УДК 342.7:004.8
DOI: https://doi.org/10.31359/1993-0909-2025-32-4-30

Андрій Олександрович Гачкевич

Кафедра міжнародного та кримінального права
Інститут права, психології та інноваційної освіти
Національного університету «Львівська політехніка»
Львів, Україна

КЛЮЧОВІ АСПЕКТИ ПРОБЛЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У КОНТЕКСТІ РОЗВИТКУ ШТУЧНОГО ІНТЕЛЕКТУ

Анотація. *Проблема захисту персональних даних набула особливої гостроти внаслідок появи сучасних систем штучного інтелекту як прогресивних технологій, спроможних виконувати завдання, які раніше були підсильними виключно людям. «Логіка» систем штучного інтелекту щодо обробки персональних даних залишається малозрозумілою, а підконтрольність людині процесів, які виконуються такими системами, не може бути забезпеченою в повній мірі. На тлі загальних питань, які визначають стан законодавчого регулювання відносин у сфері персональних даних у правових системах сучасності (обґрунтована підстава для обробки даних, належне інформування суб'єкта даних, дотримання принципу точності, проведення оцінки ризиків, строковість зберігання, обмеження мети обробки і т.ін.), за останні роки почали обговорюватись і спеціальні, зумовлені розвитком штучного інтелекту. Вони сприяють окресленню правових рамок для будь-яких операцій із персональними даними, здійснюваних системами штучного інтелекту. У цій статті узагальнені ключові аспекти проблеми захисту персональних даних під час проєктування, розробки, впровадження та використання систем штучного інтелекту, включаючи забезпечення належної підстави для обробки даних у цілях навчання систем штучного інтелекту, повідомлення необхідної інформації суб'єктам даних стосовно такого навчання, гарантування прав на доступ до даних, їхнє виправлення та видалення, а також втілення позитивних практик оцінки ризиків, людського нагляду та перетворення персональних даних за допомогою анонімізації, псевдонімізації та синтезації даних, значення яких також пояснюється. З точки зору правомірності більш детально охарактеризований процес навчання систем штучного інтелекту. Результати дослідження свідчать про те, що розвиток штучного інтелекту істотно впливає на відносини у сфері персональних даних, адже, по-перше, персональні дані є цінним ресурсом при проєктуванні, розробці та впровадженні систем штучного інтелекту, по-друге, при використанні таких систем персональні дані можуть ставати об'єктом опрацювання.*

Ключові слова: *штучний інтелект та персональні дані; персональні дані; захист персональних даних; штучний інтелект; законодавство про захист персональних даних; підстави для обробки персональних даних; перетворення персональних даних; Загальний регламент про захист даних; ChatGPT.*

Andrii O. Hachkevych
Department of International and Criminal Law
Institute for Law, Psychology, and Innovative Science
Lviv Polytechnic National University
Lviv, Ukraine

KEY ASPECTS OF PERSONAL DATA PROTECTION IN THE CONTEXT OF ARTIFICIAL INTELLIGENCE DEVELOPMENT

Abstract. *The problem of personal data protection has become particularly acute due to the emergence of modern artificial intelligence systems as progressive technologies, which can perform tasks previously only capable of humans. The processes by which artificial intelligence systems handle personal data remain poorly understood, making it difficult for humans to maintain complete control over these systems. General issues that determine the legislative regulation of personal data relationships in contemporary legal systems encompass reasonable grounds for data processing, proper informing of data subjects, compliance with the principle of accuracy, risk assessment procedure, data retention period, purpose limitation, etc. In addition to them, specific issues related to the rise of artificial intelligence have arisen in recent years. All these issues are crucial for enhancing a legal framework governing any operations involving personal data by artificial intelligence systems. This article explores in general the key aspects of personal data protection throughout the design, development, implementation, and usage of artificial intelligence systems. It addresses several widely discussed topics, including the need for reasonable legal grounds for processing data while training artificial intelligence systems, the obligation of informing data subjects about such training, and guaranteeing the rights of data subjects (access, rectification, erasure). The author also discusses data transformation techniques such as anonymization, pseudonymization, and data synthesis by GenAI systems. From the perspective of legitimacy, the training process of artificial intelligence systems is described in greater detail. The results of the study indicate that the rise of artificial intelligence significantly impacts personal data relationships. First, personal data serves as a valuable resource in the design, development and implementation of artificial intelligence systems. Secondly, in using such systems, personal data can become subject to various forms of processing.*

Keywords: *artificial intelligence and personal data; personal data; personal data protection; artificial intelligence; personal data protection legislation; grounds for processing personal data; personal data transformation; General Data Protection Regulation; ChatGPT.*

ВСТУП

Розвиток штучного інтелекту як виду технологій, спроможних виконувати раніше підсильні виключно людям завдання, є причиною докорінних змін у житті суспільства. Вплив систем штучного інтелекту на суспільні відносини перебуває в тісному взаємозв'язку з правом. З одного боку, право виконує функцію регулювання – зокрема щодо створення та використання технологій, – воно вносить більше порядку до технологічного прогресу. З іншого боку, поява та поширення

нових технологій, насамперед штучного інтелекту як найбільш передової, призводить до еволюції права, тим самим підкреслюючи його динамічний характер.

