МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

Кваліфікаційна наукова
праця на правах рукопису

МАШТАЛЯР ОЛЕКСАНДР МИХАЙЛОВИЧ

УДК 34:342.951:004.6-027.552:004.8

ДИСЕРТАЦІЯ
ПРАВОВА ОХОРОНА І ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ШТУЧНОГО ІНТЕЛЕКТУ

08 – Право
081 – Право

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____ **О. М. Машталяр**

Науковий керівник: **Хахановський Валерій Георгійович,**
доктор юридичних наук, професор

Київ–2026

АНОТАЦІЯ

Машталяр О. М. Правова охорона і захист персональних даних у сфері штучного інтелекту. – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття ступеня доктора філософії за спеціальністю 081 «Право». – Національна академія внутрішніх справ, Київ, 2026.

Дисертація присвячена дослідженню теоретико-правових, методологічних і практичних засад правової охорони та захисту персональних даних у сфері застосування технологій штучного інтелекту.

Доведено, що стрімке впровадження систем штучного інтелекту в публічне управління, економіку, сферу безпеки та цифрові сервіси супроводжується формуванням нових ризиків для прав і свобод людини, пов’язаних з автоматизованим прийняттям рішень, профілюванням, масовим збором інформації та створенням інференційних висновків.

Обґрунтовано, що традиційні механізми правового регулювання персональних даних не забезпечують належного рівня захисту в умовах алгоритмічних технологій і потребують системної адаптації. Традиційна модель захисту персональних даних була сформована для порівняно простих інформаційних систем, де обробка даних мала фіксований характер, а суб’єкт міг усвідомлено надати згоду на конкретну мету. В умовах штучного інтелекту ця логіка не працює: алгоритмічні системи здатні формувати інференційні висновки, яких не було на момент збору даних, приймати рішення без участі людини, повторно ідентифікувати знеособлених осіб і використовувати дані для завдань, не передбачуваних на початковому етапі. Принципи мінімізації даних і цільового обмеження вступають у системну суперечність з логікою машинного навчання, яке потребує максимально широких масивів інформації. Чинне законодавство не містить спеціальних гарантій щодо автоматизованих рішень, інференційних даних, алгоритмічної

відповідальності та біометричної ідентифікації, що утворює прогалини, які неможливо усунути в межах наявної моделі регулювання.

Встановлено, що традиційні механізми правового регулювання персональних даних не забезпечують належного рівня захисту в умовах використання алгоритмічних технологій та потребують адаптації до сучасних цифрових процесів.

У дисертації обґрунтовано необхідність формування ризик-орієнтованої моделі правового регулювання у сфері штучного інтелекту, орієнтованої на запобігання шкоді правам людини та забезпечення прозорості алгоритмічної обробки даних. Встановлено, що правове значення у сфері штучного інтелекту мають не лише окремі операції з персональними даними, а й архітектура алгоритмічних систем, особливості їх навчання, функціонування та соціальні наслідки використання.

Досліджено сучасні підходи до розуміння персональних даних у контексті розвитку технологій Big Data й штучного інтелекту. Доведено, що алгоритмічні системи здатні формувати похідні й інференційні дані, які можуть впливати на правовий статус особи, її можливості та реалізацію основоположних прав. З’ясовано, що інференційні дані потребують виокремлення як самостійного об’єкта правової охорони та спеціального режиму захисту.

У роботі встановлено особливості реалізації принципів privacy by design і privacy by default у системах штучного інтелекту. Систематизовано міжнародні й іноземні підходи до правового регулювання обробки персональних даних у сфері використання алгоритмічних технологій, зокрема практику Європейського Союзу, Сполучених Штатів Америки, Великої Британії, Канади та Японії. На підставі проаналізованого матеріалу встановлено тенденцію переходу від формально-процедурних моделей регулювання до моделей, орієнтованих на оцінювання ризиків і запобігання негативним наслідкам для прав людини.

Визначено критерії віднесення систем штучного інтелекту до високоризикових для приватності, доведено необхідність запровадження для таких систем підвищених гарантій прозорості, підконтрольності й відповідальності. Такими критеріями є ступінь автономності алгоритмічної системи під час прийняття рішень; масштаб і характер обробки персональних даних, зокрема біометричних, поведінкових та чутливих даних; можливість формування інференційних висновків і профілів особи; рівень впливу автоматизованих рішень на права, свободи та правовий статус людини; непрозорість алгоритмічної логіки й брак ефективного людського контролю; можливість дискримінаційних або непропорційних наслідків обробки даних; ризик повторної ідентифікації особи в умовах використання технологій Big Data й міжсистемного обміну інформацією.

Розроблено й обґрунтовано конкретні пропозиції з удосконалення законодавства України, а саме: закріплення поняття інференційних персональних даних і високоризикової обробки з використанням штучного інтелекту, запровадження обов'язкової оцінки впливу на захист персональних даних для високоризикових систем, нормативне закріплення права на пояснення автоматизованого рішення та людське втручання, визначення моделі алгоритмічної відповідальності з розмежуванням обов'язків розробника, постачальника й оператора; запровадження алгоритмічного аудиту, спеціальне регулювання біометричної ідентифікації.

Ключові слова: персональні дані, штучний інтелект, Big Data, інференційні дані, алгоритмічна відповідальність, privacy by design, автоматизовані рішення, профілювання, захист приватності, цифрова безпека, допустимість, інформаційне забезпечення, цифрові докази.

ABSTRACT

Mashtaliar O. Legal Protection and Safeguarding of Personal Data in the Field of Artificial Intelligence. – *Qualifying scientific work as a manuscript.*

Dissertation submitted for the degree of Doctor of Philosophy in Law, specialty 081 «Law». – National Academy of Internal Affairs, Kyiv, 2026.

It is substantiated that the rapid implementation of artificial intelligence systems in public administration, the economy, the security sector, and digital services is accompanied by the emergence of new risks to human rights and freedoms associated with automated decision-making, profiling, mass data collection, and the creation of inferential conclusions. It is argued that traditional mechanisms of personal data regulation do not ensure an adequate level of protection under conditions of algorithmic technologies and therefore require systemic adaptation. The traditional model of personal data protection was developed for relatively simple information systems in which data processing had a fixed nature and the data subject could consciously provide consent for a specific purpose. Under conditions of artificial intelligence, this logic no longer functions effectively: algorithmic systems are capable of generating inferential conclusions that did not exist at the time of data collection, making decisions without human involvement, re-identifying anonymized individuals, and using data for purposes that were unforeseeable at the initial stage. The principles of data minimization and purpose limitation come into systemic contradiction with the very logic of machine learning, which requires the broadest possible datasets. At the same time, current legislation does not contain special safeguards concerning automated decisions, inferential data, algorithmic liability, and biometric identification, thereby creating legal gaps that cannot be eliminated within the existing regulatory model.

Accordingly, it has been established that traditional mechanisms of personal data regulation do not ensure an adequate level of protection in the context of algorithmic technologies and require adaptation to contemporary digital processes.

The dissertation substantiates the necessity of establishing a risk-oriented model of legal regulation in the field of artificial intelligence aimed at preventing harm to human rights and ensuring transparency in algorithmic data processing. It has been established that legal significance in the field of artificial intelligence concerns not only individual operations involving personal data, but also the architecture of algorithmic systems, the peculiarities of their training and functioning, and the social consequences of their application.

The study examines contemporary approaches to understanding personal data in the context of the development of Big Data technologies and artificial intelligence. It is demonstrated that algorithmic systems are capable of generating derived and inferential data that may affect an individual's legal status, opportunities, and exercise of fundamental rights. It has been established that inferential data should be distinguished as an independent object of legal protection and should be subject to a special protection regime.

The research identifies the peculiarities of implementing the principles of privacy by design and privacy by default in artificial intelligence systems. International and foreign approaches to the legal regulation of personal data processing in the sphere of algorithmic technologies have been systematized, including the practices of the European Union, the United States, the United Kingdom, Canada, and Japan. Based on the analyzed material, a tendency has been identified toward a transition from formal procedural models of regulation to models focused on risk assessment and the prevention of adverse consequences for human rights.

Criteria for classifying artificial intelligence systems as high-risk for privacy have been determined, and the necessity of introducing enhanced guarantees of transparency, controllability, and accountability for such systems has been substantiated. These criteria include the degree of autonomy of an algorithmic system in decision-making; the scale and nature of personal data processing, including biometric, behavioral, and sensitive data; the ability to generate inferential conclusions and personal profiles; the level of impact of automated

decisions on human rights, freedoms, and legal status; the opacity of algorithmic logic and the absence of effective human oversight; the possibility of discriminatory or disproportionate consequences of data processing; as well as the risk of re-identification in the context of Big Data technologies and inter-system information exchange.

Specific proposals for improving the legislation of Ukraine have been developed and substantiated, including: the introduction of the concepts of inferential personal data and high-risk processing using artificial intelligence; the implementation of mandatory data protection impact assessments for high-risk systems; the legal consolidation of the right to an explanation of automated decisions and the right to human intervention; the establishment of a model of algorithmic accountability with differentiation of the obligations of developers, providers, and operators; the introduction of algorithmic auditing; and special regulation of biometric identification.

Keywords**:** personal data, artificial intelligence, Big Data, inferential data, algorithmic accountability, privacy by design, automated decision-making, profiling, privacy protection, digital security, admissibility, information security, digital evidence.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

у яких опубліковано основні наукові результати дисертації:

1. Машталяр О. М. Проблеми використання штучного інтелекту під час оброблення персональних даних та напрями їх вирішення. *Юридичний науковий електронний журнал*. 2024. № 8. С. 256–259.

2. Машталяр О. М., Хахановський В. Г. Масове спостереження та розпізнавання обличчя за допомогою штучного інтелекту: правові виклики та перспективи регулювання в Україні. *Юридичний науковий електронний журнал*. 2024. № 11. С. 317–321.

3. Машталяр О. М. Розпізнавання ходи як інноваційний метод ідентифікації: аналіз можливостей, ризиків та нормативно-правового середовища в Україні. *Науковий вісник Ужгородського національного університету*. *Серія «Право».* 2025. Вип. 90, ч. 4. С. 310–317.

4. Машталяр О. М., Хахановський В. Г. Людський елемент у системах ШІ, що обробляють персональні дані: європейський стандарт і український дефіцит регулювання. *Юридичний науковий електронний журнал*. 2025. № 11. С. 160–163.

5. Машталяр О. М. Штучний інтелект і біометричні дані в кримінальному процесі України: допустимість, ризики, судовий контроль. *Науковий вісник Ужгородського національного університету*. *Серія «Право».* 2025. Вип. 92, ч. 3. С. 276–283.

6. Машталяр О. М., Петрик В. В. Персональні дані як електронний доказ у кримінальному процесі. *Юридичний науковий електронний журнал.* 2026. № 5. С. 218–221.

які засвідчують апробацію матеріалів дисертації:

1. Машталяр О. М. Масове відеоспостереження як інструмент забезпечення громадського порядку: переваги та загрози для прав людини в Україні. *Застосування інформаційних технологій у правоохоронній*

діяльності : матеріали круглого столу (Харків, 14 груд. 2023 р.). Харків, 2023. С. 68–69.

2. Машталяр О. М., Хахановський В. Г. Правові аспекти захисту персональних даних при використанні технологій штучного інтелекту в експертній діяльності. *Science in the modern world: innovations and challenges* : за матеріалами XIII Міжнар. наук.-практ. конф. (Торонто, 7–9 серп. 2025 р.). Торонто, 2025. С. 254–263.

3. Машталяр О. М. Правові аспекти охорони персональних даних у період воєнного стану та трансформації системи безпеки в Україні. *Креативний простір.* 2025. № 30 : Креативна трансформація та модернізація сучасного суспільства : матеріали Міжнар. наук.-практ. конф. (Харків, 9–11 серп. 2025 р.). С. 9–11.

4. Машталяр О. М., Хахановський В. Г. Правові аспекти використання масового відеоспостереження в Україні: між потребами громадської безпеки та гарантіями прав людини. *Modern Science: Trends, Challenges, Solutions* : матеріали Міжнар. наук.-практ. конф. (Ліверпуль, 21–23 серп. 2025 р.). Ліверпуль, 2025. С. 301–305.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ……..……12
ВСТУП…….…….....14

РОЗДІЛ 1. НАУКОВА, МЕТОДОЛОГІЧНА І ТЕОРЕТИКО-ПРАВОВА ХАРАКТЕРИСТИКА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ШТУЧНОГО ІНТЕЛЕКТУ……..…….....27
1.1. Концептуальні засади правової охорони персональних даних у сфері штучного інтелекту: стан та перспективи наукових досліджень…….……27
1.2. Правове забезпечення захисту персональних даних у сфері застосування систем штучного інтелекту……..……..……...50
1.3. Методологічні підходи до правової охорони та захисту персональних даних у сфері штучного інтелекту……..…….…...…….81
Висновки до розділу 1……...……..…...…….,…113
РОЗДІЛ 2. АНАЛІЗ ЗАРУБІЖНОГО ДОСВІДУ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ШТУЧНОГО ІНТЕЛЕКТУ……..……117
2.1. Поняття та класифікація персональних даних у сфері штучного інтелекту (зарубіжний досвід)……...……..117
2.2. Міжнародні нормативно-правові акти щодо захисту персональних даних у сфері штучного інтелекту……135
2.3. Аналіз правових засад регулювання захисту персональних даних у країнах ЄС і можливість імплементації зарубіжного досвіду в законодавчу практику України…..……...……151
Висновки до розділу 2……...…...……...…171
РОЗДІЛ 3. СУЧАСНИЙ СТАН І ШЛЯХИ ВДОСКОНАЛЕННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

У СФЕРІ ШТУЧНОГО ІНТЕЛЕКТУ В УКРАЇНІ З ОГЛЯДУ НА МІЖНАРОДНИЙ ДОСВІД……..…176
3.1. Сучасний стан і тенденції розвитку національного законодавства щодо захисту персональних даних у сфері штучного інтелекту……..……176
3.2. Проблеми національного законодавства щодо захисту персональних даних у сфері штучного інтелекту та шляхи їх подолання……..……...…198
3.3. Розроблення рекомендацій та пропозицій щодо нормативно-правового забезпечення захисту персональних даних у сфері штучного інтелекту в Україні……..……..…..222
Висновки до розділу 3…….……229

ВИСНОВКИ……232
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……...238
ДОДАТКИ…….....258

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AEPD – *Agencia Española de Protección de Datos* – Іспанське агентство із захисту персональних даних, національний наглядовий орган Іспанії у сфері захисту персональних даних

AI Act – Artificial Intelligence Act, Акт Європейського Союзу про штучний інтелект

AIDA – Artificial Intelligence and Data Act (Закон про штучний інтелект і дані, Канада)

Big Data – великі масиви даних

CCPA – California Consumer Privacy Act (Закон Каліфорнії про конфіденційність споживачів)

CMA – Competition and Markets Authority (Управління з конкуренції та ринків, Велика Британія)

CNIL – Commission Nationale de l'Informatique et des Libertés (Національна комісія з інформатики та свобод, Франція)

COPPA – Children's Online Privacy Protection Act (акт США щодо захисту приватності дітей в інтернеті)

CPPA – Consumer Privacy Protection Act (Закон про приватність споживачів, Канада)

CPRA – California Privacy Rights Act (Закон Каліфорнії про права приватності)

CRM – Customer Relationship Management (система управління відносинами з клієнтами)

DPIA – Data Protection Impact Assessment (оцінка впливу на захист персональних даних)

EDPB – European Data Protection Board (Європейська рада із захисту даних)

EU4DigitalUA – проєкт/платформа EU4DigitalUA

FTC – Federal Trade Commission (Федеральна торгова комісія США)

GDPR – General Data Protection Regulation (Загальний регламент ЄС про захист даних)

IACR – International Association for Cryptologic Research

ICO – Information Commissioner's Office (Офіс Уповноваженого з інформації, Велика Британія)

IEEE – Institute of Electrical and Electronics Engineers

ISO/IEC – International Organization for Standardization / International Electrotechnical Commission (міжнародні стандарти ISO та IEC)

MHRA – Medicines and Healthcare products Regulatory Agency (орган з контролю лікарських засобів, Велика Британія)

NIST – National Institute of Standards and Technology (Національний інститут стандартів і технологій США)

OECD – Organisation for Economic Co-operation and Development (Організація економічного співробітництва та розвитку)

PIPEDA – Personal Information Protection and Electronic Documents Act (Закон Канади про захист персональної інформації та електронних документів)

Privacy Sandbox – технологічна ініціатива Google щодо приватності

RTB – Real-Time Bidding (аукціон реклами в реальному часі)

ЄС – Європейський Союз

Конвенція 108+ – модернізована Конвенція Ради Європи № 108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних

МВС – Міністерство внутрішніх справ

ООН – Організація Об'єднаних Націй

ШІ – штучний інтелект

ЮНЕСКО – Організація Об'єднаних Націй з питань освіти, науки і культури

ВСТУП

Обґрунтування вибору теми дослідження. Стрімке впровадження систем штучного інтелекту в публічне управління, економіку, сферу безпеки та цифрові сервіси кардинально змінює характер обробки персональних даних. Алгоритмічні системи здатні автоматично приймати рішення, що впливають на права людини, формувати детальні цифрові профілі, здійснювати масове спостереження та генерувати інференційні висновки – відомості про особу, яких не було на момент первинного збору даних, однак які можуть визначати її доступ до кредитів, працевлаштування, соціальних послуг і правосуддя. Традиційна модель захисту персональних даних, сформована навколо принципів інформованої згоди, цільового обмеження та мінімізації, виявляється недостатньою в умовах самонавчальних алгоритмів і масивів Big Data. Концепція згоди переживає кризу ефективності: суб’єкт даних фізично не здатен контролювати всі сценарії подальшого використання своєї інформації, а анонімізація більше не гарантує захисту в умовах комбінування різнорідних наборів даних. Чинне законодавство України не містить спеціальних гарантій щодо автоматизованих рішень, інференційних даних, алгоритмічної відповідальності та біометричної ідентифікації, що утворює системні прогалини, які неможливо усунути в межах наявної нормативної моделі.

На міжнародному рівні відповідь на ці виклики вже формується: Європейський Союз запровадив GDPR та Акт про штучний інтелект 2024 року, Рада Європи розробила рамкову конвенцію про ШІ та права людини, ЮНЕСКО ухвалила Рекомендацію з етики ШІ. Для України питання набуває стратегічного виміру: євроінтеграційний курс, статус кандидата в ЄС з 2023 року й активна цифровізація державних послуг зумовлюють необхідність системної адаптації національного законодавства. Законопроєкт № 8153 «Про захист персональних даних», прийнятий у першому читанні в листопаді 2024 року, є кроком у цьому напрямі, однак не містить

спеціального регулювання обробки персональних даних у системах штучного інтелекту.

У межах роботи над дисертаційним дослідженням автор провів опитування та анкетування 112 осіб – практичних працівників у сфері правозастосування та цифрової безпеки з питань правової охорони та захисту персональних даних у сфері штучного інтелекту (додаток А).

Опрацьовуючи та систематизуючи отримані результати, автор сформулював такі висновки. Зокрема, 20,3 % респондентів вважають, що чинного законодавчого регулювання обробки персональних даних із використанням технологій штучного інтелекту достатньо, водночас 48,6 % опитаних зазначили, що законодавство потребує суттєвого оновлення. Лише 6,3 % респондентів не змогли визначитися з відповіддю на це питання. Серед основних недоліків чинного законодавства найбільше респондентів зауважили про брак спеціального правового режиму обробки персональних даних у системах ШІ – 30,3 %, відсутність визначення інференційних персональних даних – 25,2 %, а також брак алгоритмічного аудиту – 14,8 %.

Водночас 40,9 % опитаних вважають, що в законодавстві України обов’язково потрібно окремо закріпити правовий режим обробки персональних даних у системах штучного інтелекту. Ще 25,1 % поділяють таке закріплення лише для високоризикових систем ШІ. Натомість 15,5 % респондентів вважають достатніми загальні норми про захист персональних даних, а 12,7 % не вбачають у цьому потреби. Щодо розмежування правової охорони та правового захисту персональних даних у сфері ШІ, 21,4 % респондентів схвалюють підхід, за яким правова охорона має охоплювати превентивні гарантії до порушення права, а 22,8 % зазначили, що правовий захист має охоплювати засоби реагування після порушення або загрози порушення.

