальних ринків за умови відповідності високим стандартам. Водночас виклики залишаються суттєвими.

По-перше, загальні норми захисту даних потребують деталізації для врахування специфіки ШІ – сучасні алгоритми потребують більш тонкого регулювання, ніж передбачено нині (особливо у частині контролю за навчанням моделей, запобігання дискримінації, забезпечення прозорості складних нейромереж тощо).

По-друге, реалізація прийнятих правил вимагатиме значних ресурсів та організаційних зусиль: потрібні кваліфіковані кадри, розбудова дієвого наглядового органу, підвищення обізнаності суспільства і бізнесу. МСП слід надати підтримку, щоб нові вимоги не стали для них непомірним тягарем.

По-третє, регуляторна система повинна встигати за технологічними змінами – і тут нагальним є налагодження механізмів моніторингу та гнучкого оновлення норм у разі потреби. Використання FHE відкриває нові перспективи для посилення конфіденційності даних та забезпечення нормативної відповідності сучасним стандартам. Його ключова перевага полягає у мож-

ливості виконувати обчислення безпосередньо над зашифрованими даними, без їх попереднього розшифрування. Таким чином, FHE ефективно вирішує фундаментальні проблеми традиційних методів шифрування та бездоганно відповідає принципам GDPR, зокрема принципам мінімізації даних, обмеження цілі обробки та підзвітності. Завдяки потенціалу забезпечувати безпечну транскордонну передачу інформації, зміцнювати суверенітет над даними та суттєво знижувати ризики порушень приватності, FHE має стратегічне значення як для розвитку нормативної бази Європейського Союзу, так і для процесів гармонізації законодавства України зі стандартами GDPR.

Зусилля Європейської Комісії, спрямовані на спрощення процедур GDPR, особливо для МСП, є важливим орієнтиром для України та мають бути відображені в законопроєкті. Спрощення вимог до ведення документації та зменшення адміністративних обтяжень можуть істотно полегшити умови ведення бізнесу для українських компаній, не поступаючись при цьому високими стандартами захисту персональних даних. Запровадження аналогічних реформ в Україні дасть змогу активізувати економічне зростання, підвищити рівень довіри до цифрових сервісів та поглибити інтеграцію України до Єдиного цифрового ринку ЄС.

Водночас перед Україною стоять важливі завдання, що включають посилення правозастосування, пошук ефективного балансу між потребами національної безпеки та правами громадян на приватність, а також підвищення загального рівня обізнаності населення щодо питань захисту персональних даних. Крім того, українські законодавці повинні зробити пріоритетом розвиток міжнародних партнерств і залучення технічної допомоги для зміцнення інституційної спроможності та впровадження передових технологій, включаючи FHE. Реалізація цих заходів дасть змогу Україні не тільки узгодити своє законодавство зі стандартами GDPR, а й закріпити статус регіонального лідера в галузі цифрових інновацій і захисту персональних даних, створюючи основу для подальшої правової та економічної інтеграції з Європейським Союзом.

## REFERENCES

### Bibliography

*Authored Books*

1. Bradford A, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).

*Edited books*

2. Kuner C, Bygrave L A, Docksey C (eds), *The EU General Data Protection Regulation (GDPR): A commentary* (Oxford University Press 2017).

*Journal articles*

3. Brakerski Z, Gentry C, Vaikuntanathan V, 'Fully Homomorphic Encryption without Bootstrapping' [2014] 6 ACM Transactions on Computation Theory 13.

4. Brkan M, 'Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond' [2019] 27(2) International Journal of Law and Information Technology 91–121.
5. Fan J, Vercauteren F, 'Somewhat Practical Fully Homomorphic Encryption' [2012] IACR Cryptol. ePrint Arch 144 <https://eprint.iacr.org/2012/144> (accessed 14.04.2025).

*Theses*
6. Gentry C, 'A Fully Homomorphic Encryption Scheme' (Doctoral dissertation, Stanford University 2009) <https://crypto.stanford.edu/craig/craig-thesis.pdf> (accessed 14.04.2025).

*Conference papers*
7. Vaikuntanathan V, 'Computing Blindfolded: New Developments in Fully Homomorphic Encryption' *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science* (Palm Springs, 2011) 5–16.

*Websites*
8. Myszne J, '3 Homomorphic Encryption Trends for 2025' (December 19, 2024) <https://www.itprotoday.com/data-privacy/three-homomorphic-encryption-trends-for-2025> (accessed 14.04.2025).
9. Taylor P, 'Amount of data created, consumed, and stored 2010-2023, with forecasts to 2028' (Nov 21, 2024) <https://www.statista.com/statistics/871513/worldwide-data-created> (accessed 14.04.2025).
10. Van Quathem K, 'European Commission Confirms Plans to Simplify GDPR' (March 17, 2025) <https://www.insideprivacy.com/gdpr/european-commission-confirms-plans-to-simplify-gdpr> (accessed 14.04.2025).

Maksym Surzhynskyi

## CHALLENGES AND OPPORTUNITIES FOR ADAPTING UKRAINIAN LEGISLATION TO EUROPEAN STANDARDS OF PERSONAL DATA PROTECTION IN THE FIELD OF AI

Abstract. The research on adapting Ukrainian legislation to European standards of personal data protection in the field of artificial intelligence (AI) is driven by numerous issues stemming from rapid technological advancements, as well as the need to ensure human rights, transparency, and accountability in automated processing of personal data. Particular complexity arises in regulating specific legal relationships associated with the use of artificial intelligence, including profiling, automated decision-making, ethical and non-discriminatory use of algorithms, and ensuring adequate safeguards for data subjects.

The purpose of the article is a comprehensive analysis of European legal acts (GDPR and AI Act), current Ukrainian legislation, and prospective regulatory changes, particularly Draft Law No. 8153 "On Personal Data Protection", aimed at developing an integrated understanding of the challenges and opportunities in harmonizing Ukrainian law with European standards. Additionally, the article seeks to identify directions for further improvements to national legislation capable of ensuring adequate protection of personal data when deploying AI technologies.

It was found that the current norms of Ukrainian law require substantial refinement to effectively accommodate the specifics of AI technologies, especially in matters of algorithmic transparency, protection against automated decisions, and guarantees concerning ethics and non-discrimination. It also identifies the need for supporting small and medium enterprises in adapting to the new requirements imposed by GDPR and AI Act, and resolving complex issues related to cross-border data transfers. The author formulates recommendations for introducing specialized legal instruments (ethical codes, regulatory sandboxes) to ensure a balance between protecting the rights of data subjects and promoting innovation in artificial intelligence.

Keywords: personal data; artificial intelligence; GDPR; AI Act; automated decision-making; algorithmic transparency; AI ethics; FHE; legislative harmonization.