З урахуванням взаємозв'язку такого роду, набуває особливої гостроти проблема захисту персональних даних, на якій зосереджений наш фокус уваги. В історичному ракурсі традиції правової охорони персональних даних сягають 1970-х років – задовго до епохи штучного інтелекту, – коли у США, Німеччині, Франції та інших державах були прийняті найперші закони такого плану. Апогеєм майже півстолітнього розвитку концепції захисту персональних даних стало прийняття Загального регламенту про захист даних у 2016 році (далі – GDPR).

З появою технологій штучного інтелекту, насамперед генеративних на початку 2020-х, виявилось, що правові формули для забезпечення ефективної охорони персональних даних при проєктуванні, розробці, впровадженні та використанні систем штучного інтелекту подекуди стають радше нездійсненними ідеалами, ніж втіленими на практиці стандартами.

Виходячи з цього, у контексті розвитку штучного інтелекту гостроти набула проблема захисту персональних даних, вона відзначається багатоаспектністю та дозволяє краще зрозуміти взаємовплив сучасних технологій та права.

1. ОГЛЯД ЛІТЕРАТУРИ

Те, що проблема захисту персональних даних стала більш вираженою внаслідок появи сучасних систем штучного інтелекту, підтверджує серед іншого великий інтерес до неї з боку українських учених, таких як: Арзянцева Д., Базалицький В., Бондаренко О., Гачкевич А., Деркаченко Ю., Дорош В., Дубняк М., Думчиков М., Заярний О., Карапетян О., Колесніков А., Косілова О., Машталяр О., Некрутенко В., Пунда О., Солодовнікова Х. та ін.

Зауважимо, що тематика проведених досліджень перебуває в тісному зв'язку з достатньо дискусійною правовою категорією приватності, а також підкреслює фундаментальну роль GDPR у забезпеченні ефективної охорони персональних даних.

Гиляка О. здійснює глибокий теоретико-правовий аналіз права на приватність та відзначає серед передумов належного захисту персональних даних цифрові технології безпеки (ідентифікацію, авторизацію користувачів, аутентифікацію протоколів, шифрування і контроль доступу), а також – дотримання правил і методик безпечного використання цифрових технологій. Він називає захист персональних даних однією з найбільш суттєвих проблем цифрової епохи [1].

Ще одна публікація автора – разом з Мерник А. – описує технологічні виклики для права на приватність, зокрема відстеження персональних даних, збільшення їхньої кількості в Інтернеті та появу нових форм стеження за людьми. Стаття порушує три важливі питання епохи штучного інтелекту: 1) якими є особливості реалізації та забезпечення права на приватність і конфіденційність; 2) як захищати персональні дані у цифровому суспільстві; 3) що таке «право бути забутим» [2].

Гудзь Л. вивчає потенційні загрози для права на приватність, які виникають у контексті використання штучного інтелекту, та пропонує шляхи їхнього подолання через удосконалення положень Закону України «Про захист персональних даних», зокрема забезпечуючи визначеність понять штучного інтелекту та приватності персональних даних, встановлюючи вимоги щодо прозорості та підзвітності алгоритмів штучного інтелекту, вводячи обов'язкове надання інформованої згоди та механізми її відкликання, посилюючи гарантії прав громадян на корекцію й видалення даних, запроваджуючи орган нагляду тощо [3].

У розширенні сфери застосування штучного інтелекту Кронівець Т. і Тимошенко Є. вбачають загрози для тієї інформації, яка повинна залишатися конфіденційною, через її можливий незаконний збір, обробку та розповсюдження. Вони підкреслюють, що дані є дуже чутливими до сучасних технологій – використання алгоритмів пошуку, механізмів рекомендацій і демонстрації реклами [4].

Для розуміння проблеми захисту персональних даних дуже цінними вважаємо результати дослідження, проведеного Берназюк І. стосовно аналізу положень Європейської конвенції з прав людини та практики її застосування в контексті розвитку штучного інтелекту [5]. Серед виявлених недоліків – відсутність спеціальних норм щодо штучного інтелекту, а тому – Конвенція повинна тлумачитись розширено, недостатній рівень прозорості та підзвітності алгоритмів штучного інтелекту, а також недостатній контроль за їхнім застосуванням у публічному секторі.

Остіян Є. цілком слушно підкреслює, що використання штучного інтелекту може підпадати під декілька правових режимів. Для того, щоб персональні дані були захищеними, його впровадження вимагає гнучкого підходу та відповідної адаптації вже прийнятих норм. Крім того, авторка згадує про наявність двох часто суперечливих тенденцій – прогресу технологій та дотримання прав людини [6].

Бєлова М. і Бєлов Д. досліджують виклики та загрози, характерні для відносин у сфері захисту персональних даних, що виникають при роботі зі штучним інтелектом. Автори аналізують такі проблеми, як нестабільність технологічного прогресу; забезпечення конфіденційності та цілісності даних при їхній обробці; ідентифікації та управління ризиками; алгоритмічної упередженості; недостатньої анонімізації даних [7].