Увагу в межах анкетування було зосереджено на інференційних персональних даних. 33,7 % респондентів зазначили, що добре знайомі з цим поняттям, 50,4 % – частково знайомі, а 12,1 % чули про нього, але не мають

чіткого розуміння. Лише 3,8 % опитаних не знають про це поняття. Майже половина респондентів – 49,7 % – вважають, що інференційні персональні дані обов'язково потребують окремого правового регулювання, а 24,7 % поділяють таке регулювання лише у випадках, коли ці дані істотно впливають на права особи. Найвищі ризики для прав людини респонденти пов'язують з інференційними висновками щодо оцінки кредитоспроможності – 40,1 %, прогнозу поведінки особи – 16,8 %, а також висновків щодо стану здоров'я – 16,7 %.

Аналіз відповідей також засвідчив, що 40,7 % респондентів вважають профілювання особи за допомогою ШІ таким, що створює високі ризики для права на приватність. Ще 15,2 % зазначили, що такі ризики залежать від сфери застосування ШІ. Стосовно права особи на пояснення автоматизованого рішення, прийнятого з використанням ШІ, 32,7 % опитаних вважають його законодавче закріплення обов'язковим, а 26,4 % схвалюють таку необхідність у випадках, коли рішення має істотний вплив на права особи. Крім того, 42,2 % респондентів вважають, що право особи на людське втручання або перегляд автоматизованого рішення людиною має бути закріплене в усіх випадках автоматизованого рішення, а 26,5 % – лише щодо рішень із правовими або істотними наслідками.

Питання біометричної ідентифікації з використанням ШІ також привернули увагу респондентів. Найсуворішого правового контролю, на думку опитаних, потребують усі перелічені види біометричної ідентифікації – 24,4 %, розпізнавання обличчя – 20,0 %, розпізнавання голосу – 19,8 %, поведінкова біометрія – 13,1 %, масове відеоспостереження з автоматичною ідентифікацією – 12,4 %, а також розпізнавання ходи – 10,3 %. Водночас 52,0 % респондентів вважають допустимим використання систем розпізнавання обличчя в публічних місцях без обмежень, якщо це потрібно для безпеки. Водночас 16,6 % допускають таке використання лише в чітко визначених законом випадках, а 19,0 % – тільки за рішенням суду або з дозволу незалежного органу.

Серед найсуттєвіших ризиків використання біометричних ШІ-систем респонденти визначили використання даних не за первинною метою – 18,2 %, помилкову ідентифікацію особи – 15,5 %, незаконне масове спостереження – 15,2 %, дискримінаційні помилки алгоритму – 15,1 %, відсутність незалежного контролю – 14,0 %, неможливість ефективного оскарження результату – 11,9 %, а також витік біометричних даних – 10,1 %.

Аналізуючи думки респондентів щодо впровадження ризик-орієнтованого підходу до регулювання обробки персональних даних у системах ШІ, слід зазначити, що 40,2 % цілком поділяють такий підхід, а 20,2 % більше схвалюють. Визначаючи критерії високоризикової обробки персональних даних із використанням ШІ, респонденти найчастіше вказували на профілювання особи – 19,2 %, автономність системи – 15,2 %, використання біометричних або чутливих даних – 15,2 %, масштабність обробки даних – 12,7 %, істотний вплив рішення на права людини – 10,0 %, непрозорість алгоритму – 10,2 % і ризик дискримінації – 10,2 %.

Також слід зазначити, що 19,4 % респондентів схвалюють обов’язкову оцінку впливу на захист персональних даних для високоризикових систем ШІ, 30,2 % вважають її необхідною лише в державному секторі, а 33,2 % – лише для великих приватних компаній. Щодо алгоритмічного аудиту високоризикових ШІ-систем 30,8 % опитаних вважають його обов’язковим, 15,2 % – лише для державних систем, а 20,2 % – для систем, що обробляють біометричні або чутливі дані.

Респонденти висловили позицію і щодо суб’єктів відповідальності за порушення прав особи внаслідок обробки персональних даних ШІ-системою. Найбільша частка опитаних – 30,0 % – вважає, що відповідальність мають нести всі суб’єкти залежно від їх ролі в життєвому циклі системи. Водночас 22,5 % покладають таку відповідальність на постачальника ШІ-системи, 20,7 % – розробника ШІ-системи, 15,1 % – оператора або користувача ШІ-системи, 6,5 % – орган державної влади, який використовує систему, 5,2 % – володільця персональних даних.

Аналізуючи думки респондентів щодо напрямів удосконалення законодавства України у сфері захисту персональних даних під час використання ШІ, слід зауважити, що найактуальнішими вони визначили: закріплення поняття високоризикової обробки персональних даних із використанням ШІ – 15,0 %, законодавче закріплення права на людське втручання – 13,6 %, закріплення поняття інференційних персональних даних – 12,0 %, створення незалежного органу захисту персональних даних – 11,2 %, запровадження обов'язкової оцінки впливу на захист персональних даних – 11,0 %, спеціальне регулювання біометричної ідентифікації – 10,1 %, запровадження алгоритмічного аудиту – 10,1 %, гармонізацію законодавства України з GDPR та AI Act – 10,2 %, а також законодавче закріплення права на пояснення автоматизованого рішення – 6,8 %.

Проблеми правової охорони та захисту персональних даних у контексті інформаційних технологій досліджували українські науковці І. Андрющенко, І. Арістова, Д. Арзянцева, В. Базалицький, Д. Бєлов, М. Бєлова, М. Бліхар, В. Брижко, І. Бухтіярова, Ф. Гакер, М. Дубняк, А. Енгель, О. Заярний, О. Золотар, О. Карапетян, О. Ковальова, А. Колесніков, О. Корнейко, Є. Остіян, О. Пунда, Г. Майкл, М. Маурер, В. Пилипчук, М. Погорецький, А. Радченко, Н. Савлієва, М. Співак, К. Токарєва, В. Хахановський, М. Швець та ін. Зарубіжна доктрина спрямовує значну увагу на алгоритмічну відповідальність, пояснюваність рішень ШІ й захист інференційних даних. Водночас в українській правовій науці немає комплексних досліджень, присвячених системному аналізу правової охорони та захисту персональних даних саме у сфері штучного інтелекту, з огляду на європейські регуляторні тенденції та українські реалії, що й зумовило вибір теми дослідження.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертаційне дослідження виконано відповідно до Цілей сталого розвитку України на період до 2030 року, Концепції розвитку штучного інтелекту в Україні, схваленої розпорядженням Кабінету Міністрів України від 2 грудня 2020 року № 1556-р, а також Стратегії цифрової трансформації

соціальної сфери, схваленої розпорядженням Кабінету Міністрів України від 28 жовтня 2020 року № 1353-р. Зазначені програмні документи визначають актуальність цифрової трансформації, розвитку технологій штучного інтелекту, підвищення рівня захисту прав людини в цифровому середовищі та формування сучасних правових механізмів використання даних.

Робота відповідає тематиці наукових досліджень і науково-технічних експериментальних розробок Міністерства внутрішніх справ України на 2025–2029 роки, затвердженій наказом МВС України від 21 травня 2024 року № 326, а також основним напрямам наукових досліджень Національної академії внутрішніх справ на 2025–2029 роки. Проблематика дисертації узгоджується з науковими завданнями, пов’язаними з правовим забезпеченням цифрової трансформації, інформаційною безпекою, захистом прав людини, використанням сучасних інформаційних технологій та вдосконаленням правового регулювання у сфері обробки персональних даних.

Тема дисертації також безпосередньо пов’язана з виконанням зобов’язань України за Угодою про асоціацію з Європейським Союзом в частині адаптації національного законодавства про захист персональних даних до європейських стандартів. Отже, дослідження відповідає як державним науковим програмам, так і міжнародним правовим зобов’язанням України, відображаючи інтеграцію правових і технологічних аспектів відповідно до вимог сьогодення.

Тема дисертації затверджена рішенням Вченої ради Національної академії внутрішніх справ від 26 грудня 2022 року (протокол № 16) та уточнено на засіданні Вченої ради Національної академії внутрішніх справ від 29 грудня 2023 року (протокол № 26).

Мета і завдання дослідження. *Метою* роботи є розроблення теоретико-правових засад і практичних рекомендацій з удосконалення правової охорони та захисту персональних даних у сфері застосування технологій штучного інтелекту в Україні з огляду на міжнародний досвід.

Для досягнення поставленої мети сформульовано такі основні *завдання*:

– висвітлити концептуальні засади штучного інтелекту та визначити його вплив на обробку персональних даних;

– дослідити стан наукового розроблення проблеми та генезу правових підходів до охорони персональних даних у сфері ШІ в Україні;

– окреслити методологічні підходи до правової охорони та захисту персональних даних в умовах розвитку алгоритмічних технологій;

– проаналізувати поняття та класифікацію персональних даних у сфері ШІ на основі іноземного досвіду;

– систематизувати міжнародні нормативно-правові акти у сфері захисту персональних даних під час використання ШІ;

– дослідити правові засади регулювання захисту персональних даних у країнах ЄС, а також можливості імплементації зарубіжного досвіду в законодавство України;

– розглянути сучасний стан і тенденції розвитку національного законодавства щодо захисту персональних даних у сфері ШІ;

– виявити проблеми національного законодавства у відповідній сфері та визначити шляхи їх подолання;

– розробити рекомендації щодо нормативно-правового забезпечення захисту персональних даних у сфері штучного інтелекту в Україні.

*Об'єктом дослідж*ення є суспільні відносини, що виникають у процесі використання технологій штучного інтелекту й обробки персональних даних.

Предметом дослідження є правова охорона і захист персональних даних у сфері штучного інтелекту.

Методи дослідження. Для досягнення поставлених мети й завдань використано комплекс філософських, загальнонаукових і спеціально-юридичних методів.

Компаративістський метод застосовано для аналізу закордонних моделей правового регулювання захисту персональних даних і систем ШІ,

зокрема підходів ЄС, США, Великої Британії, Канади та Японії, а також для оцінювання можливостей імплементації міжнародних стандартів у національне законодавство (усі розділи).

Догматичний метод використано для аналізу чинних норм національного законодавства, виявлення їх суперечностей та прогалин, формулювання пропозицій з удосконалення правового регулювання (розділи 2, 3).

Формально-юридичний метод застосовано для тлумачення та систематизації норм Конституції України, Закону України «Про захист персональних даних», проєкту закону № 8153, GDPR, Конвенції 108+ й Акта ЄС про штучний інтелект (усі розділи).

Логіко-семантичний метод використано для уточнення понятійно-категоріального апарату дослідження, зокрема понять «інференційні дані», «автоматизоване рішення», «алгоритмічна відповідальність», «профілювання» (усі розділи).

Системно-структурний метод застосовано для розгляду правової охорони персональних даних у сфері ШІ як цілісної системи правових, інституційних і технічних елементів (усі розділи).

Метод моделювання використано для розроблення концептуальної моделі ризик-орієнтованого правового регулювання та визначення ролей розробників, постачальників й операторів ШІ-систем (розділ 3).

Прогностичний метод застосовано для оцінювання можливих наслідків імплементації європейських стандартів і формування рекомендацій щодо запобігання майбутнім правовим ризикам (розділ 3).

Емпіричну базу дослідження становлять матеріали, що відображають практичний стан правової охорони й захисту персональних даних у сфері штучного інтелекту. Вона охопила результати анкетування 112 практичних працівників у сфері правозастосування та цифрової безпеки, офіційні звіти, аналітичні матеріали, правові публікації, узагальнення практики застосування законодавства про захист персональних даних, а також інші

джерела, що стосуються проблем обробки персональних даних, використання штучного інтелекту, автоматизованих рішень, біометричних технологій та цифрової безпеки.

Наукова новизна отриманих результатів полягає в тому, що дисертація є одним із перших комплексних досліджень правової охорони та захисту персональних даних у сфері штучного інтелекту в українській правовій науці, у якому зазначену проблематику розглядають як самостійний об’єкт правового регулювання з огляду на технологічну специфіку алгоритмічних систем і підвищених ризиків для прав та свобод людини. Найсуттєвіші результати дисертаційного дослідження, що визначають його наукову новизну, полягають:

вперше:

– сформульовано цілісну наукову концепцію правової охорони та захисту персональних даних у сфері ШІ, ґрунтовану на ризик-орієнтованому підході та принципах антропоцентричності, у межах якої персональні дані розглянуто як ключовий елемент життєвого циклу алгоритмічних систем;

– запропоновано виокремлення інференційних персональних даних як самостійного об’єкта правової охорони, визначено спеціальний режим їх захисту з огляду на здатність таких даних впливати на правовий статус особи;

– розроблено модель алгоритмічної відповідальності, яка передбачає диференціацію обов’язків між розробниками, постачальниками й операторами ШІ-систем залежно від їхньої ролі у створенні та використанні алгоритмів;

– обґрунтовано підхід до правової оцінки обробки персональних даних через архітектуру алгоритмічних систем, логіку машинного навчання та соціальні наслідки автоматизованих рішень;

удосконалено:

– підхід до застосування принципів privacy by design і privacy by default шляхом їх адаптації до алгоритмічно складних систем на всіх етапах життєвого циклу моделі;

– підхід до проведення оцінки впливу на захист персональних даних шляхом включення специфічних критеріїв ШІ, зокрема ризиків інференційного профілювання та непрозорості алгоритмів;

дістали подальший розвиток:

– наукові підходи до розуміння персональних даних шляхом розширення їх поняття за рахунок інференційних і похідних даних, які формують алгоритмічні системи;

– положення щодо ризик-орієнтованого підходу до правового регулювання ШІ стосовно архітектури та функціональних характеристик алгоритмічних систем;

– підходи до забезпечення прозорості автоматизованих рішень шляхом обґрунтування необхідності нормативного закріплення обов'язку пояснюваності як ключової гарантії захисту прав людини.

Практичне значення отриманих результатів полягає в тому, що висновки й рекомендації дисертації впроваджено та використовуються у:

– *науковій діяльності* – під час підготовки монографій, підручників, навчальних посібників, методичних рекомендацій, узагальнення аналітичних матеріалів, обґрунтування пропозицій до чинних проєктів нормативно-правових актів, підготовка яких потребує проведення відповідних наукових досліджень або містить наукову складову (акт Національної академії внутрішніх справ від 3 листопада 2025 року № 501-НД);

– *освітньому процесі* – під час викладання навчальних дисциплін «Інформаційні технології та системи», «Застосування інформаційних технологій в правоохоронній діяльності», «Аналіз та прогнозування злочинності», для підготовки навчально-методичних і дидактичних

матеріалів (акт Національної академії внутрішніх справ від 3 листопада 2025 року № 502-ОП);

– *практичній діяльності* Ради адвокатів Київської області – для організаційного, методичного й інформаційного забезпечення діяльності адвокатів з питань захисту персональних даних у сфері використання штучного інтелекту, зокрема щодо: 1) підготовки рекомендацій для адвокатів стосовно дотримання вимог законодавства про захист персональних даних під час роботи з цифровими сервісами, електронними доказами, автоматизованими системами й технологіями ШІ; 2) урахування ризиків обробки персональних, біометричних та інших чутливих даних у професійній діяльності адвоката; 3) удосконалення підходів до захисту прав клієнтів у випадках автоматизованого прийняття рішень, профілювання, використання алгоритмічних систем або цифрового спостереження; 4) використання окремих положень дисертації під час проведення освітніх заходів, семінарів, круглих столів і підвищення професійного рівня адвокатів з питань цифрової безпеки, конфіденційності, захисту персональних даних (акт Ради адвокатів Київської області від 30 грудня 2025 року № 1385/0/2-25);

– *практичній діяльності* адвокатів АБ «ОЛЕКСАНДР БАЙДИК ТА ПАРТНЕРИ» – під час надання правничої допомоги фізичним і юридичним особам у справах, пов’язаних із захистом персональних даних, використанням цифрових технологій, систем штучного інтелекту, автоматизованої обробки інформації та біометричної ідентифікації, зокрема щодо: 1) підготовки правових позицій у справах про незаконне збирання, зберігання, поширення або використання персональних даних; 2) оцінювання правомірності використання електронних доказів, цифрових слідів, відеозаписів, біометричних даних і результатів автоматизованого аналізу інформації; 3) розроблення внутрішніх рекомендацій щодо захисту адвокатської таємниці, конфіденційної інформації клієнтів і персональних даних під час використання електронних сервісів та цифрових комунікацій; 4) формування правових висновків і консультацій щодо ризиків застосування

ШІ-систем, алгоритмічного профілювання, автоматизованих рішень та необхідності людського контролю за такими процесами (акт АБ «ОЛЕКСАНДР БАЙДИК ТА ПАРТНЕРИ» від 1 грудня 2025 року).

Крім цього, висновки та рекомендації дисертації може бути використано в законотворчій діяльності для вдосконалення Закону України «Про захист персональних даних», під час доопрацювання законопроєкту № 8153 і подальшого розроблення спеціального законодавства у сфері ШІ.

Особистий внесок здобувача. Висновки та рекомендації дисертаційного дослідження, що формують його наукову новизну, розроблено відповідно до вимог законодавства України з дотриманням норм і стандартів академічної доброчесності з метою поглибленого аналізу наукових категорій та комплексного дослідження правової охорони й захисту персональних даних у сфері штучного інтелекту.

Апробація матеріалів дисертації. Ключові положення дисертаційного дослідження, а також сформульовані автором висновки та практичні рекомендації були апробовані під час виступів на міжнародних науково-практичних конференціях і засіданні круглого столу, зокрема: *«Масове відеоспостереження як інструмент забезпечення громадського порядку: переваги та загрози для прав людини в Україні»* (м. Харків, 14 грудня 2023 року); *«Правові аспекти захисту персональних даних при використанні технологій штучного інтелекту в експертній діяльності»* (м. Торонто, Канада, 7–9 серпня 2025 року); *«Правові аспекти охорони персональних даних у період воєнного стану та трансформації системи безпеки в Україні»* (м. Харків, 9–11 серпня 2025 року); *«Правові аспекти використання масового відеоспостереження в Україні: між потребами громадської безпеки та гарантіями прав людини»* (м. Ліверпуль, Велика Британія, 21–23 серпня 2025 року).

Особистий внесок здобувача. Пошук, опрацювання та аналіз наукових джерел, нормативно-правових актів, міжнародних стандартів і практичних матеріалів за темою дисертаційного дослідження здобувач здійснив

самостійно. Теоретичні положення, висновки, пропозиції та практичні рекомендації щодо правової охорони та захисту персональних даних у сфері штучного інтелекту сформульовані й обґрунтовані автором особисто. Основні наукові результати дисертації відображено в наукових публікаціях дисертанта, підготовлених і викладених автором самостійно в трьох наукових публікаціях, а також трьох наукових статтях у співавторстві. У працях, виконаних у співавторстві, особистий внесок дисертанта становить 50 % і полягає в дослідженні проблем захисту персональних даних, аналізі ризиків використання штучного інтелекту, біометричних технологій, автоматизованої обробки інформації, цифрових доказах та формулюванні пропозицій з удосконалення законодавства України в цій сфері.

Публікації. Основні наукові положення та результати дисертаційного дослідження відображено в десяти наукових працях, з яких шість статей опубліковано в наукових виданнях України, включених МОН України до переліку фахових із юридичних наук, чотири – тези доповідей, оприлюднені за результатами участі в міжнародних науково-практичних конференціях, засіданні круглого столу.

Структура та обсяг дисертації. Робота структурно містить анотації українською та англійською мовами, перелік умовних позначень, вступ, три розділи, що мають дев’ять підрозділів, висновки, список використаних джерел (172 позицій, 20 сторінок) і трьох додатків (17 сторінок). Повний обсяг дисертації становить 274 сторінки, із них обсяг основного тексту – 225 сторінок.

РОЗДІЛ 1
НАУКОВА, МЕТОДОЛОГІЧНА І ТЕОРЕТИКО-ПРАВОВА ХАРАКТЕРИСТИКА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ШТУЧНОГО ІНТЕЛЕКТУ

1.1. Концептуальні засади правової охорони персональних даних у сфері штучного інтелекту: стан та перспективи наукових досліджень

Дослідження правової охорони і захисту персональних даних у сфері штучного інтелекту доцільно, на наш погляд, розпочати із з'ясування природи самого штучного інтелекту, його інформаційної основи та особливостей впливу на обробку персональних даних. Це має значення для всієї праці, оскільки без попереднього розуміння того, як працюють алгоритмічні системи, які дані вони використовують та які ризики створюють для людини, неможливо повною мірою оцінити правові гарантії, способи охорони та механізми захисту персональних даних.