В іноземній правовій науці вищезгадана багатоаспектність проявляється ще яскравіше, а також швидко зростає кількість виданих праць, присвячених порушеній проблемі.

З-поміж досліджень, результати яких оприлюднені останнім часом, можемо назвати книгу з промовистою назвою «Захист даних: наслідки розвитку штучного інтелекту та машинного навчання» [8]. Вона містить комплексний аналіз викликів, можливостей та рішень, пов'язаних із захистом даних в епоху штучного інтелекту та машинного навчання. Одним із лейтмотивів цієї книги є те, що посилений контроль за дотриманням правил захисту даних є необхідним, та, крім

технічних рішень, слід ураховувати етичні, законодавчі та суспільні фактори. Автори розглядають такі питання, як профілювання та конфіденційність; довіра та надійність з огляду на популярність ChatGPT та інших схожих сервісів; захист даних та розвиток робототехніки; розумні міста та безпека даних тощо.

Девітте П. досліджує роль GDPR в умовах, коли системи штучного інтелекту та масштабна обробка персональних даних ставлять під загрозу основні права та свободи людини. Він зауважує, що між функціонуванням систем штучного інтелекту – свого роду «чорних скриньок» – та загальними принципами захисту персональних даних, викладеними в статті 5 GDPR (законність, прозорість, обмеження мети, мінімізація даних та підзвітність) існує певна неузгодженість [9].

У книзі «Приватність, захист даних та технології, що базуються на даних» крізь призму розвитку штучного інтелекту підняті серед інших теми біобанкінгу як процесу збору та зберігання зразків біологічних матеріалів пацієнтів, M2M-взаємодії, тобто взаємодії між машинами, в рамках якої відбувається обмін даних без втручання людини, дотримання GDPR при навчанні систем штучного інтелекту, а також блокчейну, технологій для правової сфери та персоналізованої реклами [10].

Окремі питання взаємозв'язку розробки, впровадження та використання систем штучного інтелекту та захисту персональних даних розглянуті в книзі, виданій за підсумками проведення авторитетної конференції CPDP (Computers, Privacy and Data Protection – «Комп'ютери, приватність та захист даних») у 2024 р. під гаслом «Питання полягає в тому – чи керувати, чи бути керованим», наприклад, взаємовідношення технологій для розпізнавання обличчя, прав людини та Закону ЄС про штучний інтелект, а також – використання штучного інтелекту для вдосконалення умов праці з позиції забезпечення приватності [11].

Пощер Р. пояснює, чому традиційні уявлення про захист даних складно адаптувати до сучасних систем штучного інтелекту, – останні не забезпечують прозорості при обробці даних. Водночас він пропонує акцентувати увагу на тому, щоб насамперед були реалізовані такі фундаментальні правові цінності, як свобода та рівність [12].

Фабіано Н. робить спробу дослідити взаємозв'язок між робототехнікою, штучним інтелектом, машинним навчанням, захистом даних і конфіденційністю, відводячи важливу роль явищу великих даних, а також правилам етики [13].

2. МАТЕРІАЛИ ТА МЕТОДИ

Штучний інтелект на сучасному етапі по праву став найбільш обговорюваним у наукових колах та ймовірно одним із найчастіше застосовуваним видом технологій. Разом із тим, крім характерних для всіх технологій рис, системи штучного інтелекту мають низку особливостей, що впливають на процеси обробки ними персональних даних.

На тлі загальних питань, які визначають стан законодавчого регулювання відносин у сфері персональних даних у правових системах сучасності (обґрунтова-

на підстава для обробки даних, належне інформування суб'єкта даних, дотримання принципу точності, проведення оцінки ризиків, перетворення персональних даних за допомогою анонімізації, псевдонімізації та синтезації даних), за останні роки почали обговорюватися й спеціальні, які зумовлені розвитком штучного інтелекту та сприяють окресленню правових рамок для будь-яких операцій із персональними даними, здійснюваних системами штучного інтелекту.

Для того, щоб пояснити, чому розвиток штучного інтелекту в цілому кидає виклик захисту персональних даних, у першу чергу ми розглянемо шляхом аналізу окремі особливості систем штучного інтелекту. Наступним завданням є охарактеризування процесу навчання систем штучного інтелекту з точки зору правомірності, адже часто його наслідки у сфері захисту персональних даних применшуються. Важливою частиною статті є дослідження позитивних практик для того, щоб унеможливити порушення у сфері захисту персональних даних.

Ми також зробимо спробу методом узагальнення показати, в чому полягає проблема захисту персональних у контексті розвитку штучного інтелекту, систематизуючи її ключові аспекти.

Нормативно-правовою основою для проведеного дослідження є GDPR як один із найважливіших документів сучасності (а можливо – найважливіший), присвячених порушеній проблемі. Поряд із Конвенцією Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних, GDPR займає важливу роль у процесах удосконалення стану законодавчого регулювання відносин у сфері персональних даних в українській правовій системі.

3. РЕЗУЛЬТАТИ ТА ОБГОВОРЕННЯ

Оскільки за останні роки штучний інтелект став невід'ємною частиною технологій та став широко застосовуваним у різних сферах діяльності як органами державної влади та місцевого самоврядування, так і приватними компаніями, порушену в цій статті проблему доцільно розглядати як загальнотехнологічну, тобто – як захищати персональні дані, коли вони стають або можуть стати об'єктом впливу сучасних технологій.

Водночас системи штучного інтелекту як різновид технологій, природа яких описана в об'єктивній (результати виконання конкретних завдань) та/або суб'єктивній формах (імітація когнітивних здібностей людини) [14, с. 40], володіють певними особливостями, що відображаються й на процесах обробки персональних даних. На нашу думку, такими особливостями є:

– навчання систем штучного інтелекту виконувати поставлені завдання відбувається на основі опрацювання ними величезних обсягів інформації, включаючи персональні дані;

– штучний інтелект «поглинає» загальнодоступну в мережі Інтернет інформацію, в тому числі з соціальних медіа, яка часто містить персональні дані (наприклад, відкриті для загалу відомості зареєстрованого користувача LinkedIn);

– подальша доля будь-якої введеної (пошуковий запит в Google) або завантаженої користувачами Інтернету інформації (додане зображення для обробки графічним редактором) є невідомою, швидше за все така інформація «зберігається в пам'яті»;

– у деяких випадках збір даних для обробки з використанням штучного інтелекту відбувається непомітно (відомості про діяльність користувача соціального медіа, дані відеоспостереження, записи діалогів із розмовними чат-ботами);

– зумовленість відповідей на питання користувачів, коли йдеться про сервіси типу ChatGPT, не стільки фактами як інформацією про події та явища, що відбувалися насправді, а згенерованим штучним інтелектом найбільш імовірним згідно з «логікою» системи штучного інтелекту поєднанням слів у речення.

Показовим прикладом останньої з наведених особливостей є випадок, що викликав резонанс після того, як у березні 2025 року норвезький національний орган із захисту даних (Datatilsynet) отримав на розгляд скаргу від користувача ChatGPT. Він запитав у ChatGPT: «Хто такий Арве Ялмар Холмен?», а у відповіді, яку отримав, було вказано, що Арве Ялмар Холмен – це норвежець, сумнозвісно відомий через те, що його засудили до максимального покарання за вбивство двох синів та виконання замаху на вбивство третього. При цьому скаржником став сам Холмен (разом із громадською організацією «Європейський центр цифрових прав»), який проживав у норвезькому місті Тронгейм та справді мав трьох синів. Він не був публічною особою та ніколи не притягався до кримінальної відповідальності [15].

Архітектура законодавчого регулювання відносин у сфері захисту персональних даних розроблена на співставленні інтересів суб'єктів даних, тобто фізичних осіб, персональні дані яких підлягають обробці, а також контролерів (розпорядників) та операторів, тобто тих, хто визначає цілі та способи обробки персональних даних суб'єктів даних, та тих, хто здійснює обробку.

Крім того, держава забезпечує нагляд за тим, наскільки дотримані національні стандарти щодо захисту персональних даних, – наглядова діяльність державних органів із захисту даних згідно з GDPR проявляється у трьох ролях: слідчого, судді та експерта [16, с. 157–158].

Як ми вже згадували, критерії оцінювання правомірності будь-яких операцій із персональними даними почали формуватись у 1970-х роках, і досягли свого апогею в середині 2010-х, коли був прийнятий GDPR як стандарти, що діють далеко за межами ЄС.

Зважаючи на вищезгадані види суб'єктів відносин у сфері захисту персональних даних, фактор штучного інтелекту найчастіше проявляється в тому, що обробка персональних даних здійснюється із застосуванням систем штучного інтелекту, як-от у ще одному резонансному випадку, коли приватна компанія Amazon нібито користувалась програмою на основі штучного інтелекту для того, щоб аналізувати подані резюме та визначати найбільш підходящі в цілях працевла-

штування кандидатури [17]. Як виявилось, результати автоматизованого відбору були упередженими за статевою ознакою.

Достатньо суперечливим стало й упровадження пілотного проєкту iBorderCtrl наприкінці 2010-х – ідеї розумного кордону ЄС – коли штучний інтелект мав би перевіряти осіб, які не мають громадянства держав-учасниць ЄС, при перетині кордонів ЄС [18]. В основу перевірки покладено експериментальний детектор брехні, здатний за виразом обличчя розпізнавати правду. Для того, щоб провести автоматизовану перевірку особи, система попередньо опрацьовувала дані про цю особу, зокрема її активність у соціальних медіа, біометричну інформацію, документи для перетину кордону тощо.

Подібно до інших сучасних технологій, штучний інтелект базується на даних. Саме дані є тим навчальним матеріалом для систем штучного інтелекту, від якого залежать їхні результати та продуктивність.