Після цього звернемо увагу на сучасний стан та перспективи наукових досліджень з цієї проблематики, основні доктринальні підходи українських і зарубіжних учених, проаналізуємо наявну наукову полеміку.

Для ґрунтовного аналізу питань правового захисту персональних даних у сфері штучного інтелекту першочерговим є з'ясування концептуальних засад явища ШІ, специфіки інформаційних процесів, що є основою його функціонування, та історії створення ШІ. Штучний інтелект не є ізольованою технологією, а функціонує в межах складної цифрової екосистеми, де дані є ключовим ресурсом, тому без попереднього теоретичного окреслення подальший аналіз правових механізмів захисту даних втрачає системність. В умовах сьогодення поняття «штучний інтелект» не має єдиного універсального визначення, закріпленого в міжнародному праві. Несформованість усталеної дефініції зумовлена як новизною цього

феномена, так і стрімкими темпами його технологічного розвитку, які ускладнюють формування стабільних правових конструкцій та формулювання дефініцій. У науковій та нормативній площині співіснують різні підходи до розуміння ШІ – від вузькотехнічних до міждисциплінарних, що охоплюють соціальні, етичні та правові аспекти [31, с. 47–53]. З огляду на те, що штучний інтелект використовують у всіх сферах (міждисциплінарно, від сфери соціальної до сфери права), його міжгалузеве правове значення стає значущішим [27].

Брак встановлених процедур перевірки законності отримання та використання біометричних даних створює ризики легалізації недопустимих доказів і формування неконтрольованої практики спостереження. Тому постає необхідність розроблення нормативних критеріїв допустимості алгоритмічних доказів, визначення меж застосування ШІ правоохоронними органами, а також механізмів незалежного аудиту й перевірки точності алгоритмів.

Для формування вичерпного розуміння значення такого феномену, як штучний інтелект, слід з’ясувати, що саме він опрацьовує, а це передусім інформація. Адже штучний інтелект працює зрештою з інформацією та даними.

Відомо, що у праві категорія «інформація» має загальне значення. Так, Закон України «Про інформацію» визначає інформацію як «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [38]. Це формулювання є загальним і охоплює широкий обсяг відомостей про осіб, події, явища, процеси та інші об’єкти.

Водночас для розуміння штучного інтелекту важливо розмежовувати такі два поняття, як «інформація» та «дані». Адже інформація відображає зміст певних відомостей, а дані є формою, у якій ці відомості можуть бути зчитані, оброблені, зіставлені або використані комп’ютерною системою. Саме тому в системах ШІ дані мають не пасивне, а активне значення: вони

використовуються для навчання алгоритмів, перевірки їх роботи, побудови прогнозів, класифікації осіб і формування нових висновків.

У цьому контексті персональні дані є особливо важливими, оскільки вони пов’язані з конкретною фізичною особою або можуть дати змогу її ідентифікувати. Якщо традиційні інформаційні системи переважно зберігали чи передавали такі дані, то системи штучного інтелекту можуть аналізувати їх, поєднувати з іншими масивами інформації та створювати нові висновки про людину. Саме ця обставина зумовлює потребу в подальшому аналізі правової охорони і захисту персональних даних у сфері ШІ.

Отже, штучний інтелект працює з даними, а персональні дані в таких системах стають не лише об’єктом зберігання, а й ресурсом для аналізу, прогнозування та формування нових висновків про особу.

Слід зазначити, що правова проблема використання штучного інтелекту не виникла відразу. Еволюція розвитку ШІ в Україні з 1950-х років до сучасного стану включає декілька важливих етапів. Спочатку ШІ розвивався як технічне явище та науковий напрям, пов’язаний із математикою, кібернетикою, інформатикою, програмуванням. Почалося створення певних моделей, які імітували окремі інтелектуальні дії людини. Надалі ШІ перейшов до машинного навчання. Якщо ранні системи працювали переважно за наперед заданими правилами, то сучасні системи навчаються на великих масивах даних, виявляють закономірності й формують прогнози [35, с. 48–54].

У другій половині ХХ ст. домінували підходи, що ґрунтувалися на символічному представленні знань і використанні експертних систем, у межах яких інтелект тлумачили як сукупність формалізованих правил і логічних конструкцій. Дані системи своєю чергою мали обмежений рівень автономності та функціонували виключно в межах чітко визначених сценаріїв, що істотно звужувало як сферу їх застосування, так і потенційний вплив на соціальні процеси. Обробка інформації на цьому етапі не була масовою, а використання даних, пов’язаних із конкретними особами, було

винятком, а не системною практикою [35]. Подальшим етапом розвитку штучного інтелекту став перехід до розроблення, орієнтованого на аналіз даних і здатність систем до навчання на підставі емпіричних масивів інформації. Розширення обчислювальних потужностей, поширення цифрових технологій і накопичення значних обсягів інформації спричинили зміну дослідної парадигми, у межах якої дані поступово перетворилися на ключовий ресурс функціонування інтелектуальних систем. На цьому етапі штучний інтелект розвивається як технологія, здатна не лише відтворювати задані алгоритми, а й адаптувати свою поведінку відповідно до нових вхідних даних [35]. Така еволюція зумовила переосмислення ролі штучного інтелекту в суспільстві та його впливу на різні сфери людської діяльності. Від інструмента автоматизації окремих процесів він поступово трансформувався в складні системи, інтегровані в економічні, адміністративні та соціальні відносини, що зумовило необхідність інтегрування в системи штучного інтелекту надмасивних обсягів інформації різного типу, які в сучасному світі називають Big Data. Зв’язок з ними став фактично визначальною рисою для наявних алгоритмічних систем. Big Data також слід розглядати не лише як великі за обсягом масиви інформації, а і як специфічний режим обробки даних, що вирізняється їх різнорідністю, високою швидкістю оновлення та можливістю багаторазового поєднання різних джерел. У таких умовах традиційні методи збору, зберігання та аналізу інформації виявляються неефективними, що зумовлює застосування спеціалізованих алгоритмічних й обчислювальних технологій [14, с. 72].

Згодом в Україні, коли ШІ почали використовувати у сфері державного управління, безпеки, медицини, фінансів, через цифровізацію держави, електронні послуги, відеоспостереження, біометричні технології та автоматизовану аналітику, він почав набувати правового значення. Перехід до правового значення безперечно пов’язаний з обробкою персональних даних. Адже, чим більше ШІ використовується для аналізу даних про особу,

тим більше виникає питань щодо приватності, обробки персональних даних, автоматизованих рішень та відповідальності.

Слід зазначити, що державне закріплення розвитку ШІ в Україні відбулося у 2020 році, коли розпорядженням Кабінету Міністрів України була схвалена Концепція розвитку штучного інтелекту в Україні, затверджену розпорядженням КМУ від 02.12.2020 № 1556-р. У ній визначаються мета, принципи та завдання розвитку технологій ШІ в Україні як одного з пріоритетних напрямів науково-технологічних досліджень. В Концепції штучний інтелект визначено як організовану сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань [34].

Щодо міжнародних нормативно-правових документів, у першу чергу, на наш погляд, слід згадати Регламент (ЄС) 2024/1689 Європейського Парламенту та Ради від 13 червня 2024 року, що встановлює гармонізовані правила щодо штучного інтелекту та вносить зміни до Регламентів ЄС 2008, 2013, 2018, 2019 та Директив 2014, 2016 та 2020 років [118].

Це свідчить про поступовий перехід від сприйняття ШІ як суто технічного явища до його розуміння як сфери, що потребує правового, організаційного та етичного врегулювання.

Отже, ШІ вже має правове значення, надалі в нашій роботі доцільно з’ясувати, як саме його визначають у науці, українських документах та міжнародних актах.

Поняття «штучний інтелект» вперше запропонував у 1955 році Джон Маккарті, на той час доцент математики Дартмутського коледжу. Він прагнув відмежувати цю нову галузь наукових досліджень від добре відомої кібернетики [50, с. 242–248]. Трохи пізніше він визначив ШІ як науку і

техніку створення інтелектуальних машин, а також особливо інтелектуальних комп'ютерних програм [108].

Так, експертна група Європейської комісії зі штучного інтелекту запропонувала визначати штучний інтелект як «системи, розроблені людьми, які, отримавши комплексну мету, діють у фізичному чи цифровому світі, сприймаючи навколишнє середовище, інтерпретуючи зібрані структуровані або неструктуровані дані, на основі знань, отриманих з цих даних, приймають найкращі рішення (відповідно до попередньо визначених параметрів) для досягнення заданої мети [52].

У загальному значенні штучним інтелектом вважають комплекс програмно-апаратних рішень й алгоритмічних методів, здатних імітувати окремі когнітивні людські функції, здійснювати навчання на основі даних і генерувати результати, які можуть впливати на поведінку людей або процеси ухвалення рішень. Такий підхід простежується, зокрема, у документах Європейського Союзу, де ШІ-систему визначають як програмне забезпечення, що використовує машинне навчання, логічне виведення чи статистичні методи для формування прогнозів, рекомендацій, рішень або контенту відповідно до поставлених завдань [124]. Таке визначення акцентує саме на функціональних характеристиках ШІ. Серед них ключовими є автономність й адаптивність.

Автономність означає здатність системи діяти без постійного втручання людини, а адаптивність – можливість змінювати свою поведінку або параметри функціонування на основі аналізу нових даних. Ці властивості зумовлюють підвищені ризики для персональних даних, оскільки процеси їх обробки стають менш передбачуваними для суб'єктів даних і навіть для операторів систем.

Дискусії навколо визначення поняття «штучний інтелект» тривають. Існує декілька груп вчених різних наукових галузей, які використовують для цього різні підходи: комп'ютерний; хімічний; біологічний тощо [95].

Слід з позитивного боку відзначити універсальне визначення поняття ШІ О.А. Баранова, який розглянув спочатку окремо поняття «штучний» та «інтелект». Отже, на думку автора, штучний інтелект – це сукупність методів, способів, засобів і технологій (у першу чергу – комп'ютерних), що імітує (моделює) когнітивні функції, які мають критерії, характеристики та показники еквівалентні показникам відповідних когнітивних функцій людини [45, с. 32-49].

Для нашої роботи вкрай важливо підкреслити, що ШІ не можна розуміти лише як програму або технічний інструмент. У нашому випадку ми розуміємо штучний інтелект як складну комплексну систему, яка працює з даними, спроможна їх аналізувати, формувати висновки, прогнози або рекомендації, а в окремих випадках – впливати на рішення щодо конкретної особи. Саме таке розуміння дає змогу надалі оцінити, чому використання ШІ змінює традиційну модель обробки персональних даних і потребує спеціальних правових гарантій.

Закон України «Про захист персональних даних» визначає персональні дані як відомості чи сукупність відомостей про фізичну особу, яку ідентифіковано або може бути конкретно ідентифіковано [36]. Це визначення охоплює не лише прямі ідентифікатори, а й відомості, які дають змогу встановити особу опосередковано. В сфері ШІ таке розуміння має особливе значення, бо алгоритми можуть поєднувати різні масиви інформації й робити висновки про людину.

Обробка персональних даних – це будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем [36]. Тобто, в традиційному правовому розумінні обробка персональних даних – це сукупність дій із такими даними: збирання, зберігання, використання, зміна, поширення, знеособлення, знищення тощо.

Разом з тим, у сфері штучного інтелекту обробка стає складнішою. Вона вже не обмежується простим збиранням або зберіганням інформації. Персональні дані можуть використовуватися для: навчання алгоритмічної моделі; тестування її роботи; перевірки точності результатів; автоматизованого оцінювання особи; профілювання; прогнозування поведінки; формування інференційних або похідних висновків.

Розвиток технологій штучного інтелекту зумовлює глибинну трансформацію процесів обробки персональних даних, що ставить під сумнів здатність національної моделі правового захисту адекватно реагувати на нові виклики цифрової реальності. На відміну від традиційних інформаційних систем, у яких обробка персональних даних відбувається за заздалегідь визначеними сценаріями та підлягає відносно простому правовому контролю, сучасні ШІ-системи вирізняються динамічністю, самонавчанням і стохастичним характером результатів. У таких умовах право постає перед об’єктивними складнощами встановлення чітких меж допустимої обробки та визначення моменту, з якого виникають правові ризики для суб’єктів персональних даних [101].

Технологічна специфіка сучасних систем штучного інтелекту полягає у використанні великих масивів даних, розподілених обчислювальних середовищ і моделей машинного навчання, здатних до самостійної адаптації. У таких умовах обробка персональних даних часто виходить за межі однократних або чітко локалізованих операцій і набуває безперервного характеру. Чинне законодавство натомість орієнтоване на фіксацію окремих актів обробки та не враховує кумулятивний ефект алгоритмічних процесів, у межах яких персональні дані можуть неодноразово використовувати, поєднувати з іншими джерелами і трансформувати в похідні результати [105; 129].

Вплив штучного інтелекту на обробку персональних даних не є однозначним і виявляється як у позитивному, так і в проблемному аспектах. З одного боку, сучасні алгоритмічні рішення здатні підвищувати рівень

захисту інформації, автоматизувати виявлення аномалій та потенційних витоків даних, а також забезпечувати застосування технік шифрування, псевдонімізації або анонімізації в режимі реального часу [31, с. 51; 58]. Крім того, ШІ використовують як інструмент забезпечення дотримання вимог законодавства про персональні дані, зокрема шляхом автоматизованого управління згодами користувачів, ідентифікації персональних даних у внутрішніх інформаційних системах організацій або реалізації прав суб'єктів даних на доступ чи видалення інформації відповідно до вимог GDPR [118].

Водночас проблемний аспект впливу ШІ на приватність є також значущим. Характер функціонування алгоритмічних систем передбачає масове поглинання даних з різних джерел, часто без безпосередньої взаємодії із суб'єктами даних і без достатнього рівня прозорості щодо завдань і способів їх подальшого використання [25, с. 257; 130]. Через непрозорість таких алгоритмічних рішень виникає значна кількість неточностей та контраверсійностей під час обробки персональних даних: відсутність повного контролю людини за автоматизованою обробкою, ризики некоректного використання згоди суб'єкта даних і складнощі забезпечення принципів законності, пропорційності й мінімізації даних. Швидкість розвитку ШІ значно випереджає національне нормативне забезпечення, що створює правову невизначеність у питаннях відповідальності та захисту прав суб'єктів даних, про що буде йтися згодом [25, с. 258]. Такі практики автоматизованого збору інформації з відкритих інтернет-ресурсів і соціальних мереж знані як web-scraping (процес автоматичного збору інформації в мережі інтернет). Вони дедалі частіше стають предметом публічних дискусій та судових спорів. Резонансу це питання набуло у зв'язку з позовами до великих технологічних компаній, яких звинувачують у неправомірному використанні користувацького контенту для навчання моделей штучного інтелекту без належної згоди або ліцензійної підстави. Показовим у цьому сенсі є судовий спір між платформою Reddit і компанією

Anthropic, у межах якого поставлено під сумнів правомірність повторного використання публічно доступних даних для машинного навчання [117].

Правова охорона персональних даних відрізняється від їх правового захисту. Адже правова охорона персональних даних носить попереджувальний характер.

Правова охорона діє до вчинення правопорушення права. Її мета – створити такі правила й гарантії, які мають не допустити незаконної або ризикованої обробки персональних даних.

До правової охорони належать: правила обробки, принципи законності, прозорості, мінімізації даних, вимоги до безпеки, права суб'єкта даних, обов'язки володільців і розпорядників, обмеження щодо чутливих даних, оцінка ризиків. У сфері ШІ правова охорона має діяти ще раніше – не лише під час використання системи, а вже на етапі її проєктування, навчання, тестування і впровадження. Одним із ключових елементів сучасної методології правової охорони персональних даних у сфері застосування штучного інтелекту є принципи privacy by design та privacy by default.

Правовий захист, на відміну від правової охорони, має інше призначення. Він застосовується тоді, коли порушення вже відбулося або існує реальна загроза його настання. Наприклад, коли дані незаконно зібрані, використані, поширені, передані третім особам, використані для профілювання або автоматизованого рішення.

До засобів захисту належать: оскарження незаконної обробки, вимога про виправлення або видалення даних, припинення неправомірної обробки, обмеження доступу, відшкодування шкоди, притягнення винних осіб до відповідальності.

У сфері ШІ захист ускладняється. Особа часто не знає, які саме дані використані, як працював алгоритм, хто відповідає за результат, чому система сформувала саме такий висновок і як його оскаржити.

Отже, правова охорона і правовий захист персональних даних не є тотожними поняттями. Охорона має превентивний, попереджувальний

характер, а захист – реактивний характер і застосовується після порушення або при загрозі порушення. В ШІ це розмежування особливо важливе: алгоритмічна обробка може бути прихованою, складною, тривалою, а її наслідки можуть проявлятися не відразу.

Якщо розглядати персональні дані як ресурс життєвого циклу ШІ, вони використовуються: для формування навчальних наборів; під час навчання моделі; для тестування, перевірки точності, валідації результатів; після запуску системи дані можуть знову використовуватися для донавчання, корекції алгоритмічної поведінки або аудиту.

Тому ризик для особи виникає не лише в момент первинного збирання даних, а протягом усього життєвого циклу ШІ-системи.

Слід наголосити, що ШІ істотно змінює обробку персональних даних. Ці зміни є такими:

- збільшується обсяг даних, необхідних для роботи системи ШІ;

- дані можуть використовуватися повторно, зокрема для навчання або донавчання моделей;

- ускладнюється контроль за метою обробки, бо дані, зібрані для однієї мети, можуть надалі використовуватися в іншому алгоритмічному контексті;

- зростає ризик повторної ідентифікації, коли різні набори даних окремо не ідентифікують людину, але разом дозволяють встановити її особу;

- ШІ може формувати нові висновки про людину, навіть якщо вона прямо не надавала таких відомостей.

Сучасний ШІ пов’язаний із надмасивними обсягами інформації, тобто Big Data, а Big Data слід розглядати не лише як великі обсяги інформації, а як специфічний режим обробки, що характеризується різнорідністю, швидким оновленням і можливістю багаторазового поєднання різних джерел.

Доречним буде, на наш погляд, торкнутися поняття «інференційні персональні дані». Такі дані – це не ті відомості, які людина прямо надала про себе. Це висновки, оцінки, припущення, прогнози або профілі, які система формує на основі інших даних. Такі висновки можуть стосуватися

платоспроможності, поведінки, стану здоров'я, професійної придатності, рівня ризику, соціальних зв'язків або ймовірних дій осіб.

Головна проблема полягає у тому, що людина часто не знає про існування таких висновків. Вона не завжди може перевірити, чи ці висновки правильні, і не завжди має ефективний спосіб їх оскаржити. Саме тому інференційні дані треба розглядати як окремий об'єкт правової охорони і захисту у сфері ШІ.

Автоматизовані рішення, профілювання і людський контроль. Результат роботи ШІ може використовуватися для ухвалення рішень щодо людини. Це можуть бути рішення про кредит, роботу, соціальну допомогу, доступ до послуги, перевірку особи, безпекові заходи, правоохоронну аналітику. Персональні дані в таких випадках стають основою для оцінювання людини. Профілювання може впливати на можливості людини, навіть якщо формально рішення приймає не алгоритм, а орган чи компанія.

Головна проблема полягає у непрозорості алгоритмічного рішення. Тому особа повинна мати можливість дізнатися про автоматизоване рішення, зрозуміти його загальну логіку, висловити свою позицію, вимагати людського перегляду та оскаржити результат.

Біометричні дані як приклад впливу ШІ. Відомо, що біометричні дані пов'язані з унікальними фізіологічними або поведінковими ознаками людини, а системи ШІ можуть використовуватися для розпізнавання обличчя, голосу, ходи, відбитків, поведінкових характеристик тощо.

Такі системи можуть бути корисними для безпеки, ідентифікації, контролю доступу, правоохоронної діяльності. Водночас вони створюють підвищені ризики для приватності, бо стосуються унікальних характеристик людини. У правоохоронній сфері додатково виникають питання допустимості таких даних, точності алгоритмів, помилкової ідентифікації, судового контролю і незалежного аудиту.