Відповідно одним із ключових аспектів проблеми захисту персональних даних є розуміння правових рамок обробки персональних даних у цілях навчання систем штучного інтелекту.

Навчання систем штучного інтелекту можуть помилково сприймати як нешкідливий для суб'єкта даних та безпечний для самих персональних даних процес.

По-перше, дані опрацьовують «чорні скриньки» без доступу третіх осіб. По-друге, не формуються записи з персональними даними та не створюються відповідні бази даних. По-третє, сама обробка проходить «в оперативній пам'яті».

Однак усі ці аргументи в жодному разі не легітимізують можливість вільно використовувати персональні дані для навчання систем штучного інтелекту, пов'язаного з етапом їхньої розробки (хоча самі системи можуть бути запрограмованими на навчання та вдосконалення й після розробки та впровадження). Для будь-якого використання – від збору до розкриття – має бути надана згода суб'єкта даних або наявна будь-яка інша належна підстава. Таким чином, використання для навчання підпадає під категорію обробки, а тому повинно здійснюватися відповідно до встановлених принципів, з забезпеченням прав суб'єктів даних.

Зауважимо, що визначені в GDPR підстави включають згоду – вільне, усвідомлене та недвозначне волевиявлення, але не обмежуються нею. Згода надається суб'єктом даних у тому випадку, якщо він погоджується на те, що діалог із розмовним чат-ботом буде використаним для навчання систем штучного інтелекту. Водночас при отриманні згоди необхідно вказати певний вид обробки, її цілі, а також – конкретизувати, про які персональні дані йде мова. Крім згоди, використання даних для навчання може бути обґрунтованим законним інтересом, який полягає в тому, що контролер зацікавлений в обробці даних для того, щоб здійснювати свою діяльність. Така обробка не повинна завдавати шкоди інтересам суб'єктів даних.

Право бути поінформованими про обробку персональних даних гарантоване суб'єктам даних відповідно до GDPR та є одним із найважливіших їхніх прав. Водночас для його забезпечення слід надати відомості щодо того, які саме дані

будуть використані, як вони будуть оброблятися під час навчання, скільки часу такі дані будуть зберігатись. Безумовно, інформація такого роду повинна бути вказана в політиках конфіденційності соціальних медіа та умовах використання програмного забезпечення. На жаль, змістовне ознайомлення з ними відбувається дуже рідко, натомість користувачі дають згоду автоматично, прагнучи якнайшвидше отримати нові можливості. Виходячи з цього та інших факторів, які негативно впливають на формування обізнаності суспільства з явищем захисту персональних даних у контексті розвитку штучного інтелекту, національні органи із захисту даних своїми рішеннями можуть зобов'язувати контролерів даних, які порушили прийняті правила, проводити інформаційні кампанії про процеси обробки даних та права суб'єктів даних [16, с. 158].

При впровадженні систем штучного інтелекту виникає необхідність інтегрувати їх у діяльність органів державної влади та місцевого самоврядування, а також приватних компаній. При цьому особливої уваги потребують наступні питання:

– налагодження сумісності штучного інтелекту з уже впровадженими технологіями та системами;

– отримання гарантій від інших організацій, з якими в той чи інший спосіб відбувається взаємодія щодо забезпечення конфіденційності;

– виявлення й усунення вразливостей технологій та систем, використовуваних для діяльності.

Поза всяким сумнівом, упровадження систем штучного інтелекту інтенсифікує небезпеку витоку даних, як і призводить до додаткових загроз для їхньої цілісності. Водночас сучасні штучно-інтелектуальні розробки дозволяють у режимі реального часу здійснювати моніторинг стану кіберзахищеності та реагувати на можливі несанкціоновані втручання.

При використанні систем штучного інтелекту персональні дані як самого користувача (повідомлені в процесі розмови з ChatGPT), так й інших осіб (наприклад, для автоматизованого прийняття рішення про кредитоспроможність особи на користь банку за відсутності належної підстави) можуть бути введеними або завантаженими для подальшої обробки.

Такий спосіб набуття персональних даних не є єдиним. Варто згадати в цьому контексті і про веб-скрейпинг як про видобування величезних обсягів загальнодоступних даних першочергово з вебсайтів.

Персональні дані також можуть ставати об'єктом нелегальної торгівлі або передаватися недобросовісними контролерами даних після незаконного збору.

Варто зауважити, що з формуванням високої правової культури у сфері захисту персональних даних перелічені негативні практики будуть зустрічатися все рідше й рідше, особливо на тлі посилення кримінальної відповідальності за порушення у сфері захисту персональних даних.

Серед інших ключових аспектів досліджуваної проблеми – перешкоди для забезпечення дотримання прав суб'єктів даних на доступ до даних, на виправлення та видалення даних, а також – труднощі реалізації принципу точності.

Коли будь-які дані стали доступними для опрацювання системою штучного інтелекту, такі дані практично не підлягають відокремленню від системи штучного інтелекту. За таких обставин відсутня можливість точково впливати на персональні дані, видаляти їх або навіть виправляти. Не менш проблематичною є реалізація принципу точності, що підтверджує відповідь на питання: «Хто такий Арве Ялмар Холмен?».

Разом з тим, ми вважаємо, стандарти захисту персональних даних дають поштовх на сучасному етапі шукати нові технічні рішення для застосування штучного інтелекту, щоб не допускати ситуацій, коли малозрозуміла «логіка» систем штучного інтелекту унеможливлює в будь-який момент часу ідентифікування будь-яких персональних даних або сприяння впровадженню позитивних практик, про які піде мова далі.

Ідея оцінювати ймовірні ризики, реалізація якої дозволяє зменшити рівень потенційної небезпеки, знайшла своє втілення і в сфері захисту персональних даних, і по відношенню до штучного інтелекту. Квінтесенцією цієї ідеї є те, що в процесі збору, опрацювання та розкриття персональних даних, а також застосування систем штучного інтелекту можуть виникати фактори, які несуть загрозу для прав та свобод людини. Якщо така загроза відповідно до обґрунтованих очікувань призведе до заподіяння істотної шкоди, то потрібно вжити всіх необхідних заходів для мінімізації ризиків, а в деяких випадках – взагалі відмовитися від небезпечної діяльності (неприйнятний рівень ризику згідно з Законом ЄС про штучний інтелект).

Положення ст. 35 GDPR зобов'язують контролерів даних проводити оцінку впливу на захист даних у випадку приналежності типу обробки персональних даних до таких, що несуть високий ризик для прав та свобод фізичної особи.

Зауважимо, що високий ризик у контексті цієї статті пов'язаний із конкретними випадками, переліченими у п. 3, що включають профілювання, тобто охарактеризоване раніше формування свого роду портрету особи (як правило – користувача соціального медіа) на основі аналізу даних, що включають інформацію, надану при реєстрації.

Ще одна ідея – людського нагляду – бере свій початок від визнання того, що техніка може помилятись та завдавати шкоди суб'єктам даних, а отже людина повинна залишати за собою можливість наглядати, тобто «пильнувати, слідкувати за ким-, чим-небудь для контролю, забезпечення порядку і т. ін.» [19]) за процесами.

Чи можна перетворити оригінальні персональні дані в інші формати, щоб обробка відповідної інформації була законною, незважаючи на наявність належної підстави та дотримання принципів обробки?

Ствердна відповідь на це питання пов'язана з позитивними практиками анонімізації, псевдонімізації та синтезації даних, завдяки яким дані перестають бути такими, що стосуються ідентифікованої або придатної до ідентифікування особи.

Зауважимо, що внаслідок анонімізації втрачається зв'язок між даною інформацією та конкретною особою, наприклад, шляхом видалення прізвища особи. При псевдонімізації відбувається заміна прізвища псевдонімом, водночас додаткова інформація – щодо заміни – дозволяє такі дані депсевдонімізувати. Синтезація даних пов'язана з генеруванням контенту, коли системи штучного інтелекту шифрують персональні дані в такий спосіб, щоб при подальшій обробці інформація була повністю деперсоналізованою.

ВИСНОВКИ

Проблема захисту персональних даних полягає в тому, що збір, опрацювання та розкриття інформації, яка прямо чи опосередковано стосується конкретної фізичної особи, часто відбувається незаконно, а сама інформація не є охоронюваною належним чином.

З розвитком технологій, які базуються на даних, насамперед штучного інтелекту, спроможного виконувати завдання, які раніше були підсильними виключно людям, ця проблема пронизує відносини, що виникають у різних сферах, починаючи від медичної й аж до охорони громадського порядку.

Узагальнюючи ключові аспекти проблеми захисту персональних даних у контексті розвитку штучного інтелекту, варто відзначити, що показані в статті особливості систем штучного інтелекту зумовлюють появу цілої низки спеціальних питань для вирішення, які умовно можна об'єднати за такими критеріями:

– етапи життєвого циклу штучного інтелекту (проєктування, розробка, впровадження, використання);

– процеси обробки персональних даних із використанням штучного інтелекту (веб-скрейпинг, профілювання, генерування контенту тощо);

– удосконалення комплексу заходів із захисту персональних даних – правових, організаційних і технічних, що включають анонімізацію, псевдонімізацію та синтезацію даних.

Варто зауважити, що ідея синтезації даних демонструє високий потенціал систем штучного інтелекту для того, щоб забезпечувати законність операцій із персональними даними. Вона демонструє те, що сучасні технології можуть сприяти й більш ефективному захисту персональних даних.

Так саме те, що штучний інтелект – це не тільки загрози й виклики для приватності, а нові можливості, підтверджує його здатність здійснювати моніторинг стану кіберзахищеності та реагувати на можливі несанкціоновані втручання.

Результати дослідження свідчать про те, що розвиток штучного інтелекту істотно впливає на відносини у сфері персональних даних, адже, по-перше, персональні дані є цінним ресурсом при розробці та впровадженні систем штучного інтелекту, по-друге, при використанні таких систем персональні дані можуть ставати об'єктом опрацювання.