Перехід до ризик-орієнтованого підходу.

Традиційна модель захисту персональних даних значною мірою ґрунтувалася на згоді особи, інформуванні, цільовому обмеженні й мінімізації даних. У системах ШІ людина часто не може наперед знати, як саме її дані будуть використані.

Дані можуть поєднуватися з іншими наборами, використовуватися повторно, застосовуватися для навчання або донавчання моделей. Алгоритм може сформувати висновки, яких людина прямо не надавала, тому регулювання має враховувати не лише факт згоди, а й рівень ризику. Основними критеріями ризику є характер даних, масштаб обробки, автономність системи, вплив на права людини, можливість дискримінації, непрозорість алгоритму й наявність людського контролю.

Детального аналізу потребує феномен «кризи згоди», який дедалі частіше розглядають у науковій літературі як системну проблему захисту персональних даних в умовах розвитку штучного інтелекту. Традиційна модель інформованої згоди ґрунтується на припущенні, що суб’єкт даних здатний усвідомлено оцінити обсяг і наслідки обробки своєї інформації. Проте в середовищі, де дані обробляють автоматизованими системами безперервно, у великих масштабах і з використанням складних алгоритмічних механізмів, таке припущення втрачає зв’язок із реальністю [127]. Обсяги та складність обробки унеможливлюють для пересічного користувача вичерпне розуміння того, на що саме він дає згоду, а повторне використання даних для нових, не передбачених спершу завдань лише посилює цю проблему.

Унаслідок цього постає ситуація, яку в доктрині описують як формальну законність без реального контролю з боку суб’єкта даних. Згода, надана в одному контексті, фактично поширюється на інші, не відомі особі сценарії використання її інформації, що створює ефект «законного беззаконня» з позицій матеріального захисту приватності [130]. Посилення вимог до форм згоди або підвищення санкцій за порушення законодавства про персональні дані не завжди призводить до реального підвищення рівня

захисту, а інколи лише формалізує відповідні процедури, не змінюючи суті відносин між суб'єктами даних і розробниками ШІ-систем [127].

У відповідь на ці виклики в міжнародних підходах до регулювання дедалі важливішими стають моделі, орієнтовані на управління ризиками, а не виключно на контроль з боку користувача. Такий підхід передбачає перенесення основної відповідальності за мінімізацію шкоди на розробників й операторів ШІ-систем незалежно від факту отримання згоди [103; 104]. Його закладено в рамкові документи OECD, а також у рекомендації Національного інституту стандартів і технологій США, які передбачають інтеграцію питань приватності безпосередньо в архітектуру алгоритмічних систем на етапах їх проєктування, упровадження та експлуатації [64, с. 19; 86, с. 10].

Складність у контексті застосування штучного інтелекту під час аналізу даних становить дотримання принципу мінімізації даних, який традиційно вважають одним із базових принципів правового режиму захисту персональної інформації. Відповідно до положень GDPR, персональні дані мають бути адекватними, релевантними й обмеженими тим, що є необхідним для досягнення конкретної мети обробки [118]. Однак у випадку ШІ-систем логіка їх функціонування суперечить цьому принципу. Алгоритмічні моделі, зокрема ґрунтовані на машинному та глибинному навчанні, демонструють вищу точність, стабільність й адаптивність за умови використання максимально широких і різноманітних масивів даних. На практиці це призводить до збору інформації «із запасом», коли розробники не можуть наперед визначити, які змінні виявляться критичними для навчання моделі, а які залишаться другорядними.

Цей парадокс між вимогою мінімізації та прагненням до підвищення ефективності ШІ є не лише технічною, а й глибоко правовою проблемою. Частина зібраних даних може виявитися чутливою, надмірною або такою, що не має прямого зв'язку з первинною метою обробки, однак її зберігання та аналіз розглядають як виправдані з погляду оптимізації алгоритмічної

роботи. Унаслідок цього складається ситуація, за якої формально задекларована мета обробки не відповідає реальному обсягу та характеру даних, які використовують, а це ставить під сумнів ефективність традиційних правових обмежень [14, с. 70]. З огляду на це, штучний інтелект не просто ускладнює застосування принципу мінімізації, а фактично змушує переглядати його зміст у світлі нових технологічних реалій.

Проблемним постає ще й вплив ШІ на сферу автоматизованого прийняття рішень і профілювання. Профілювання в правовому значенні охоплює будь-яку форму автоматизованої обробки персональних даних, спрямовану на оцінку особистих характеристик фізичної особи, зокрема її поведінки, інтересів, економічного становища або стану здоров'я. Системи штучного інтелекту здатні поєднувати різнорідні джерела інформації та формувати детальні цифрові профілі, які використовують для прогнозування подальших дій або прийняття рішень, що безпосередньо впливають на права та свободи людини [30; 130]. Складність становлять так звані інференційні дані, тобто висновки, сформовані алгоритмічними системами на основі аналізу інших відомостей.

Інференційні дані можуть формально не підпадати під класичне визначення персональних даних, оскільки вони не завжди безпосередньо ідентифікують особу, проте з практичної позиції такі дані часто дають змогу з високою точністю характеризувати конкретну людину, прогнозувати її поведінку або приписувати їй певні властивості. Наприклад, аналіз історії пошукових запитів і покупок може привести до висновків щодо політичних поглядів, релігійних переконань, стану здоров'я користувача, його особистих переживань чи навіть нещодавніх дій. Це порушує складне питання правового статусу інференційних висновків, зокрема питання права особи знати про їх існування, оскаржувати їх точність або дискримінаційний характер [48; 130].

Чинне європейське законодавство наразі лише частково реагує на ці виклики. GDPR закріплює право особи не бути підданою рішенню, що

ґрунтується виключно на автоматизованій обробці, однак не встановлює обов’язку повного висвітлення логіки формування всіх алгоритмічних оцінок. Унаслідок цього між формальними гарантіями та реальною прозорістю алгоритмічних процесів утворюється значний розрив. Саме тому в наукових і політичних дискусіях дедалі частіше порушують питання необхідності забезпечення пояснюваності ШІ-систем і зрозумілості їх рішень не лише для регуляторів, а й для суб’єктів даних [93, с. 6].

Відповіддю на ці проблеми стають комплексні міжнародні підходи до регулювання штучного інтелекту, які виходять за межі класичних моделей захисту приватності. Модернізована Конвенція Ради Європи 108+ розглядає захист персональних даних як динамічний процес, що має адаптуватися до розвитку технологій і враховувати ризики, пов’язані з автоматизованими рішеннями та профілюванням [102]. У межах такого підходу правове значення надають не лише окремим операціям з інформацією, а й загальному контексту функціонування алгоритмічних систем, зокрема рівню їх автономності, масштабам впливу й можливості людського контролю. Схожа логіка простежується і в документах OECD, де обробку персональних даних у системах штучного інтелекту розглядають як складову ширшої системи управління ризиками. Принципи та рекомендації OECD орієнтують регулювання на запобігання потенційній шкоді для прав людини, а не лише на формальне дотримання процедурних вимог [103; 104]. Це означає, що оцінювання правомірності обробки даних слід здійснювати з огляду на ймовірні соціальні наслідки використання ШІ, включно з ризиками дискримінації, маніпуляції поведінкою та інформаційної асиметрії [63, с. 92–95].

Практичне втілення такого підходу відображено в рамкових моделях управління ризиками, розроблених NIST, які пропонують інтегрувати питання приватності, безпеки й підзвітності безпосередньо в архітектуру ШІ-систем [64, с. 5; 86, с. 4]. Аналогічні орієнтири закріплено і в міжнародних стандартах, зокрема ISO/IEC 23894, який засвідчує необхідність системного

оцінювання ризиків для прав і свобод людини, з огляду на конкретний контекст використання штучного інтелекту [60, с. 12]. Для України додаткове значення мають рекомендаційні документи EU4Digital, спрямовані на адаптацію цих підходів до національних правових й інституційних умов [90, с. 43–46].

У сукупності окреслені положення констатують, що штучний інтелект істотно трансформує логіку обробки персональних даних, зміщуючи акцент з окремих дій з інформацією на архітектуру алгоритмічних процесів і наслідки їх функціонування. На відміну від традиційних інформаційних систем, у яких обсяг і мета обробки даних є порівняно стабільними й передбачуваними, ШІ-системи вирізняються динамічністю, здатністю до самонавчання та повторного використання результатів обробки в нових контекстах. Це ускладнює застосування класичних правових інструментів контролю, зокрема принципів цільового обмеження, мінімізації даних й інформованої згоди, які формувалися за умов значно простіших технологічних процесів [118; 130].

Водночас аналіз міжнародних підходів до регулювання ШІ демонструє тенденцію поступового відходу від виключно формального розуміння законності обробки персональних даних, натомість у фокусі уваги опиняється питання потенційної шкоди для прав і свобод людини, що може виникати внаслідок автономного функціонування алгоритмічних систем, їх масштабування та використання інференційних висновків.

Важливим аспектом також є те, що проблематика обробки персональних даних у сфері штучного інтелекту не зводиться виключно до юридичних або технічних аспектів, а має виразний етичний вимір, який дедалі частіше розглядають як самостійний критерій оцінювання допустимості використання алгоритмічних систем.

У сучасних дослідженнях акцентовано, що навіть формально правомірна обробка персональних даних може призводити до етично проблемних наслідків, якщо вона супроводжується непрозорими

алгоритмічними рішеннями, асиметрією інформації між розробником і користувачем або формуванням інференційних висновків, здатних впливати на соціальний статус, можливості чи поведінку особи [14, с. 73–74; 130]. У цьому контексті інструментом постає етика, вона заповнює ті прогалини, які об'єктивно виникають у ситуації швидкого розвитку технологій. Документи міжнародних організацій безпосередньо засвідчують необхідність орієнтованості систем штучного інтелекту на повагу до людської гідності, недопущення дискримінації та забезпечення справедливості, незалежно від того, чи всі відповідні ризики вже врегульовано на рівні позитивного права [65; 103]. Етична проблематика тісно пов'язана з питанням відповідальності. У разі автономного функціонування ШІ складно однозначно встановити, хто саме має нести моральну й соціальну відповідальність за наслідки обробки персональних даних: розробник алгоритму, постачальник даних (особа, дані якої збирають), розробник системи чи держава, що в теорії має поставати основним регулятором [63, с. 81–88]. Етичне напруження спричиняє ще й практика навчання моделей на великих масивах публічно доступної інформації, де формальна відкритість даних не завжди означає згоду суб'єктів на їх подальше алгоритмічне використання для реалізації завдань, що виходять за межі первинного контексту публікації [95; 117]. У цьому сенсі етичні принципи дедалі частіше застосовують як критерій оцінювання соціальної прийнятності технологічних рішень ще до моменту їх правової кваліфікації, що відображено як у рекомендаційних документах OECD, так і в підходах, закладених у рамкові моделі управління ризиками, де питання приватності, автономності людини та недопущення шкоди розглядають комплексно [64, с. 7; 86, с. 12–19; 104].

Надалі слід, на наш погляд, приділити увагу сучасному стану та перспективам наукових досліджень з цієї проблематики, основним доктринальним підходам українських і зарубіжних учених, аналізу наявної наукової полеміки.

Питання правового захисту персональних даних у сфері застосування технологій штучного інтелекту цікавило таких науковців, як І. Андрющенко, І. Арістова, Д. Арзянцева, В. Базалицький, Д. Бєлов, М. Бєлова, М. Бліхар, В. Брижко, І. Бухтіярова, Ф. Гакер, М. Дубняк, А. Енгель, О. Заярний, О. Золотар, О. Карапетян, О. Ковальова, А. Колесніков, О. Корнейко, Є. Остіян, О. Пунда, Г. Майкл, М. Маурер, В. Пилипчук, М. Погорецький, А. Радченко, Н. Савлієва, М. Співак, К. Токарєва, В. Хахановський, М. Швець та ін. Наявність значної кількості підходів зумовлює формування стійкої наукової полеміки, яка розгортається як щодо фундаментальних засад правового регулювання, так і щодо прикладних аспектів обробки персональних даних.

Ці та інші вчені займалися різними аспектами розглядуваної тематики. Перший напрямок досліджень – загальні питання інформаційного права, приватності та персональних даних. До нього можна віднести І. Арістову, І. Андрющенка, В. Брижка, І. Бухтіярову, О. Золотар, В. Пилипчука, М. Співак, М. Швеця та інших авторів, які досліджували базові питання інформаційного права, правової охорони персональних даних, інформаційної безпеки та захисту приватності.

Другий напрямок – цифровізація, штучний інтелект, автоматизовані рішення та інформаційні права. До нього можна віднести О. Заярного, М. Дубняк, А. Колеснікова, О. Карапетяна, О. Ковальову та інших авторів, які аналізували вплив цифрових технологій, автоматизованих систем, алгоритмічної обробки та штучного інтелекту на права людини.

Третій напрямок – біометричні технології, відеоспостереження, електронні докази та кримінально-процесуальний аспект. До нього можна віднести Д. Арзянцеву, М. Бліхар, М. Погорецького, О. Пунду, В. Хахановського та інших авторів, праці яких пов’язані з використанням цифрових технологій, біометричної ідентифікації, електронних доказів та інформаційних систем у правоохоронній діяльності.

Одним із показових прикладів того, наскільки складною може бути робота з цифровою інформацією у кримінальному процесі, є ситуація із

даними, здобутими із захищених месенджерів. Дослідження М. Погорецького, присвячене платформі EncroChat, показово ілюструє цю проблематику. У контексті даної роботи принципово важливим є не технічний бік здобуття таких даних, а та обставина, що будь-яка цифрова інформація, яка стосується конкретної особи, вимагає окремої оцінки – чи було її отримано законно, чи вона є допустимою, достовірною і чи не порушує права на справедливий розгляд справи. Якщо подібні дані стають предметом подальшої автоматизованої обробки, питання законності, допустимості та захисту прав особи набувають ще більшої гостроти - проте вже в контексті інших досліджень цього автора [170].

Четвертий напрям – зарубіжна доктрина щодо GDPR, AI Act, генеративного штучного інтелекту, великих мовних моделей, ChatGPT та алгоритмічної відповідальності. До нього можна віднести Ф. Гакера, А. Енгеля, М. Маурера, Г. Майкла та інших зарубіжних дослідників.

Наявність різних наукових підходів зумовлює формування наукової полеміки щодо того, чи достатньо адаптації чинного законодавства про захист персональних даних до умов штучного інтелекту, чи є необхідним створення спеціального правового режиму обробки персональних даних у системах ШІ.

При цьому у межах першої лінії полеміки порушується питання про те, чи здатне чинне законодавство про захист персональних даних бути адаптованим до умов функціонування ШІ-систем, чи все ж необхідним є формування спеціального правового режиму алгоритмічної обробки.

Друга лінія полеміки пов’язана зі співвідношенням безпекових інтересів держави та права особи на приватність, особливо у випадках використання біометричної ідентифікації, масового відеоспостереження та автоматизованого аналізу поведінки.

Третя лінія стосується балансу між інноваційним розвитком і посиленням контролю за алгоритмічними системами, зокрема через оцінку впливу, алгоритмічний аудит, право на пояснення та людське втручання.

Перші наукові роботи, присвячені штучному інтелекту в українському правовому дискурсі, зосереджувалися переважно на загальних питаннях його правового статусу, можливостей і ризиків використання, а також потенційного впливу на систему права загалом. У цьому контексті захист персональних даних розглядали як один із низки аспектів подальшого регулювання, а не як самостійну проблему, що потребує спеціального концептуального осмислення. Такий підхід був притаманний початковому етапу, коли штучний інтелект сприймали радше як перспективну технологію, ніж як чинник трансформації правових інститутів [44, с. 128–153]. Проте технології ШІ градуально розвивалися та поширювалися вглиб різних сфер, згодом у наукових дослідженнях сформувалося чіткіше усвідомлення того, що таке ШІ, яким є його вплив, що передбачає обробка персональних даних, причому є центральним елементом функціонування більшості сучасних систем штучного інтелекту. У працях українських авторів фокус уваги було зміщено з абстрактних міркувань про автоматизацію до аналізу конкретних ризиків, пов’язаних із масовим збором даних, профілюванням й алгоритмічним прийняттям рішень. Зокрема, акцентували на небезпеці алгоритмічної дискримінації, втраті контролю за подальшим використанням інформації та складності забезпечення ефективної анонімізації в умовах великих даних [14, с. 64–74; 31, с. 47–53]. У межах такого доктринального зсуву формується розуміння того, що класичні інструменти захисту персональних даних, зосереджені на формальних процедурах, не відповідають природі алгоритмічних систем. У науковій літературі аргументовано, що проблема полягає не лише у відсутності спеціальних норм, а й у зміні логіки обробки даних, яка стає багаторівневою, динамічною та часто не прозорою для суб’єкта даних. Це зумовлює потребу в переосмисленні традиційних правових категорій, таких як мінімізація даних, мета їх обробки та пропорційність втручання [72].

У доктринальних дослідженнях також увагу спрямовано на питанні автоматизованого прийняття рішень і профілювання. Українські науковці

зазначають, що чинне законодавство протягом тривалого часу не містило спеціальних гарантій щодо таких практик і відповідно не забезпечувало належного рівня захисту у випадках, коли рішення, що мають юридичні або фактичні наслідки для особи, їх ухвалюють без участі людини. У цьому контексті дедалі частіше порушують питання про необхідність закріплення права на пояснення алгоритмічного рішення та можливості його ефективного оскарження [93; 138, с. 15–18].

Тут варто звернутися до позиції М. Погорецького щодо місця штучного інтелекту в процесі доказування. З його підходу випливає, що результат автоматизованого аналізу даних сам по собі не може слугувати повноцінним доказом – без належної процесуальної перевірки він залишається лише вихідним матеріалом. Ключовими є питання про те, яким чином і на якій підставі отримані відповідні дані, чи можна відстежити їх походження, наскільки достовірним є отриманий результат і чи забезпечено судовий контроль за цим процесом. Для цієї дисертації такий підхід є значущим, оскільки біометричні та інші цифрові персональні дані, оброблені ШІ-системами, одночасно виступають і потенційним джерелом доказів, і об'єктом підвищеного правового захисту [171].

Важливим напрямом наукової дискусії стало й оцінювання ефективності механізмів знеособлення та анонімізації персональних даних у контексті машинного навчання. Дослідження засвідчують, що навіть за умови застосування класичних методів деперсоніфікації ризик повторної ідентифікації суттєво підвищується в разі комбінування різних наборів даних і використання статистичних закономірностей для відновлення індивідуальних характеристик [105]. Це поставило під сумнів звичне уявлення про анонімізацію як універсальний засіб виведення даних за межі правового регулювання. У зв’язку із цим у наукових працях дедалі активніше досліджують технології підвищення приватності, зокрема диференційної приватності, яку пропонують як один з інструментів зниження ризику розкриття інформації про конкретних осіб під час аналізу або навчання

моделей. Такі підходи розглядають не як альтернативу правовому регулюванню, а як його функціональне доповнення, що надає можливість перевести абстрактні принципи захисту даних у вимірювані технічні рішення [58].

Паралельно в національній доктрині відбувається переосмислення ролі згоди суб'єкта даних як ключового механізму легітимації обробки. В умовах складних алгоритмічних систем інформована згода дедалі частіше набуває формального характеру та не забезпечує реального контролю за подальшим використанням даних, а це зумовлює перехід до підходів, які покладають більшу відповідальність на володільців і розробників систем, а не на інформаційно слабшого користувача [127].

Розвиток наукової думки в Україні щодо захисту персональних даних у сфері штучного інтелекту вирізняється поступовим переходом від фрагментарних і загальних міркувань до комплексного та ризик-орієнтованого підходу (виявлення, оцінювання та мінімізація потенційних загроз і використання можливостей). Хоча національна доктрина ще не сформувала єдиної усталеної концепції, наявні дослідження заклали підґрунтя для подальшого реформування законодавства та вплинули на формування порядку денного у сфері державної політики щодо регулювання штучного інтелекту [26, с. 310–315].