Вважаємо, що визначені законодавчо загальні правила GDPR, на які повинен орієнтуватися й український законодавець, сформували надійний каркас для забезпечення захисту персональних даних на етапі розвитку штучного інтелекту.

Тенденції подальших досліджень визначають особливості застосування GDPR щодо обробки персональних даних системами штучного інтелекту, а також пошук нових правових, організаційних і технічних шляхів для того, щоб така обробка відбувалася законно.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Гиляка О. С. Право на приватність та захист персональних даних в умовах цифровізації. *Вісник Національної академії правових наук України.* 2023. Том 30. № 1. С. 15–30.

[2] Гиляка О. С., Мерник А. М. Деякі питання реалізації права на приватність та конфіденційність в умовах сучасних цифрових технологій. *Вісник Національної академії правових наук України.* 2023. Том 30. № 3. С. 156–172.

[3] Гудзь Л. В. Забезпечення права на приватність у контексті використання штучного інтелекту: потенційні загрози та шляхи їх подолання. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Вип. 86. Ч. 1. С. 175–180.

[4] Кронівець Т. М., Тимошенко Є. А. Правові аспекти захисту приватності життя людини в контексті використання штучного інтелекту. *Юридичний науковий електронний журнал.* 2022. № 12. С. 295–297.

[5] Берназюк І. М. Штучний інтелект і права людини: виклики для Європейської конвенції з прав людини. *Аналітично-порівняльне правознавство.* 2025. Вип. 3. Ч. 1. С. 89–99.

[6] Остіян Є. З. Штучний інтелект та персональні дані: захист приватності в цифровому середовищі. *Науковий вісник Ужгородського університету. Серія: Право.* 2024. Вип. 85. Ч. 3. С. 47–53.

[7] Бєлова М. В., Бєлов Д. М. Виклики та загрози захисту персональних даних у роботі зі штучним інтелектом. 2023. *Науковий вісник Ужгородського університету. Серія: Право.* Вип. 79. Т. 2. С. 17–22.

[8] Hewage C., Yasakethu L., Jayakody D. N. K. Data Protection: The Wake of AI and Machine Learning. Cham : Springer Nature, 2025. 308 p.

[9] Dewitte P. AI Meets the GDPR: Navigating the Impact of Data Protection on AI Systems. Smuha N. (Ed.). *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*. Cambridge : Cambridge University Press, 2025. P. 133–157.

[10] Ebers M., Sein K. (Eds.). Privacy, Data Protection and Data-driven Technologies. London : Routledge, 2024. 430 p.

[11] Kosta E., Hallinan D., de Hert P., Nusselder S. (Eds.). Data protection, privacy and artificial intelligence: To govern or to be governed, that is the question. *Computers, Privacy and Data Protection*. Vol. 17. Oxford : Hart Publishing, 2025. 328 p.

[12] Poscher R. Artificial Intelligence and the Right to Data Protection / Voeneky S., Kellmeyer P., Mueller O., Burgard W. (Eds.). *The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives.* Cambridge: Cambridge University Press, 2022. P. 281–289.

[13] Fabiano N. Robotics, Big Data, Ethics and Data Protection: A Matter of Approach. Aldinhas Ferreira M., Silva Sequeira J., Singh Virk G., Tokhi M., Kadar E. (Eds.). *Robotics and Well-Being. Intelligent Systems, Control and Automation: Science and Engineering.* Vol. 95. Cham : Springer, 2019. P. 79–87.

[14] Гачкевич А. О. До питання правової визначеності поняття штучного інтелекту. *Вісник Національної академії правових наук України.* 2025. №1. С. 27–46.
[15] Complaint regarding the processing of personal data that results in inaccurate outputs including them by the controller, violating Article 5(1)(d) GDPR by Arve Hjalmar Holmen represented by noyb. URL: https://noyb.eu/sites/default/files/2025–03/OpenAI_complaint_redacted.pdf (дата звернення: 20.07.2025).
[16] Гачкевич А. О. Нагляд національних органів ЄС із захисту даних за обробкою персональних даних системами штучного інтелекту (на прикладі ChatGPT). *Аналітично-порівняльне правознавство*. 2025. Вип. №4. Ч. 2. С. 154–160.
[17] Dastin J. Insight – Amazon scraps secret AI recruiting tool that showed bias against women. 2018. URL: https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/ (дата звернення: 20.07.2025).
[18] Chelioudakis E. Greece: Clarifications sought on human rights impacts of iBorderCtrl. URL: https://edri.org/our-work/greece-clarifications-sought-on-human-rights-impacts-of-iborderctrl/ (дата звернення: 20.07.2025).
[19] Наглядати. URL: https://slovnyk.ua/index.php?swrd=наглядати (дата звернення: 20.07.2025).