Щодо перспектив наукових досліджень в сфері правових проблем ШІ, можна передбачити, що такі дослідження будуть одним із найдинамічніших та найактуальніших напрямів сучасної юридичної науки. Вони включатимуть:

- розробку моделі алгоритмічної відповідальності – методології розподілу відповідальності за шкоду, завдану автономними системами (хто має відповідати: розробник алгоритму, власник системи чи оператор);

- визначення правового статусу нейромереж – включає дослідження меж правосуб'єктності автономних систем, пошук балансу між наданням ШІ функціонального статусу та збереженням етично-правових стандартів;

- захист авторських прав та прав інтелектуальної власності – включає вирішення проблем авторського права на твори та винаходи, створені за допомогою генеративного ШІ;

- розроблення правових засад інтеграції ШІ у систему правосуддя та судочинства – включає оцінку ризиків та перспектив автоматизації юридичної діяльності, використання аналітичних інструментів для суддів та дослідження допустимості доказів, згенерованих системами ШІ;

- вивчення питань конфіденційності, алгоритмічної дискримінації, маніпуляцій поведінкою та захисту персональних даних відповідно до європейських стандартів, зокрема вимог Artificial Intelligence Act [122].

1.2. Правове забезпечення захисту персональних даних у сфері застосування систем штучного інтелекту

Слід зазначити, що проблема правового регулювання та розвитку охорони та захисту персональних даних у сфері штучного інтелекту в Україні нині перебуває у стані переосмислення.

У межах цього підрозділу доцільно послідовно розглянути генезу правового регулювання захисту персональних даних в Україні, проблеми чинного законодавства та авторське бачення подальшого розвитку правової охорони і захисту персональних даних у сфері штучного інтелекту.

Правове регулювання захисту персональних даних в нашій країні відбувається у всіх галузях права та охоплює низку нормативно-правових актів. На наш погляд, доцільно стисло розглянути ці документи.

Так, уже згаданий Закон України «Про захист персональних даних» є базовим актом у цій сфері – він закріплює загальні засади обробки персональних даних, права суб'єкта даних та обов'язки володільців і розпорядників [36]. Попри широке розуміння персональних даних, на якому ґрунтується цей Закон, він орієнтований на класичну модель обробки

інформації й не передбачає спеціальних гарантій щодо алгоритмічних систем, автоматизованого прийняття рішень та інференційних даних. Саме це й зумовлює потребу в адаптації базового регулювання до умов застосування ШІ, де алгоритми здатні поєднувати різнорідні масиви даних і формувати нові висновки про особу.

Закон України «Про доступ до публічної інформації» відіграє ключову роль у правовому забезпеченні захисту персональних даних при використанні систем ШІ, оскільки допомагає визначити межу між загальною доступністю інформації та потребою в охороні приватного життя особи. Ст. 6 цього Закону окреслює умови, за яких доступ до інформації може бути обмежений, а саме, коли її розповсюдження може зашкодити правам та законним інтересам фізичної особи. Таким чином, зазначений Закон підтримує систему захисту персональних даних [139].

Закон України «Про електронну ідентифікацію та електронні довірчі послуги» стосується розглядуваної теми, оскільки встановлює правила взаємодії, що стосуються електронного підтвердження особи, застосування електронного підпису та інших цифрових методів верифікації. У сфері ШІ цей Закон є актуальним насамперед тому, що електронна ідентифікація практично завжди включає опрацювання персональних даних. Однак, Закон не передбачає специфічних норм щодо використання ШІ в процесах електронної ідентифікації [140].

Єдиний державний демографічний реєстр та документи, що посвідчують громадянство України, особу чи її особливий статус, відіграють ключову роль у правовому захисті персональної інформації. Це зумовлено тим, що законодавство регламентує формування та функціонування державного реєстру, де акумулюються дані, що ідентифікують особу, включно з біометричними. В контексті розвитку ШІ особливої уваги заслуговує аспект, що згадані дані можуть бути застосовані не лише для виготовлення документів чи верифікації особи, а також потенційно – для автоматизованої ідентифікації, підтвердження автентичності, розпізнавання

обличчя та в інших технологічних процесах. Саме тому зазначений Закон має неабияке значення для дисертаційного дослідження [141].

Закон України «Про захист інформації в інформаційно-комунікаційних системах» має значення в частині технічного та організаційного забезпечення безпеки інформації, яка обробляється в автоматизованих системах. У сфері застосування ШІ персональні дані обробляються саме в таких системах, тому їх захист не може зводитися лише до юридичної заборони незаконного використання [142].

Закон України «Про основні засади забезпечення кібербезпеки України» є важливим для аналізу, оскільки ефективне збереження особистої інформації у сфері ШІ неможливе без належного рівня кіберзахисту. Системи ШІ працюють у цифровій сфері, де особисті відомості можуть зазнати несанкціонованого доступу, витоку, спотворення або бути використаними для атак на інформаційні мережі. У цій ситуації кібербезпека стає не тільки технічною передумовою, але й частиною правового захисту персональних даних [143].

Далі розглянемо в контексті цієї праці галузеві кодекси України.

Один із засобів правового реагування на порушення законодавства про захист персональних даних міститься в Кодексі України про адміністративні правопорушення. Найбільш релевантною є стаття 188-39 КУпАП, яка встановлює адміністративну відповідальність за недотримання вимог щодо захисту персональних даних. У контексті нашого дослідження, цю норму слід розглядати як складову частину системи правового захисту, що означає реакцію держави на неправомірне опрацювання або неналежне виконання обов’язків у сфері персональних даних [144].

Низка статей Кримінального кодексу України мають значення в контексті роботи. Зокрема, стаття 145 «Незаконне розголошення лікарської таємниці» має значення для захисту персональних даних у сфері ШІ в частині охорони медичної інформації як особливо чутливої категорії даних. Стаття 163 «Порушення таємниці листування, телефонних розмов, телеграфної чи

іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер» є важливою для дослідження, оскільки охороняє приватність комунікацій особи, у тому числі тих, що передаються через комп'ютер. У сфері ШІ ця норма має значення у випадках, коли алгоритмічні системи можуть використовуватися для автоматизованого аналізу електронного листування, повідомлень, голосових розмов, метаданих або іншої цифрової комунікації. Стаття 168 «Розголошення таємниці усиновлення (удочеріння)» передбачає відповідальність за розголошення таємниці усиновлення всупереч волі усиновителя. Для теми захисту персональних даних ця норма має значення як приклад кримінально-правової охорони окремої категорії особливо чутливої інформації про сімейний і правовий статус особи. Стаття 182 «Порушення недоторканності приватного життя» є основною кримінально-правовою нормою у сфері захисту персональних даних, оскільки передбачає відповідальність за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконну зміну такої інформації. Стаття 231 «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю», відіграє допоміжну роль у дослідженні захисту персональних даних у контексті ШІ [145].

Стаття 361 КК України «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж» відіграє значну роль у забезпеченні безпеки персональних даних у системах ШІ, адже системи ШІ діють саме в межах таких інформаційних, автоматизованих та інформаційно-комунікаційних систем. Стаття 361^1 «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів» має безпосереднє відношення до нашої теми. Вона охоплює боротьбу з розробкою та розповсюдженням шкідливого програмного забезпечення та технічних пристроїв, що можуть бути використані для несанкціонованого проникнення

в інформаційні системи. Стаття 361[2] «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації» є однією з найбільш релевантних до питань захисту персональної інформації в цифровій сфері. Стаття 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї» набуває особливого значення під час аналізу захисту персональних даних у контексті ШІ, адже це не зовнішні загрози, а незаконні дії осіб, які мають законний доступ до інформації. У сфері ШІ така норма може бути застосована до ситуацій, коли відбувається несанкціоноване копіювання, модифікація, блокування чи витік персональних даних, що використовуються для навчання або функціонування алгоритмічних систем. Стаття 363 «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється» має значення для правового забезпечення захисту персональних даних у випадках, коли шкода виникає через порушення правил експлуатації систем або правил захисту інформації. У сфері ШІ це може стосуватися неналежного адміністрування систем, слабкого контролю доступу, порушення вимог інформаційної безпеки, неправильної організації зберігання наборів даних або відсутності належних технічних заходів захисту. Стаття 363[1] КК України «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку» має допоміжне значення для теми дослідження, оскільки спрямована на захист стабільної роботи автоматизованих систем і комп'ютерних мереж [145].

Отже, КК України не містить спеціальних норм, які б прямо врегульовували застосування ШІ чи відповідальність за порушення прав особи в результаті алгоритмічної обробки персональної інформації. Водночас певні його пункти формують систему кримінально-правового захисту приватності, конфіденційної інформації, медичних відомостей, таємниці зв'язку, інформації з обмеженим доступом, а також даних, що обробляються в автоматизованих системах. Проте, ці норми створювалися без урахування особливостей ШІ, тому не повністю охоплюють сфери, такі як: персональні дані, отримані шляхом виведення (інференції), автоматизоване створення профілів, повторна ідентифікація знеособлених даних, алгоритмічна дискримінація, неправомірне навчання моделей на персональних даних, а також відповідальність за збитки, спричинені автоматизованими рішеннями.

Цивільний кодекс України має важливе значення для правового забезпечення захисту персональних даних у сфері застосування систем ШІ, оскільки закріплює особисті немайнові права фізичної особи та способи їх судового захисту. Зокрема, це статті 277, 285, 286, 301, 302, 306, 307, 308 ЦК України [146].

Отже, Цивільний кодекс України не є спеціальним актом у сфері ШІ або персональних даних, однак його положення формують важливу приватно-правову основу захисту особи від неправомірної обробки інформації про неї. У сфері застосування систем ШІ ці положення можуть використовуватися для захисту особи від незаконного збору даних, прихованого профілювання, помилкових алгоритмічних висновків, неправомірного використання зображення чи біометричних даних, а також для компенсації шкоди, завданої автоматизованим рішенням. Водночас ЦК України не містить спеціальних норм щодо інференційних персональних даних, алгоритмічного аудиту, людського втручання та розподілу відповідальності між учасниками життєвого циклу ШІ-системи, що свідчить про потребу подальшого оновлення цивільно-правових механізмів захисту приватності.

У травні 2025 р. розпорядженням Кабінету Міністрів був затверджений План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025–2026 роки [147]. Це свідчить про поступовий перехід державної політики у сфері ШІ до практичних кроків. Для дисертаційного дослідження цей документ є важливим тому, що підтверджує наявність потреби у подальшому нормативному оформленні сфери штучного інтелекту. Водночас план заходів не встановлює самостійного правового режиму обробки персональних даних у системах ШІ, а лише визначає напрями подальших дій держави. Тому його можна розглядати як доказ того, що українське законодавство перебуває на етапі формування спеціального регулювання ШІ.

Закон України «Про Єдиний державний реєстр призовників, військовозобов'язаних та резервістів» має особливе значення для дослідження, оскільки регулює функціонування одного з найбільш чутливих державних реєстрів, у якому зосереджуються персональні та службові дані значної кількості громадян. У контексті застосування систем ШІ цей Реєстр є показовим прикладом державного масиву даних, який може використовуватися для автоматизованої перевірки, аналітики, актуалізації відомостей, міжреєстрового обміну та прийняття управлінських рішень. Саме тому законодавче регулювання такого Реєстру має розглядатися не лише як питання військового обліку, а і як складова правового забезпечення захисту персональних даних у цифровій державі [148].

Основи законодавства України про охорону здоров'я є важливим джерелом для аналізу правового забезпечення захисту персональних даних у сфері ШІ, оскільки медична інформація належить до найбільш чутливих категорій даних. Для теми дослідження це має особливе значення, оскільки медичні дані можуть використовуватися в діагностичних, аналітичних і прогнозних ШІ-системах, а отже, створюють підвищені ризики для приватності особи [149].

Податковий кодекс України також є дотичним до правового забезпечення захисту персональних даних, оскільки у статті 70 передбачено

функціонування Державного реєстру фізичних осіб – платників податків. У контексті систем штучного інтелекту такі дані можуть мати значення для автоматизованої аналітики, оцінювання фінансової поведінки, виявлення ризиків або формування цифрового профілю особи [150].

Закон України «Про державну реєстрацію актів цивільного стану» має значення для дослідження як акт, що регулює облік базових юридично значущих відомостей про фізичну особу (про народження, походження, шлюб, розірвання шлюбу, зміну імені та смерть особи). У контексті застосування ШІ такі відомості можуть бути використані для автоматизованої верифікації, зіставлення даних у різних реєстрах, виявлення невідповідностей або формування цифрового профілю особи [151].

Закон України «Про Національну програму інформатизації» має значення для дослідження у тій частині, що він стосується формування та розвитку інформаційної інфраструктури держави. У контексті ШІ цей Закон можна розглядати як один із актів, що створює організаційне підґрунтя для накопичення, обміну й використання значних обсягів інформації в державному секторі. Його значення полягає у формуванні загальної державної політики інформатизації [152].

Закон України «Про публічні електронні реєстри» є одним із найбільш важливих актів для аналізу великих масивів даних у державному секторі. У контексті застосування ШІ Закон має особливе значення, оскільки реєстрові дані можуть стати основою для навчання або функціонування алгоритмічних систем [153].

Закон України «Про хмарні послуги» має значення для теми великих масивів даних, оскільки сучасна обробка Big Data часто здійснюється не на локальних серверах, а за допомогою хмарної інфраструктури. У сфері ШІ така інфраструктура фактично є технічною основою для навчання моделей, обробки великих наборів даних і масштабування цифрових сервісів [154].

Постанова Кабінету Міністрів України № 835 має безпосереднє значення для аналізу великих масивів даних, оскільки регулює питання

оприлюднення, оновлення та використання наборів даних у формі відкритих даних. У контексті ШІ відкриті дані можуть використовуватися для аналітики, машинного навчання, побудови прогнозних моделей та ін. [155].

Виборчий кодекс України є дотичним до правового забезпечення захисту персональних даних у сфері застосування систем ШІ, оскільки виборчий процес пов'язаний з обробкою значних масивів персональних даних виборців, кандидатів, членів виборчих комісій та ін. [156].

Господарський процесуальний кодекс України має значення для теми дослідження в частині регулювання електронних доказів. У господарських спорах дедалі частіше можуть використовуватися цифрові документи, електронне листування, вебсторінки, метадані, бази даних, результати автоматизованої обробки інформації та інші електронні матеріали. У сфері ШІ це важливо тому, що результати роботи алгоритмічних систем можуть бути використані як докази у спорах між суб'єктами господарювання [157].

Кодекс адміністративного судочинства України є важливим для захисту персональних даних у сфері застосування систем ШІ, оскільки саме в порядку адміністративного судочинства особа може оскаржувати рішення, дії або бездіяльність суб'єктів владних повноважень. У контексті ШІ це дозволяє розглядати цифрові сліди, записи з інформаційних систем і результати автоматизованої обробки як потенційні докази [158].

Кримінальний процесуальний кодекс України має особливе значення для захисту персональних даних, оскільки кримінальне провадження часто пов'язане з отриманням, зберіганням, аналізом і використанням чутливої інформації про особу. У Кодексі серед загальних засад кримінального провадження закріплено таємницю спілкування та невтручання у приватне життя. Також передбачено, що інформація про приватне життя особи, отримана в порядку кримінального провадження, не може використовуватися інакше як для виконання його завдань. Особливе значення має також регулювання тимчасового доступу до речей і документів. У сфері ШІ це важливо для випадків використання цифрових доказів, відеоаналітики,

біометричної ідентифікації, аналізу телефонних з’єднань, електронних повідомлень або даних з інформаційних систем [159].

У сфері правоохоронної та безпекової діяльності цифрові інструменти дедалі активніше залучаються для збору, зіставлення й аналізу інформації, що може нести доказову або орієнтовну цінність. Досліджуючи використання цифрових технологій у справах, пов'язаних зі злочинами проти національної безпеки України, М. Погорецький наголошує: подібні практики мають бути узгоджені з процесуальними гарантіями та стандартами, прийнятими на рівні ЄС. Для галузі захисту персональних даних це має пряме значення: залучення цифрових слідів, системних даних чи результатів автоматизованого аналізу повинне передбачати чітко визначену мету обробки, встановлені межі, регламентований порядок доступу та дієві механізми контролю [172].

Кримінально-виконавчий кодекс України передбачає функціонування автоматизованої електронної бази даних – Єдиного реєстру осіб, засуджених за злочини проти статевої свободи та статевої недоторканості малолітньої особи. У контексті ШІ ця норма є особливою, оскільки йдеться про централізовану автоматизовану базу даних, яка містить вкрай чутливу інформацію про кримінально-правовий статус особи [160].

Митний кодекс України є важливим для аналізу великих масивів персональних даних у державному секторі. У сфері ШІ дані можуть використовуватися для автоматизованого аналізу ризиків, виявлення порушень митних правил, прогнозування переміщення товарів або оцінки поведінки суб’єктів зовнішньоекономічної діяльності [161].

Сімейний кодекс України має значення для захисту окремих категорій чутливої інформації про особу, насамперед відомостей про усиновлення. У контексті ШІ ці положення мають значення через ризик непрямого встановлення сімейних обставин особи шляхом поєднання даних з різних реєстрів, судових рішень, відкритих джерел або електронних баз [162].

Цивільний процесуальний кодекс України є важливим в частині судового захисту прав особи та використання електронних доказів. У контексті ШІ такі докази можуть включати результати автоматизованого аналізу, логи системи, цифрові профілі або дані, використані алгоритмом [163].

Закон України «Про електронні документи та електронний документообіг» регулює електронні документи, електронний документообіг і процеси створення, оброблення, передавання, зберігання, використання та знищення електронних документів. Для ШІ це важливо в частині електронних доказів, цифрових документів, автоматизованої обробки та даних у електронній формі [164].

Закон України «Про електронні комунікації» важливий через комунікаційні дані, метадані, електронні повідомлення, цифрову інфраструктуру і приватність комунікацій [165].

У контексті дослідження варто згадати також закони України: «Про Національну поліцію» [166]; «Про оперативно-розшукову діяльність» [167]; «Про Державний реєстр виборців» [168]; «Про медіа» [169] тощо.

Генеза розвитку правової охорони і захисту персональних даних у сфері штучного інтелекту (ШІ) в Україні відображає еволюційний перехід від базового захисту загальної інформації про особу до спроб формування комплексного, проактивного регулювання обробки великих масивів даних (Big Data) алгоритмічними системами. Цей процес розвивається під потужним впливом євроінтеграційних зобов’язань України та стандартів Європейського Союзу. Цей процес не зводиться до формального оновлення окремих норм, оскільки він розгортається на тлі швидкої зміни технологічних практик, трансформації уявлень про роль даних у суспільстві й перегляду класичних підходів до охорони приватності. Саме тому аналіз генези національного законодавства потребує не лише хронологічного викладу, а й виявлення тих концептуальних обмежень, у межах яких формувалася українська модель захисту персональних даних.

Генезу правової охорони і захисту персональних даних у сфері штучного інтелекту в Україні доцільно розглядати через кілька взаємопов'язаних етапів.

Перший етап – загальноінформаційний, коли захист персональних даних забезпечувався через загальні норми про інформацію, приватність, недоторканність особистого життя та конституційні гарантії прав людини.

Другий етап – пов'язаний із прийняттям Закону України «Про захист персональних даних» 2010 року, яким персональні дані були оформлені як самостійний предмет правового регулювання. Цей Закон орієнтувався на вимоги Конвенції Ради Європи № 108 та регулював традиційні бази даних, містив лише загальну заборону на прийняття рішень виключно на основі автоматизованої обробки без згоди особи. За змістом Закон 2010 року відтворював класичну модель захисту персональних даних, притаманну європейському праву кінця XX – початку XXI ст., сформовану під впливом директивного підходу Європейського Союзу [44, с. 148–153].

Третій етап – охоплює організаційно-корекційні зміни 2012–2013 років, спрямовані на спрощення адміністративних процедур та зміну моделі нагляду. Зміни до законодавства, внесені протягом цих років, були спрямовані переважно на організаційне коригування вже наявної моделі [1; 21, с. 1–13]. Скасування обов'язкової державної реєстрації баз персональних даних і передання наглядових повноважень Уповноваженому Верховної Ради України з прав людини мали на меті спростити адміністративні процедури й наблизити національну практику до європейської. Водночас ці зміни не стосувалися глибинної логіки регулювання та не переосмислювали його з огляду на майбутні технологічні виклики.

Четвертий етап – пов'язаний із цифровізацією, поширенням Big Data, платформних сервісів, профілювання та автоматизованого прийняття рішень, що виявило обмеженість традиційної моделі захисту персональних даних. У грудні 2020 р. затверджено Концепцію розвитку штучного інтелекту в Україні. 2022 рік: реєстрація євроінтеграційного законопроєкту № 8153 «Про

захист персональних даних». Його норми спрямовані на адаптацію українського права до GDPR та встановлення жорсткіших правил для профайлінгу й автоматизованого ухвалення рішень, що є критично важливим для роботи алгоритмів ШІ. Жовтень 2023 року: Міністерство цифрової трансформації України оприлюднило дорожню карту з регулювання ШІ, обравши підхід «м'якого регулювання» (soft law) на перших етапах, щоб не обмежувати розвиток інновацій під час воєнного стану.

П'ятий, сучасний етап – формується під впливом європейських стандартів GDPR, AI Act, Конвенції 108+, а також законопроєкту № 8153, які актуалізують потребу у спеціальному регулюванні обробки персональних даних у системах штучного інтелекту.

Перелом у сприйнятті національного законодавства відбувся одночасно з поширенням цифрових платформ, великих даних і систем машинного навчання, що активно аналізують у сучасній правовій та міждисциплінарній літературі [14, с. 64–74; 130]. Персональні дані дедалі частіше стали використовувати не лише як об'єкт зберігання, а як ресурс для побудови моделей, прогнозування поведінки й автоматизованого прийняття рішень.

Саме тоді в українській науковій думці починає формуватися критичне ставлення до чинної моделі захисту персональних даних. У наукових працях акцентували на тому, що формальна відповідність базовим європейським стандартам ще не гарантує ефективного захисту прав людини в умовах цифрової економіки, де обробка даних набуває масштабного, багатоцільового та часто непрозорого характеру. Чинна нормативна конструкція не була розрахована на сценарії повторного використання даних, комбінування різнорідних масивів і формування інференційних висновків, які можуть мати істотний вплив на правове становище особи [14, с. 64–74; 31].

На цій підставі питання зміни ролі персональних даних у правовому регулюванні стало вкрай актуальним. Якщо на початковому етапі розвитку національного законодавства персональні дані сприймали передусім як об'єкт охорони, що потребує захисту від несанкціонованого доступу або

розголошення, то внаслідок поширення алгоритмічних систем вони поступово перетворюються на активний елемент цифрової інфраструктури. Оскільки дані не є статичними, їх уже використовують для навчання моделей, оптимізації процесів, прогнозування поведінки та прийняття рішень, що виходить за межі класичного уявлення про їх фіксований характер. Така трансформація зумовлює необхідність перегляду традиційних правових інструментів, зокрема концепції згоди як центрального механізму легітимації обробки персональних даних. У наукових дискусіях дедалі частіше зауважують, що в умовах складних алгоритмічних екосистем інформована згода не завжди забезпечує реальний контроль суб'єкта за подальшим використанням його даних, а пов'язано це з інформаційною асиметрією між суб'єктом даних й оператором системи, об'єктивною неможливістю передбачити всі подальші сценарії обробки на етапі первинного збору інформації [127, с. 171–182]. Зазначені міркування безпосередньо впливають на розуміння конкретно генези правового регулювання захисту персональних даних в Україні, адже вони сприяють зміщенню акценту з формально-процедурної моделі контролю до ризик-орієнтованого підходу, у межах якого вирішальне значення мають не лише наявність правової підстави, а й оцінювання потенційної шкоди для прав і свобод людини. Такий підхід відповідає загальним тенденціям розвитку європейського права про захист даних і створює підґрунтя для подальшого реформування національного законодавства України в цьому питанні.

На ранніх етапах розвитку українського законодавства питання автоматизованого прийняття рішень і профілювання не були предметом правозастосовної практики. Лише після появи платформних сервісів, систем скорингу й алгоритмічного аналізу поведінки користувачів проблему автоматизованих рішень стали розглядати як таку, що має безпосередні правові наслідки для суб'єктів даних [130]. Отже, еволюція національного законодавства про захист персональних даних до появи спеціальних ініціатив у сфері штучного інтелекту характеризується поступовим накопиченням

концептуальних джерел і можливих питань. Формально стабільна нормативна модель дедалі більше суперечила реальним практикам обробки даних, що й зумовило необхідність її подальшого переосмислення в контексті розвитку алгоритмічних технологій. Ці міркування заклали підґрунтя для подальшого переосмислення генези правового регулювання захисту персональних даних в умовах розвитку штучного інтелекту.

Узагальнення генези правового регулювання, стану наукового дослідження та наукової полеміки дає підстави виокремити основні проблеми сучасної моделі правової охорони і захисту персональних даних у сфері штучного інтелекту в Україні.

До таких проблем належать:

- відсутність спеціального правового режиму обробки персональних даних у системах штучного інтелекту;

- відсутність законодавчого визначення інференційних персональних даних;

- недостатнє регулювання автоматизованого прийняття рішень і профілювання;

- відсутність повноцінного алгоритмічного аудиту високоризикових ШІ-систем;

- слабкість інституційного нагляду у сфері захисту персональних даних;

- недостатня врегульованість біометричної ідентифікації, зокрема розпізнавання обличчя, голосу, ходи та поведінкової біометрії;

- невизначеність моделі алгоритмічної відповідальності між розробником, постачальником, оператором, користувачем ШІ-системи та володільцем персональних даних;

- недостатнє поєднання правових, технічних, організаційних та етичних гарантій захисту персональних даних».

На нашу думку, подальший розвиток правової охорони і захисту персональних даних у сфері штучного інтелекту в Україні має ґрунтуватися

не на механічному копіюванні європейських моделей, а на поєднанні загальних принципів захисту персональних даних із спеціальними гарантіями для алгоритмічної обробки.

Такими гарантіями мають стати:

1. Законодавче закріплення поняття інференційних персональних даних;

2. Визначення високоризикової обробки персональних даних із використанням штучного інтелекту;

3. Запровадження обов'язкової оцінки впливу на захист персональних даних для високоризикових ШІ-систем;

4. Нормативне закріплення права особи на пояснення автоматизованого рішення;

5. Закріплення права на людське втручання або перегляд автоматизованого рішення людиною;

6. Запровадження алгоритмічного аудиту;

7. Спеціальне регулювання біометричної ідентифікації;

8. Розмежування відповідальності між розробником, постачальником, оператором, користувачем ШІ-системи та володільцем персональних даних.

Важливим етапом генези правового регулювання захисту персональних даних у сфері штучного інтелекту є формування світових і європейських тенденцій, які поступово набули нормативного, доктринального та практичного оформлення. Саме в цьому просторі відбувалося концептуальне переосмислення приватності як правової цінності в умовах цифровізації, що згодом істотно вплинуло на національні правопорядки, зокрема й український. Початково міжнародний дискурс у сфері захисту персональних даних розвивався поза безпосереднім зв'язком зі штучним інтелектом. Увагу було зосереджено передусім на контролі за обігом інформації, захисті від несанкціонованого доступу та забезпеченні прозорості базових операцій з даними. Однак після поширення великих даних й алгоритмічних методів аналізу стало очевидно, що традиційні підходи не враховують якісної зміни

характеру обробки інформації. Персональні дані дедалі рідше використовують ізольовано, вони частіше стають елементом складних систем.

У європейському праві було зафіксовано необхідність переходу від формального контролю до змістового управління ризиками. Загальний регламент про захист даних (тобто GDPR) став певного роду концептуальним переломом у підході до приватності. Його значення полягає не стільки в переліку прав суб'єкта даних, скільки в упровадженні принципу відповідальності володільця даних, який зобов'язаний не просто дотримуватися вимог, а й бути здатним довести таке дотримання [118]. Саме GDPR уперше системно закріпив ідею ризик-орієнтованого підходу, що має безпосереднє значення для систем штучного інтелекту. Хоча термін «штучний інтелект» у тексті Регламенту не використано, його положення охоплюють ключові аспекти алгоритмічної обробки даних, зокрема автоматизоване прийняття рішень і профілювання. Встановлення спеціальних гарантій у таких випадках відображає розуміння того, що шкода для прав і свобод людини може виникати не на етапі збору даних, а внаслідок інтерпретації та використання результатів алгоритмічного аналізу [138, с. 20–25].

Подальший розвиток європейського підходу був зумовлений усвідомленням того, що GDPR не вичерпує всіх регуляторних потреб у сфері штучного інтелекту. Це призвело до формування окремої нормативної рамки, Регламенту про штучний інтелект (AI Act), який доповнює правила захисту персональних даних. Його ключовою особливістю є класифікація AI-систем за рівнем ризику та встановлення спеціальних вимог до високоризикових застосувань, зокрема в частині управління даними, забезпечення людського нагляду й безпеки [93, с. 1–6; 124].

Слід зауважити, що AI Act фактично інституціоналізує зв'язок між захистом персональних даних і безпекою алгоритмічних систем. Дані розглядають не лише як об'єкт приватності, а як фактор, що безпосередньо впливає на надійність, недискримінаційність і передбачуваність

функціонування ШІ. Такий підхід відображає ширшу тенденцію європейського права до інтеграції прав людини в технічне регулювання цифрових технологій.

Паралельно з нормативним розвитком істотну роль відіграють позиції та тлумачні документи європейських регуляторних органів. Рекомендації та висновки Європейської ради з питань захисту даних і Європейського наглядового органу з питань захисту даних формують практичні орієнтири застосування GDPR до сценаріїв машинного навчання та генеративних моделей. У цих документах зазначено, що використання складних алгоритмів не звільняє володільців даних від обов'язків щодо законності, мінімізації та прозорості обробки, навіть якщо реалізація цих принципів потребує нових технічних рішень [61; 106].

З огляду на те, що ШІ в правовій системі повинен мати етичне підґрунтя, значення набувають і ширші міжнародні рамки. Документи Організації економічного співробітництва та розвитку, ЮНЕСКО, а також підходи, закладені в рекомендаціях щодо відповідального використання ШІ, засвідчують пріоритет прав людини, справедливості й недискримінації. У цих актах приватність розглядають як умову збереження автономії особи в цифровому середовищі, а не як другорядне обмеження інновацій [103; 116].

У міжнародному дискурсі увагу також зосереджено на проблемі ефективності знеособлення даних. Дослідження засвідчують, що в умовах великих даних класичні підходи до анонімізації часто не забезпечують належного рівня захисту, оскільки комбінування наборів і статистичні методи надають можливість відновлювати персональні характеристики з високою точністю [105]. Це зумовило інтерес до технологій підвищення приватності, зокрема диференційної приватності, яку поступово визнають не лише технічним, а й регуляторно значущим інструментом [58].

Світові тенденції демонструють зсув від індивідуалізованої моделі захисту до врахування колективних ефектів алгоритмічної обробки. Наприклад, у межах концепції data justice (про що детально йтиметься

згодом) акцентовано, що шкода може виникати на рівні груп і соціальних категорій, навіть якщо формально права окремих суб'єктів даних не порушено. Це ставить під сумнів достатність традиційних правових механізмів і стимулює пошук нових форм регуляторного втручання [131].

Розвиток правового регулювання у сфері захисту персональних даних, пов'язаного з використанням ШІ, відбувається в напрямі ускладнення регуляторної логіки. Якщо раніше право прагнуло контролювати окремі операції з даними, то нині основну увагу приділено системним ризикам, які супроводжують увесь життєвий цикл алгоритмічної системи. Така зміна підходу формує підґрунтя для впливу міжнародних стандартів і практик на національне законодавство, у тому числі українське. Помітно й те, що регуляторна відповідь на проблеми ШІ не обмежується ухваленням обов'язкових нормативних актів. Значну роль відіграють інструменти «м'якого права» – рекомендації, керівні принципи, рамкові документи, які прямої юридичної сили не мають, проте задають стандарти належної практики. У сфері захисту персональних даних вони дають змогу швидко реагувати на технологічні зміни та заповнювати прогалини, що виникають через розрив між темпами інновацій і темпами правотворення.

Показовою є активна діяльність європейських регуляторних органів, які через висновки й орієнтаційні документи фактично конкретизують застосування загальних принципів GDPR до нових сценаріїв використання штучного інтелекту. Такі документи деталізують вимоги до законності обробки даних для навчання моделей, допустимості повторного використання наборів даних, а також меж застосування прав суб'єктів даних у випадках, коли обробка має високий рівень технічної складності. Це формує своєрідний «практичний шар» регулювання, який має не менший вплив, ніж текст нормативних актів [61; 106].

Окремої уваги заслуговує співвідношення захисту персональних даних та інноваційної політики. Ранні підходи нерідко протиставляли приватність технологічному розвитку, проте сучасна практика поступово відмовляється

від такого протиставлення. У міжнародних документах ефективний захист персональних даних дедалі частіше тлумачать як умову довіри до цифрових технологій і передумову їх сталого розвитку. За такого розуміння приватність постає не бар'єром для інновацій, а складовою інфраструктури цифрової економіки [103; 63].

За схожою системою відбувається й інтеграція етичних міркувань у правове регулювання штучного інтелекту. Міжнародні організації зауважують, що формально законна обробка даних може водночас призводити до соціально небажаних наслідків, зокрема виключення або маніпуляції поведінкою. Це зумовлює необхідність доповнення позитивного права етичними принципами, які виконують роль орієнтирів у ситуаціях регуляторної невизначеності. За такого підходу захист персональних даних тісно пов'язаний з питаннями людської гідності й автономії [116].

Розширюється і коло суб'єктів відповідальності за обробку даних. Класичні моделі зосереджувалися переважно на володільцеві даних, однак у складних алгоритмічних системах відповідальність дедалі частіше розглядають як розподілену між кількома учасниками – розробниками моделей, постачальниками інфраструктури, інтеграторами та користувачами. В основі цього підходу лежить розуміння того, що загрози приватності виникають на різних етапах життєвого циклу ШІ-системи, а отже, їх неможливо усунути, поклавши обов'язки лише на одного суб'єкта.

Дедалі більшого значення набуває транснаціональний характер обробки персональних даних. Алгоритмічні системи зазвичай працюють у глобальних інфраструктурах, де дані переміщуються між юрисдикціями, що ускладнює застосування національних норм. За цих умов міжнародні стандарти виконують координаційну роль: вони обмежують фрагментацію регулювання та гарантують базовий рівень захисту незалежно від місця обробки інформації.

Викладене дає підстави стверджувати, що сучасні світові та європейські тенденції у сфері захисту персональних даних поєднують

нормативні, інституційні, етичні й технічні складові. Саме в такому поєднанні вони слугують орієнтиром для національних правопорядків, які перебувають у процесі пристосування до наслідків алгоритмічної трансформації.

Коли йдеться про вплив світових тенденцій і наукових підходів на формування українського законодавства у сфері захисту персональних даних у контексті штучного інтелекту, слід розуміти, що вплив є наявним, проте не має характеру прямого нормативного запозичення. Ідеться радше про поступову трансформацію регуляторної логіки, у межах якої міжнародні стандарти, доктринальні концепції та регуляторні сигнали створюють рамку, у якій національний законодавець змушений переосмислювати власні підходи до правового захисту приватності.

На ранніх етапах розвитку українського законодавства вплив міжнародного досвіду виявлявся переважно у формальному запозиченні базових принципів захисту персональних даних. Закон України «Про захист персональних даних» 2010 року відтворював загальну європейську модель, орієнтовану на контроль за обігом інформації та процедурну легітимацію її обробки [36]. У той період національне регулювання не знаходилося під тиском складних алгоритмічних практик, а отже, не відчувало потреби в глибшій інтеграції доктринальних і ризик-орієнтованих підходів.

Ситуація поступово змінилася як відповідь на посилення ролі цифрових сервісів, платформних рішень і систем автоматизованого аналізу даних. Тоді міжнародні тенденції, насамперед європейські, стали виконувати для України функцію не лише орієнтира, а й зовнішнього стимулу реформування. Прийняття GDPR у Європейському Союзі стало точкою, після якої збереження чинної редакції Закону 2010 року дедалі частіше оцінювали як недостатнє для забезпечення належного рівня захисту прав суб’єктів даних [3; 21; 118]. Вплив наукової думки в цьому процесі виявляється в зміні акцентів законодавчої дискусії. Якщо раніше центральним питанням залишалася формальна відповідність обробки даних

закону, то під впливом доктринальних досліджень увагу зосереджували на оцінюванні фактичних наслідків алгоритмічної обробки для прав і свобод людини. Це відображено в законодавчих ініціативах, де поряд із традиційними принципами з'являються категорії управління ризиками, підзвітності та превентивного захисту [31, с. 47–53; 64, с. 20–23; 127]. Проєкт нового Закону України «Про захист персональних даних» № 8153, безпосередньо орієнтований на гармонізацію з умовами GDPR [37], стає наочним прикладом. Його положення свідчать про спробу імплементувати не лише окремі норми, а й загальну філософію європейського підходу, що полягає в покладанні активного обов'язку із забезпечення приватності на володільців і розпорядників даних. Закріплення принципів «приватність за проєктуванням» і «приватність за замовчуванням» демонструє зміщення регуляторного фокуса з реагування на порушення до їх запобігання [37].

Міжнародні тенденції, зрештою, впливають на інституційну архітектуру захисту персональних даних в Україні. Дискусія щодо створення незалежного спеціалізованого наглядового органу, зокрема Національної комісії з питань захисту персональних даних і доступу до публічної інформації, безпосередньо пов'язана з вимогами Конвенції 108+ та європейською практикою інституційного нагляду [39; 102]. Такий орган розглядають не лише як інструмент контролю, а і як суб'єкт формування практики застосування законодавства в умовах технологічної невизначеності.

Зміна автоматизованого прийняття рішень і профілювання теж є одним із наслідків впливу. Європейська доктрина й судова практика в українському правовому полі дедалі частіше порушують питання необхідності спеціальних гарантій у випадках, коли рішення ухвалюють алгоритмічні системи без безпосередньої участі людини. Це стосується не лише формального права на заперечення, а й реальної можливості зрозуміти логіку рішення та ефективно його оскаржити [93, с. 1–6; 138]. Під впливом наукових досліджень і європейських регуляторних позицій український законодавець дедалі глибше усвідомлює обмеженість згоди як універсального механізму легітимації

обробки в умовах складних алгоритмічних систем. Це сприяє переходу до моделей, у яких центральне значення мають законні інтереси, суспільна необхідність і пропорційність втручання, за умови посилення обов'язків володільців даних щодо мінімізації ризиків [106; 127].

Техніко-організаційні заходи захисту теж не оминули змін. У проєктних і стратегічних документах дедалі частіше акцентують на необхідності впровадження практик оцінки впливу на захист даних, документування процесів обробки та застосування технологій підвищення приватності. Хоча ці інструменти ще не набули повноцінного закріплення в національному праві, їх поява в дискурсі свідчить про зміну розуміння ефективного захисту персональних даних як поєднання правових і технічних гарантій [58; 60; 64].

Важливою є роль міжнародних кейсів в українському баченні допустимих меж використання персональних даних у сфері штучного інтелекту. Резонансні приклади, пов'язані з регуляторним втручанням у діяльність генеративних моделей у країнах ЄС, демонструють, що навіть технологічно передові рішення можуть бути обмежені в разі недотримання стандартів приватності. Такі прецеденти виконують для України превентивну функцію, окреслюючи потенційні ризики й напрями майбутнього правозастосування [99; 106].

Слід ураховувати, що вплив описаних тенденцій на українське законодавство неоднорідний. Інституційні обмеження, рівень правозастосування та стан цифрової культури вимагають адаптації міжнародних підходів, а не їх механічного перенесення. У цьому процесі наукова думка виконує роль посередника між міжнародними стандартами й національним правом: саме доктринальні дослідження дають змогу пристосувати загальні принципи до конкретних правових і соціальних умов та обґрунтувати потрібні законодавчі зміни. Поступове зближення української доктрини з європейськими підходами створює підґрунтя для

системного реформування відповідного правового інституту й окреслює напрями його подальшого розвитку.

Судові органи, органи нагляду й інші суб'єкти дедалі частіше звертаються до європейських стандартів і тлумачень як до орієнтирів у ситуаціях правової невизначеності. Це формує своєрідний «неписаний» шар регулювання, який доповнює формальні норми та впливає на реальний рівень захисту персональних даних.