REFERENCES

[1] Hyliaka, O. (2023). Right to privacy and protection personal data in digitalization conditions. *Journal of the National Academy of Legal Sciences of Ukraine,* 30(1), 15–30.
[2] Hyliaka, O., & Mernyk, A. (2023). Some issues of implementation of the right to privacy and confidentiality in the conditions of modern digital technologies. *Journal of the National Academy of Legal Sciences of Ukraine,* 30(3), 156–172.
[3] Gudz, L. (2024). Ensuring the right to privacy in the context of artificial intelligence: potential threats and ways to overcome them. *Uzhhorod National University Herald. Series: Law,* 86(1), 175–180.
[4] Kronivets, T., & Tymoshenko, Y. (2022). Legal aspects of human privacy protection in the context of the use of artificial intelligence. *Juridical scientific and electronic journal,* 12, 295–297.
[5] Bernaziuk, I. (2025). Artificial Intelligence and Human Rights: Challenges for the European Convention on Human Rights. *Analytical and Comparative Jurisprudence,* 3, 89–99.
[6] Ostiian, Y. (2024). Artificial intelligence and personal data: privacy protection in the digital environment. *Uzhhorod National University Herald. Series: Law*, 85(3), 175–180.
[7] Bielova, M., & Bielov, D. (2023). Challenges and threats of personal data protection in working with artificial intelligence. *Uzhhorod National University Herald. Series: Law,* 79(2), 17–29.
[8] Hewage, C., Yasakethu, L., Jayakody, D. N. K. (2025). *Data Protection: The Wake of AI and Machine Learning.* Springer Nature.
[9] Dewitte, P. (2025). AI Meets the GDPR: Navigating the Impact of Data Protection on AI Systems. In N. A. Smuha (Ed.), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (pp. 133–157). Cambridge University Press.
[10] Ebers, M., & Sein, K. (Eds.). (2024). *Privacy, Data Protection and Data-driven Technologies.* Routledge.

[11] Kosta, E., Hallinan, D., de Hert, P., & Nusselder, S. (Eds.) (2025). *Data protection, privacy and artificial intelligence: To govern or to be governed, that is the question* (Vol. 17. Computers, Privacy and Data Protection). Hart Publishing.
[12] Poscher, R. (2022). Artificial Intelligence and the Right to Data Protection. In S. Voeneky, P. Kellmeyer, O. Mueller, & W. Burgard (Eds.), *The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives* (pp. 281–289). Cambridge: Cambridge University Press.
[13] Fabiano, N. (2019). Robotics, Big Data, Ethics and Data Protection: A Matter of Approach. In: Aldinhas Ferreira, M., Silva Sequeira, J., Singh Virk, G., Tokhi, M., E. Kadar, E. (Eds.), *Robotics and Well-Being. Intelligent Systems, Control and Automation: Science and Engineering* (pp. 79–87). Springer.
[14] Hachkevych, A. (2025). Revisiting the issue of legal determination of the concept of artificial intelligence. *Journal of the National Academy of Legal Sciences of Ukraine,* 32(1), 27–46.
[15] European Center for Dgitial Rights. (2025). *Complaint regarding the processing of personal data that results in inaccurate outputs including them by the controller, violating Article 5(1) (d) GDPR.* Retrieved from https://noyb.eu/sites/default/files/2025–03/OpenAI_complaint_redacted.pdf
[16] Hachkevych, A. (2025). The Supervision of EU National Data Protection Authorities over personal data processing by AI Systems (The case of ChatGPT). *Analytical and Comparative Jurisprudence,* 4, 154–160.
[17] Dastin, J. (2018). *Insight – Amazon scraps secret AI recruiting tool that showed bias against women.* Reuters. Retrieved from https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/
[18] Chelioudakis, E. (2018, November 21). *Greece: Clarifications sought on human rights impacts of iBorderCtrl.* European Digital Rights. Retrieved from https://edri.org/our-work/greece-clarifications-sought-on-human-rights-impacts-of-iborderctrl/
[19] Dmytriiev, O. (n.d.). *SURVEIL – interpretation, spelling, new spelling online.* Retrieved from https://slovnyk.ua/index.php?swrd=наглядати

Андрій Олександрович Гачкевич
Кандидат юридичних наук, доцент
Доцент кафедри міжнародного та кримінального права
Інститут права, психології та інноваційної освіти
Національного університету «Львівська політехніка»
79000, вул. Князя Романа, 1/3, Львів, Україна

Andrii O. Hachkevych
PhD in Law, Associate Professor
Associate Professor of the Department of International and Criminal Law
Institute for Law, Psychology, and Innovative Science
Lviv Polytechnic National University
79000, 1/3 Kniazia Romana St., Lviv, Ukraine

Рекомендоване цитування: Гачкевич А. О. Ключові аспекти проблеми захисту персональних даних у контексті розвитку штучного інтелекту. *Вісник Національної академії правових наук України*. 2025. Т. 32(4). С. 30–44.

Suggested Citation: Hachkevych, A. O. (2025). Key Aspects of Personal Data Protection in the Context of Artificial Intelligence Development. *Journal of the National Academy of Legal Sciences of Ukraine*, 32(4), 30–44.

Стаття надійшла / Submitted: 15/09/2025
Доопрацьовано / Revised: 15/10/2025
Схвалено до друку / Accepted: 18/12/2025