У ширшій перспективі вплив наукової думки та міжнародних підходів сприяє поступовому переосмисленню балансу між публічними інтересами та приватністю [65; 116]. В умовах розвитку штучного інтелекту держава зацікавлена у використанні даних для забезпечення безпеки, ефективності управління та розвитку цифрових сервісів. Водночас міжнародні стандарти наполягають на тому, що навіть у таких випадках втручання в приватне життя має бути необхідним, пропорційним й обґрунтованим. Це напруження між ефективністю та правами людини стає одним із ключових викликів для українського законодавця.

Крім цього, під впливом міжнародних тенденцій у національному праві поступово з'являється усвідомлення довгострокових наслідків алгоритмічної обробки даних [63; 131]. Ідеться не лише про миттєві порушення, а й про кумулятивні ефекти, які можуть виявлятися з часом у вигляді соціальної сегрегації, посилення нерівності або втрати автономії особи. Включення такого горизонту аналізу в правове регулювання є складним завданням, але саме воно відрізняє сучасні підходи від ранніх моделей захисту персональних даних.

Водночас роль світових тенденцій та доктринальних підходів на формування українського законодавства у сфері захисту персональних даних під впливом штучного інтелекту не можна зводити виключно до формальної адаптації норм або запозичення термінології. Показовою є трансформація регуляторної логіки, за якої персональні дані починають розглядати не лише як об'єкт охорони, а як елемент складної соціотехнічної системи, у межах

якої взаємодіють технології, інституції та права людини [116; 118]. Саме така зміна фокуса поступово проникає і в український правовий дискурс, хоча її практичне закріплення ще знаходиться на початковому етапі.

Сучасні підходи до регулювання ШІ дедалі рідше апелюють до універсальних заборон або жорстких технічних приписів. Натомість домінує модель диференційованого впливу, за якої правові вимоги корелюють з рівнем потенційної шкоди для прав і свобод людини. Така логіка безпосередньо відображена в ризик-орієнтованому підході, закріпленому в AI Act, і поступово знаходить відображення в українських стратегічних документах та експертних обговореннях [43; 93, с. 1–6; 124]. Для національного законодавства це означає необхідність переосмислення традиційної моделі контролю, побудованої навколо формальної законності обробки даних [7; 8].

Відбувається також і переорієнтація на процесуальний характер захисту персональних даних. У європейській доктрині дедалі чіткіше простежується підхід, за якого правомірність обробки оцінюють не одноразово, а протягом життєвого циклу системи – від проєктування і навчання моделі до її практичного застосування та подальшої модифікації [64; 86]. Такий підхід істотно відрізняється від класичної української практики, де традиційно було акцентовано на моменті збору даних й отриманні згоди суб’єкта.

У цьому зв’язку показовою є поступова зміна ставлення до інституту згоди як центрального механізму легітимації обробки персональних даних. Під впливом міжнародних досліджень і практики регуляторів згоду дедалі частіше розглядають як недостатній інструмент контролю в умовах складних алгоритмічних систем, де суб’єкт об’єктивно не здатен оцінити всі можливі сценарії подальшого використання своїх даних [127; 130]. Для українського законодавства це створює потребу в зміщенні акценту з формального волевиявлення особи на підвищену відповідальність володільців й операторів ШІ-систем.

Природа шкоди порушення персональних даних трансформується також, проте в не найкращу версію. Якщо раніше порушення приватності здебільшого асоціювали з неправомірним доступом або розголошенням інформації, то в умовах ШІ першочерговими стають непрямі й відкладені наслідки алгоритмічної обробки, які охоплюють дискримінаційні ефекти, маніпуляцію поведінкою, обмеження доступу до соціальних благ [63; 131]. Такі наслідки часто не мають чітко окресленого «моменту порушення», що ускладнює їх правову кваліфікацію в межах традиційних механізмів захисту.

Для українського правового поля це означає необхідність розширення інструментарію захисту персональних даних за межі індивідуальних скарг і реактивного нагляду. У наукових роботах увагу спрямовують на доцільність урахування групових і системних ризиків, які виникають унаслідок масового застосування алгоритмічних систем, зокрема у сферах соціального скорингу, кредитування, зайнятості або безпеки [131]. Такий підхід лише частково сумісний із чинною моделлю українського законодавства, що традиційно орієнтоване на індивідуалізований захист прав.

Каналом впливу світових тенденцій є формування нових стандартів належної поведінки через практику наглядових органів. Європейські органи із захисту даних відіграють активну роль у конкретизації вимог законності, прозорості й мінімізації даних у контексті навчання та застосування ШІ-моделей [61; 106]. Для України це має подвійне значення: з одного боку, такі позиції формують орієнтири для майбутньої гармонізації законодавства, з іншого – демонструють, що ефективний захист персональних даних не можливий без сильної інституційної спроможності регулятора [39; 102].

У цьому контексті поступово актуалізується питання інституційного дизайну системи нагляду в Україні. Перехід від мінімалістичної моделі контролю до активної регуляторної ролі, що охоплює роз’яснення, рекомендації та превентивний нагляд, відповідає сучасним європейським стандартам [102]. Однак така трансформація потребує не лише змін у законодавстві, а й перегляду ролі держави у взаємодії з приватними

розробниками та користувачами ШІ-систем. Додатковим аспектом є посилення ролі техніко-організаційних заходів як складової правового захисту персональних даних. Принципи privacy by design і privacy by default поступово перестають бути суто декларативними і перетворюються на практичні критерії оцінювання належності обробки даних [37; 118]. Для українського законодавства це означає необхідність інтеграції правових вимог у технологічну архітектуру систем, що використовують ШІ, а не лише в супровідну документацію.

Активізується також інтерес до технологій підвищення приватності, зокрема диференційної приватності, як інструментів, що дають змогу поєднати аналітичну цінність великих даних із мінімізацією ризиків повторної ідентифікації [58, с. 1–23]. Вплив цих підходів на українську доктрину ще є обмеженим, однак у перспективі вони можуть стати важливим елементом реалізації оновленого законодавства, гармонізованого з європейськими стандартами.

Отже, вплив наукової думки та світових тенденцій на розвиток українського законодавства у сфері захисту персональних даних в умовах застосування штучного інтелекту має багатовимірний характер. Він охоплює зміну регуляторної логіки, трансформацію уявлень про шкоду, переосмислення ролі згоди, посилення інституційного нагляду та інтеграцію технічних гарантій приватності. Сукупно ці процеси формують підґрунтя для переходу від формально-правової моделі захисту до системи управління ризиками, здатної реагувати на складні й динамічні виклики алгоритмічного середовища [64; 116].

Генеза правового регулювання захисту персональних даних в умовах розвитку штучного інтелекту в Україні постає як складний і багаторівневий процес, що формується на перетині внутрішніх трансформацій правової системи та зовнішніх регуляторних імпульсів.

Початкове запозичення базових європейських принципів у сфері захисту персональних даних забезпечило мінімальну нормативну

інфраструктуру, однак не було розраховане на масштаб і характер алгоритмічної обробки інформації, притаманної сучасним ШІ-системам. Подальший розвиток наукової думки й міжнародних підходів зумовив поступове усвідомлення того, що персональні дані в алгоритмічному середовищі перестають бути лише об'єктом правової охорони, а набувають статусу ресурсу, від якого безпосередньо залежать функціонування та ефективність ШІ-моделей. Це своєю чергою актуалізувало ризики, які не вкладаються в класичні уявлення про порушення приватності, виявило обмеженість процедурної моделі захисту, орієнтованої виключно на згоду й формальну законність обробки. Вплив світових тенденцій, зокрема європейського ризик-орієнтованого підходу, поступово трансформує національний дискурс у бік превентивного та процесуального розуміння захисту персональних даних. У такій моделі ключового значення набувають оцінка впливу, управління ризиками, техніко-організаційні гарантії та інституційна спроможність наглядових органів, а не лише санкційні механізми реагування на вже вчинені порушення [37; 64; 118].

Головною особливістю українського етапу розвитку залишається асинхронність між науковими підходами, стратегічними документами та позитивним правом. Попри активізацію законодавчих ініціатив і посилення уваги до етичних і безпекових аспектів застосування штучного інтелекту, практична імплементація нових регуляторних моделей ще не набула системного характеру. Це зумовлює ситуацію, за якої правове поле формально існує, але не завжди відображає реальну структуру ризиків алгоритмічних екосистем [14; 31; 116].

Передусім дискусія зосереджується навколо питання достатності чинного правового регулювання. О. Заярний послідовно обстоює позицію про необхідність удосконалення способів захисту інформаційних прав, аргументуючи це тим, що специфіка функціонування систем штучного інтелекту не вкладається в традиційні юридичні конструкції [15; 18]. Його підхід фактично передбачає формування спеціалізованих механізмів

правового захисту. Натомість В. Брижко, аналізуючи сучасну практику захисту персональних даних, має стриманішу позицію, засвідчуючи адаптивний потенціал уже наявних правових інститутів [12, с. 35–40; 13]. У цьому аспекті простежується класичне протиставлення інноваційного й еволюційного підходів до правового регулювання. Водночас позиція про достатність чинного регулювання не видається цілком переконливою. Хоча базові принципи справді мають універсальний характер, однак їх практична реалізація в умовах автономних алгоритмів значно ускладнюється. Тож доцільним є компромісний підхід, що поєднує збереження загальних принципів з розробленням спеціальних процедур їх застосування до систем штучного інтелекту. О. Заярний, аналізуючи діяльність правоохоронних органів, обґрунтовує необхідність суворого дотримання принципу правомірності й міжнародних стандартів [16]. Його позиція фактично передбачає посилення контролю за використанням таких даних. Водночас у ширшому науковому контексті, зокрема у працях О. Пунди та Д. Арзянцевої, зауважено, що розвиток технологій штучного інтелекту об’єктивно розширює сферу використання персональних даних, що ускладнює забезпечення їх належного захисту [41, с. 135–138]. У цьому випадку постає суперечність між безпековими інтересами держави та правом особи на приватність. Надмірне посилення контролю може обмежувати ефективність правоохоронної діяльності, натомість його недостатність створює ризики зловживань.

Посилену увагу в науковій полеміці спрямовують на оцінювання переваг і загроз використання штучного інтелекту. А. Колесніков та О. Карапетян акцентують на двоїстій природі таких технологій, аргументуючи їх ефективність й одночасно виявляючи потенційні ризики для інформаційної безпеки [21]. Аналогічні висновки містяться в дослідженні М. Бєлової та Д. Бєлова, які зосереджують увагу на посиленні загроз несанкціонованого доступу до персональних даних [4–6]. Водночас зазначені підходи є обмеженими, оскільки здебільшого зосереджуються на фіксації

ризиків, не пропонуючи конкретних механізмів їх мінімізації. У цьому контексті перспективнішими видаються дослідження, що поєднують аналіз ризиків із розробленням інструментів управління ними [9; 10].

В іноземній науковій літературі полеміка набуває іншого характеру й зосереджується на співвідношенні різних регуляторних режимів. Ф. Гакер, А. Енгель і М. Маурер зазначають про складність правового регулювання генеративних моделей, таких як ChatGPT, у межах традиційних підходів [92]. Вони фактично засвідчують необхідність перегляду базових концепцій правового регулювання. Натомість Г. Майкл аналізує взаємодію AI Act та GDPR, зауважуючи про їх часткове дублювання та потенційні колізії [94]. Такий підхід демонструє іншу площину проблеми – не брак регулювання, а його надмірну фрагментацію. Схожі висновки містяться і в дискусійному документі органу із захисту даних Гамбурга, де акцентовано на складності визначення статусу великих мовних моделей у правовій системі [133]. У європейській доктрині простежується протиставлення двох підходів – необхідності створення нових норм й оптимізування вже наявних. На нашу думку, обґрунтованим є другий підхід, оскільки надмірне нормативне навантаження може призводити до правової невизначеності.

Специфічним напрямом полеміки є використання чат-ботів зі штучним інтелектом. Дослідження, присвячені аналізу ChatGPT, виявляють складність визначення меж правомірної обробки персональних даних, зокрема в частині їх збору та подальшого використання [17; 20; 30]. У цьому контексті актуалізується питання відповідальності розробників і користувачів таких систем.

Водночас у науковій літературі розглядають проблеми доказового значення даних, отриманих за допомогою штучного інтелекту. В. Хахановський обґрунтовує, що використання таких технологій ставить під сумнів автентичність електронних доказів [46]. Розвиваючи цей підхід, у подальших дослідженнях учений акцентує на складності ідентифікації цифрових зображень як джерел доказів [100]. Зазначена позиція видається

обґрунтованою, однак вона потребує уточнення. Проблема полягає не стільки в технології, скільки у браку належних процедур верифікації. Тож розвиток процесуальних механізмів може суттєво знизити зазначені ризики. О. Золотар визначає її як комплексне явище, що охоплює правові та соціальні аспекти [19, с. 6–70]. Схожу позицію обстоюють В. Пилипчук і В. Брижко, які доводять необхідність поєднання правових і технічних засобів захисту [33]. М. Бліхар акцентує на адміністративно-правових механізмах забезпечення інформаційної безпеки [11]. Порівняльно-правовий вимір досліджуваної проблематики представлено в роботі М. Швеця, який аналізує відповідність українського законодавства європейським стандартам [13]. Його висновки свідчать про наявність часткової гармонізації, водночас аргументують необхідність подальшого вдосконалення нормативної бази. М. Дубняк зазначає, що забезпечення прозорості штучного інтелекту є необхідною умовою захисту прав суб'єктів персональних даних [76]. Водночас реалізація цього принципу постає перед об'єктивними технічними обмеженнями, що створює ще одну площину для наукових дискусій.

Отже, стан наукового дослідження та генеза розвитку правової охорони і захисту персональних даних у сфері штучного інтелекту в Україні свідчать про поступовий перехід від класичної формально-процедурної моделі захисту персональних даних до ризик-орієнтованої, превентивної та технологічно адаптованої моделі. Українська правова доктрина вже сформувала належне теоретичне підґрунтя для такого переходу, однак чинне законодавство поки що не забезпечує повного регулювання інференційних даних, автоматизованих рішень, профілювання, біометричної ідентифікації та алгоритмічної відповідальності.

Подальший розвиток відповідного правового інституту має відбуватися шляхом поєднання європейських стандартів, національних правових реалій і спеціальних гарантій захисту прав людини в алгоритмічному середовищі. Саме це зумовлює необхідність звернення до методологічних підходів

правової охорони і захисту персональних даних у сфері штучного інтелекту, що становить предмет наступного підрозділу.

1.3. Методологічні підходи до правової охорони та захисту персональних даних у сфері штучного інтелекту

Метою цього підрозділу є визначення методологічних підходів, принципів і методів, які дають змогу комплексно дослідити правову охорону та захист персональних даних у сфері штучного інтелекту, враховуючи технологічну складність алгоритмічної обробки, ризики для приватності, потребу людського контролю та необхідність адаптації національного законодавства до європейських стандартів.

Слід підкреслити, що правова охорона і захист персональних даних у сфері ШІ не можуть досліджуватися лише через аналіз норм Закону України «Про захист персональних даних», GDPR або AI Act. Це пов’язано з тим, що ШІ-системи не просто зберігають дані, а: навчаються на персональних даних; формують нові інференційні висновки; здійснюють профілювання; приймають або підтримують автоматизовані рішення; можуть повторно ідентифікувати особу; створюють ризики дискримінації, непрозорості та втрати контролю людини над даними. Саме тому методологія дослідження має бути комплексною, а не суто формально-юридичною.

Основні методологічні підходи, використані у дослідженні.

1. Системний підхід – правова охорона та захист персональних даних у сфері ШІ є не простим набором окремих норм, а системою правових, технічних, організаційних та інституційних гарантій.

2. Міждисциплінарний підхід – дослідження потребує поєднання права, інформаційних технологій, кібербезпеки, етики, адміністративного регулювання та захисту прав людини.

3. Ризик-орієнтований підхід – цей підхід є, на наш погляд, одним із центральних. Адже правове регулювання має залежати від рівня ризику обробки персональних даних із використанням ШІ. Особливо це пов'язано із високоризиковою обробкою, біометричними даними, інференційними висновками, профілюванням і автоматизованими рішеннями.

4. Антропоцентричний / людиноцентричний підхід – права, свободи, приватність і гідність людини мають перевагу над технологічною ефективністю ШІ-систем. Тут методологія пов'язана з правом на людське втручання, пояснення автоматизованого рішення та ефективне оскарження.

5. Порівняльно-правовий підхід – використовується для аналізу європейського та зарубіжного досвіду, зокрема GDPR, AI Act, Конвенції 108+, а також моделей США, Великої Британії, Канади та Японії.

6. Інституційний підхід – ефективний захист персональних даних у сфері ШІ залежить не лише від норм закону, а й від діяльності інституцій: наглядового органу, суду, володільця даних, оператора ШІ-системи, розробника, постачальника, аудитора.

7. Функціональний підхід – персональні дані в системах ШІ виконують не лише інформаційну, а й функціональну роль: використовуються для навчання моделей, прогнозування, класифікації, ідентифікації, оцінки поведінки та прийняття рішень.

Перелік методів дослідження був наданий в роботі вище (у вступі дисертації). Доречним буде коротко пов'язати заявлені методи з методологічною логікою підрозділу.

Формально-юридичний, догматичний, компаративістський, логіко-семантичний, системно-структурний методи, метод моделювання, прогностичний та емпіричний методи є інструментами реалізації обраної методології. Ці методи допомагають дослідити правову охорону і захист персональних даних у сфері штучного інтелекту.

Окремо слід підкреслити, що частина положень є не методами дослідження, а принципами або практико-методологічними орієнтирами

побудови правового режиму. До них треба віднести: privacy by design; privacy by default; прозорість алгоритмічної обробки; підзвітність; мінімізацію даних; цільове обмеження; людський контроль; недискримінацію; алгоритмічний аудит; оцінку впливу на захист персональних даних. Їх потрібно розглядати як принципи побудови правового та технічного захисту персональних даних у системах ШІ.

З огляду на міждисциплінарний характер проблематики, методологічні підходи до правової охорони персональних даних під час застосування ШІ поєднують правові, організаційні та технічні заходи. Метою цього передусім є створення такого комплексного механізму, який забезпечить ефективний захист прав людини на приватність, не стримуючи обґрунтований розвиток і впровадження інновацій. Розглянемо ключові підходи та принципи, що є основою формування сучасної системи захисту персональних даних у сфері ШІ.

Методологія правової охорони персональних даних у сфері застосування штучного інтелекту формується в умовах істотної зміни характеру інформаційних процесів, що не можуть бути цілком охоплені традиційними моделями правового регулювання. Використання ШІ зумовлює не лише появу нових способів обробки інформації, а й трансформацію уявлення про персональні дані як об’єкт правової охорони. У сучасних алгоритмічних системах дані функціонують не як пасивний набір відомостей, а як активний ресурс, що постійно переосмислюють, поєднують з іншими масивами, використовують для навчання моделей і формування інференцій [118; 124]. За таких умов зведення захисту приватності до формального дотримання окремих норм або процедур виявляється недостатнім.

Комплексний характер методології означає необхідність одночасного застосування таких інструментів: правових, організаційних, технічних та етичних. Жоден із цих елементів не може забезпечити ефективну охорону

персональних даних самостійно, оскільки кожен з них охоплює лише окремий вимір проблеми.

Правові норми визначають загальні принципи, межі допустимої обробки та наслідки їх порушення, однак без відповідних організаційних механізмів вони залишаються декларативними. Технічні рішення хоча й можуть зменшувати ризики розкриття або зловживання даними, однак без нормативного закріплення їх застосування залежить виключно від волі розробників або операторів систем [103; 60]. Етичні межі тут виконують допоміжну, але важливу функцію, заповнюючи регуляторні прогалини в умовах, коли позитивне право відстає від темпів технологічного розвитку [116]. Міждисциплінарність методологічного підходу зумовлена тим, що захист персональних даних у сфері ШІ не може бути адекватно осмислений виключно в межах юридичної науки. Право в цій сфері тісно взаємодіє з інформатикою, кібербезпекою, теорією управління та соціальними науками. Зокрема, без розуміння принципів машинного навчання, роботи великих мовних моделей або особливостей обробки великих даних складно оцінити реальні ризики для прав і свобод людини. Сучасні регулятори й підходи дедалі частіше апелюють не лише до юридичних категорій, а й до опису фактичних технологічних процесів, у межах яких відбувається обробка персональних даних [64; 86].

Однією з рис міждисциплінарного підходу є зміщення акценту з окремих операцій з даними на управління процесами загалом. Якщо класичні моделі захисту персональних даних зосереджувалися переважно на моменті збору інформації та наявності правової підстави для її використання, то в умовах застосування ШІ ключового значення набуває контроль упродовж усього життєвого циклу даних. Це охоплює етапи первинного отримання інформації, її зберігання, подальшого використання для навчання моделей, повторного застосування з іншою метою, а також створення похідних результатів. У такій логіці захист персональних даних вже не є разовою дією, а стає безперервним процесом оцінювання та коригування ризиків [103; 130].

Співвідношення між приватністю та інноваційним процесом має деякі аспекти, що потребують роз’яснення.

Упродовж тривалого часу в наукових і політичних дискусіях захист персональних даних нерідко сприймали як фактор, що потенційно стримує технологічний прогрес. Натомість сучасні підходи дедалі частіше керуються протилежною логікою, відповідно до якої ефективна охорона приватності є необхідною умовою довіри до цифрових технологій, як наслідок – їх сталого впровадження. У цьому сенсі комплексна методологія не протиставляє правове регулювання та розвиток ШІ, а розглядає їх у взаємозв’язку, де право встановлює межі безпечного використання інновацій [63; 65].

Важливим тут є і організаційний вимір захисту персональних даних. Реалізація правових вимог безпосередньо залежить від внутрішніх процедур суб’єктів, які розробляють або використовують ШІ-системи, від рівня підготовки персоналу, культури управління даними та наявності механізмів внутрішнього контролю. У практиці застосування ШІ ключові рішення щодо архітектури систем, вибору наборів даних або параметрів навчання часто ухвалюють не юристи, а інженери чи менеджери проєктів. Це зумовлює необхідність інтеграції вимог захисту персональних даних безпосередньо в процеси проєктування та експлуатації систем, а не їх формального врахування постфактум [37; 64].

Проблемним аспектом, який виразно виявляється у сфері ШІ, є розподіл відповідальності між учасниками алгоритмічних екосистем. Розробники моделей, постачальники даних, оператори платформ і кінцеві користувачі виконують різні функції, що ускладнює застосування традиційних моделей юридичної відповідальності. У зв’язку з цим методологічний підхід до захисту персональних даних має поєднувати елементи приватного й публічного права, а також передбачати використання організаційних і технічних механізмів підзвітності, які дають змогу ідентифікувати зони ризику ще до виникнення порушення [46; 93].

Тому комплексний, міждисциплінарний підхід до правової охорони персональних даних у сфері штучного інтелекту можна схарактеризувати як перехід від фрагментарного регулювання до системного управління ризиками для прав і свобод людини. Ідеться не про механічне поєднання різних інструментів, а про формування узгодженої методології, що враховує реальні технологічні процеси, організаційні практики та соціальні наслідки використання ШІ. Саме така логіка закладає підґрунтя для подальшого аналізу конкретних принципів і механізмів захисту персональних даних.

Одним із ключових елементів сучасної методології правової охорони персональних даних у сфері застосування штучного інтелекту є принципи *privacy by design ma privacy by default,* закріплені на нормативному рівні й водночас такі, що мають виразно практичне спрямування.

Їх поява зумовлена усвідомленням того, що захист персональних даних не може бути ефективним, якщо його розглядають як зовнішнє обмеження, яке накладається на систему вже після її створення. Натомість у контексті ШІ йдеться про необхідність інтеграції вимог приватності безпосередньо в логіку проєктування, архітектуру та функціонування алгоритмічних рішень

Принцип *privacy by design* керується тим, що потенційні ризики для прав і свобод людини необхідно ідентифікувати та мінімізувати ще на стадії розроблення інформаційної системи або ШІ-моделі [64, с. 20–33]. Це означає, що питання обсягу даних, тривалості їх зберігання, можливостей повторного використання, а також доступу до них не можна розглядати як другорядні або технічні деталі. Навпаки, вони стають складовою правової відповідальності розробника чи оператора системи. У практичному вимірі це призводить до зміщення акценту з формального дотримання вимог закону на активне управління ризиками в процесі створення технологічних рішень.

Особливість застосування принципу privacy by design у сфері штучного інтелекту полягає в тому, що низку рішень, які мають правове значення, приймають на етапах, що традиційно знаходяться поза сферою уваги юристів. Ідеться, зокрема, про вибір навчальних наборів даних, визначення

параметрів моделі, архітектури нейронних мереж, способів оновлення алгоритмів і механізмів обробки похідних результатів.

Саме на цих етапах закладають передумови як для дотримання принципів мінімізації та обмеження мети, так і для потенційних порушень приватності, які згодом можуть бути складними для виправлення [95; 130].

Методологічно важливим є те, що privacy by design не зводиться до використання окремих технічних інструментів. Ідеться про системний підхід, у межах якого правові вимоги трансформуються в конкретні проєктні рішення. Наприклад, замість централізованого збирання великих масивів персональних даних можуть обирати децентралізовану модель обробки, замість зберігання ідентифікаторів застосовують псевдонімізацію, а замість необмеженого повторного використання даних – чітко визначені сценарії доступу й видалення інформації [60; 103]. Такі рішення не лише знижують ризики порушення прав суб’єктів даних, а й полегшують подальше доведення відповідності системи вимогам законодавства.

Принцип *privacy by default* доповнює логіку захисту за задумом та орієнтує її на практичну взаємодію з користувачем. Його суть полягає в тому, що за замовчуванням система повинна функціонувати в максимально захисному для приватності режимі, без необхідності активних дій з боку суб’єкта даних. У контексті ШІ це означає, що алгоритмічні системи не повинні автоматично використовувати персональні дані в ширшому обсязі, ніж це об’єктивно необхідно для досягнення заявленої мети обробки. Будь-яке розширення функціоналу, пов’язане з додатковим використанням даних, має бути результатом свідомого вибору користувача, а не наслідком непрозорих налаштувань [106; 118].

Практичне значення принципу privacy by default найчіткіше виявляється в масових цифрових сервісах, у яких застосовують системи штучного інтелекту й де користувачі не усвідомлюють реального обсягу та складності обробки персональних даних. У такій ситуації перенесення відповідальності за захист приватності на суб’єкта даних через формальне

надання згоди не забезпечує належного рівня охорони його прав. Конструкція системи має керуватися протилежною логікою: навіть за мінімальної поінформованості користувача втручання в приватне життя має залишатися обмеженим. Саме такий підхід відповідає зміні акцентів у праві захисту персональних даних – від дотримання процедур до оцінки фактичних ризиків для прав і свобод людини [63; 127].

Застосування принципів privacy by design і privacy by default у сфері штучного інтелекту ускладнене властивостями ШІ-систем. Ідеться, зокрема, про їхню здатність змінювати поведінку в процесі навчання або адаптації до нових наборів даних. За таких умов вичерпне прогнозування всіх сценаріїв обробки інформації на етапі проєктування є майже неможливим через їх різноманітність. Це зумовлює потребу в регулярному перегляді проєктних рішень і підтверджує, що захист приватності не може обмежуватися початковим етапом розроблення. Його має бути включено в процес експлуатації, коригування і технічного оновлення системи [86]. Проблемним залишається і поєднання принципів privacy by design з вимогами прозорості та пояснюваності алгоритмічних рішень. Мінімізація обсягу даних й обмеження доступу до них здатні обмежувати можливості зовнішнього контролю за функціонуванням ШІ-систем. Водночас непрозорість алгоритмічних процесів створює додаткові ризики для реалізації прав суб’єктів даних. У цьому контексті методологічне завдання полягає не у формальному пріоритеті одного принципу над іншим, а у вибудовуванні таких рішень, які дають змогу узгодити вимоги захисту приватності з потребами контролю й підзвітності. Реалізація цього підходу неможлива без взаємодії правників, інженерів і фахівців з етики [138].

На цьому етапі постає потреба в ризик-орієнтованому підході. Ризик-орієнтований підхід у сфері захисту персональних даних виник не як теоретичне нововведення, а як реакція на практичну неспроможність класичних моделей регулювання забезпечити ефективний захист прав людини в умовах алгоритмічної обробки інформації. Застосування штучного

інтелекту змінило характер загроз: шкода для приватності дедалі рідше виявляється у формі очевидного порушення, натомість вона набуває опосередкованого, накопичувального або відкладеного характеру, що ускладнює її своєчасне виявлення [118; 124]. За таких умов формальну перевірку наявності згоди або іншої правової підстави вже не можна розглядати як достатню гарантію правомірності обробки. Ризик у контексті застосування ШІ охоплює значно ширший спектр можливих негативних наслідків, ніж традиційні загрози витоку чи несанкціонованого доступу до даних. Алгоритмічні системи здатні формувати профілі, робити інференційні висновки, поєднувати різнорідні набори інформації та застосовувати результати такого аналізу в процесах ухвалення рішень, які безпосередньо впливають на доступ особи до ресурсів, послуг або соціальних благ. У низці випадків суб'єкт даних дізнається про наявність такої обробки лише на стадії виникнення її наслідків, що істотно ускладнює реалізацію права на захист [64, с. 12–19]. Така обставина спричиняє методологічний зсув від оцінювання окремих операцій з даними до аналізу потенційної шкоди для прав і свобод людини.

Центральним інструментом реалізації ризик-орієнтованого підходу в праві Європейського Союзу стало оцінювання впливу на захист персональних даних (Data Protection Impact Assessment). Її значення полягає у створенні механізму попереднього осмислення ризиків, які можуть виникнути внаслідок функціонування конкретної ШІ-системи. DPIA має забезпечити ситуацію, за якої потенційно проблемні аспекти обробки ідентифікують ще до моменту фактичного втручання у сферу приватності, а не після настання негативних наслідків [106; 118].

У випадку застосування штучного інтелекту оцінювання впливу є ускладненим. Це пов'язано з тим, що ризики часто формуються не на етапі первинного збору даних, а у процесі навчання або донавчання моделей, повторного використання наборів інформації та створення похідних результатів. Крім того, складність сучасних алгоритмічних рішень

унеможливлює повну прозорість логіки їх функціонування, що підвищує значення процедур документування та фіксації управлінських рішень у межах DPIA [93].

Методологічно важливо, що ризик-орієнтований підхід не обмежується індивідуальним виміром захисту персональних даних. Алгоритмічні системи часто створюють групові ризики, коли шкода виявляється не щодо конкретної особи, а щодо певних соціальних категорій або статистичних кластерів. Такі ефекти не завжди можуть бути охоплені класичними інструментами індивідуального правового захисту, що зумовлює необхідність у ширших концепціях справедливості даних і колективного виміру шкоди [131]. У цьому контексті оцінка впливу є не лише інструментом приватноправового захисту, а й елементом публічного управління ризиками. Такий підхід спричиняє зміни в традиційному розподілі відповідальності між учасниками інформаційних відносин. Якщо в класичних моделях значну частину тягаря контролю покладали на суб'єкта даних через механізм згоди, то в умовах використання ШІ така модель виявляється концептуально хибною. Суб'єкт даних не володіє достатньою інформацією для оцінки складних алгоритмічних процесів і не може прогнозувати всі можливі наслідки обробки. Тож відповідальність за ідентифікацію та мінімізацію ризиків логічно зміщується в бік володільців й операторів ШІ-систем [64, с. 15; 127]. Це означає, що правова охорона персональних даних дедалі більше ґрунтується на обов'язку прогнозування шкоди, а не лише реагування на вже допущені порушення.

Нормативне закріплення ризик-орієнтованого підходу відображається як у GDPR, так і в Регламенті про штучний інтелект, який вводить диференціацію ШІ-систем залежно від рівня ризику. Такий підхід демонструє загальну тенденцію розвитку сучасного права, яка іде від універсальних правил до контекстуального регулювання, ґрунтованого на оцінюванні наслідків застосування технологій [93; 124].

Для України інтеграція ризик-орієнтованої моделі має важливе значення з огляду на процес гармонізації з європейськими стандартами. Закон України «Про захист персональних даних» № 8153 передбачає обов'язок оцінювання впливу для операцій з високим рівнем ризику, що свідчить про поступовий перехід від формального підходу до системи управління ризиками. Водночас ефективність цього інструменту залежатиме не лише від законодавчого закріплення, а й від формування сталої правозастосовної практики й експертної спроможності наглядових органів [37; 106]. Проте ризик-орієнтований підхід не усуває нормативної невизначеності, притаманної сфері ШІ. Навпаки, він визнає її існування та пропонує процесуальні механізми роботи з нею. Оцінка впливу в цьому сенсі є способом фіксації логіки прийняття рішень в умовах неповної передбачуваності, що підвищує рівень підзвітності та прозорості дій операторів алгоритмічних систем [86; 118].

Не слід ігнорувати й роль технічних механізмів захисту персональних даних. У сфері застосування штучного інтелекту вони відіграють не допоміжну роль, як може здаватися, а структуроутворювальну роль у сучасній моделі правової охорони приватності. Умови алгоритмічної обробки інформації істотно обмежують ефективність виключно нормативних приписів, оскільки значну частину рішень, що мають правове значення, реалізують на рівні архітектури системи, вибору моделей та способів роботи з даними. Саме на цьому рівні визначають, чи будуть персональні дані використовувати централізовано або децентралізовано, чи зберігатимуть ідентифікатори, чи формуватимуть похідні профілі, чи можливе подальше відновлення інформації про конкретну особу. Технічні рішення, закладені під час проєктування, часто є незворотними або такими, що потребують значних ресурсів для коригування. Це надає технологічним механізмам захисту важливого значення в методології правового регулювання ШІ [60; 103].

На практиці технологічний вимір захисту персональних даних виявляється через концепцію privacy-enhancing technologies, яка охоплює

сукупність інструментів, спрямованих на зниження ризиків ідентифікації та зловживання інформацією без повного припинення її використання.

Одним з найобговорюваніших технічних підходів у контексті ШІ є диференційована приватність. Її методологічна цінність полягає в зміні логіки обробки даних: замість того, щоб намагатися приховати доступ до інформації, система модифікує результати обчислень так, щоб внесок окремої особи не міг бути виокремлений із загального масиву. Цього досягають шляхом додавання контрольованого статистичного шуму, параметри якого визначають допустимий баланс між точністю результатів і рівнем захисту приватності. У сфері машинного навчання диференційована приватність надає можливість здійснювати тренування моделей на великих наборах персональних даних, мінімізуючи ризик відновлення окремих записів навіть у разі доступу до моделі або її вихідних параметрів. Такий підхід поступово інтегрується в практику великих технологічних компаній, його розглядають регулятори як приклад належної технічної реалізації принципів мінімізації та обмеження мети обробки [58; 59].

Застосування диференційованої приватності пов’язане з низкою обмежень, що мають значення для правового аналізу. Зниження точності результатів, обумовлене додаванням шуму, може впливати на якість рішень, що приймають на основі ШІ, передусім у сферах із високими вимогами до достовірності, таких як медицина або фінанси. Це породжує питання пропорційності, де рівень технічного захисту має співвідноситися з характером обробки й можливими наслідками для суб’єктів даних. Тож вибір параметрів диференційної приватності не можна розглядати як суто інженерне рішення, він набуває ознак юридично значущого управлінського вибору [105].

Важливим є і федеративне навчання, яке змінює традиційну модель централізованого збору даних. За такого підходу алгоритмічна модель переноситься безпосередньо до місця зберігання інформації, а навчання відбувається локально, без передачі «сирих» даних до центрального сервера.

Після завершення навчання агрегуються лише параметри моделі, що істотно знижує ризики масових витоків і несанкціонованого доступу. Федеративне навчання розглядають як перспективний інструмент у сферах, де централізація даних є особливо чутливою, зокрема у сфері охорони здоров'я або фінансових послуг. Для правової методології важливо те, що такий підхід дає змогу реалізувати вимоги мінімізації обробки без повної відмови від використання великих даних [64; 86; 95].

Федеративне навчання не усуває всіх ризиків, пов'язаних із приватністю. Навіть агреговані параметри моделей можуть у певних умовах містити інформацію, придатну для реконструкції окремих елементів навчальних даних. Це означає, що правова оцінка таких технологій має враховувати не лише формальну відсутність передачі персональних даних, а й потенційні можливості зворотного аналізу. У цьому контексті технічні механізми захисту не замінюють правових вимог, а вимагають їх адаптації до нових форм ризику [106].

Окрему групу технічних засобів становлять криптографічні методи, зокрема шифрування та багатосторонні обчислення. Традиційне шифрування залишається базовою гарантією безпеки персональних даних під час зберігання та передачі, однак розвиток ШІ актуалізує складніші підходи, такі як гомоморфне шифрування, що дає змогу виконувати обчислення із зашифрованими даними. Теоретично це створює можливість використання ШІ без розкриття вихідної інформації навіть для оператора системи. Практичне застосування таких технологій поки обмежене через високі обчислювальні витрати, проте їх розвиток має потенціал змінити уявлення про допустимі межі обробки персональних даних у майбутньому [60]. Застосування технічних механізмів захисту персональних даних у сфері ШІ не можна розглядати ізольовано від організаційних і правових аспектів. Ефективність технологічних рішень залежить від того, чи закріплено їх у внутрішніх політиках суб'єктів, чи супроводжуються вони належними процедурами контролю та аудиту, чи враховують регулятори під час

оцінювання відповідності законодавству. У практиці Європейського Союзу спостерігається тенденція до визнання використання PETs як фактора, що може впливати на оцінювання ризиків й обсяг регуляторних обов'язків, зокрема в межах ризик-орієнтованих моделей регулювання [59; 134].

Для України методологічне значення технічних механізмів полягає в можливості поєднання євроінтеграційних вимог із реаліями національного цифрового середовища. Упровадження технологій підвищення приватності може слугувати інструментом поступової адаптації до стандартів ЄС без різкого обмеження інноваційної діяльності. Ключовим викликом залишається забезпечення того, щоб технічні рішення не перетворювалися на формальну імітацію захисту, а реально знижували ризики для прав і свобод людини. Саме у взаємодії технологічних, правових й організаційних елементів формується сучасна методологія охорони персональних даних у сфері застосування штучного інтелекту.

Слід ураховувати, що алгоритмічні системи функціонують у режимі постійної динаміки: моделі донавчаються, змінюються джерела даних, коригуються завдання використання. За таких умов правозастосування, яке ґрунтується виключно на постфактумних перевірках або розгляді скарг, втрачає значну частину своєї ефективності. Саме тому в сучасних підходах дедалі важливішими стають превентивні та супровідні форми нагляду, що дають змогу втручатися ще до того, як ризик реалізується в конкретне порушення прав суб'єкта даних.

Складності набуває питання перевірюваності ШІ-систем з боку наглядових органів. На відміну від традиційних інформаційних систем, де обробка персональних даних часто має лінійний і документований характер, алгоритмічні моделі оперують статистичними залежностями, які не завжди можуть бути безпосередньо інтерпретовані в правових категоріях. Це створює методологічний розрив між вимогою юридичної обґрунтованості та фактичною непрозорістю внутрішніх механізмів ШІ. У цьому контексті інституційний нагляд змушений еволюціонувати в напрямі поєднання

правової експертизи з технічною, що своєю чергою ставить питання про кадрове й організаційне забезпечення відповідних органів [93].

Ще одним виміром інституційного контролю є проблема стандартів доказування відповідності. Якщо у класичних моделях достатнім вважали формальне підтвердження виконання нормативних вимог, то у сфері ШІ дедалі частіше постає потреба в демонстрації фактичної ефективності застосованих заходів захисту. Ідеться не лише про наявність політик або процедур, а про здатність суб'єкта довести, що конкретна архітектура системи, обрані параметри моделі чи організаційні рішення реально знижують ризики для персональних даних. Такий підхід поступово змінює уявлення про compliance, наближаючи його до концепції безперервної підзвітності [86]. У національному контексті ці виклики посилюються обмеженістю інституційних ресурсів. Українська модель нагляду у сфері захисту персональних даних історично формувалася в умовах порівняно простих сценаріїв обробки інформації, де ключовими об'єктами контролю були реєстри, бази даних й адміністративні процедури. Упровадження ШІ-систем потребує переходу до якісно іншого рівня регуляторної спроможності, що охоплює розуміння алгоритмічних ризиків, оцінку технічних рішень і здатність вести діалог з розробниками складних технологій [21].

Так формується поняття сертифікації та стандартизації як інструментів методологічного впливу. На відміну від жорстких заборон або санкцій, ці механізми дають змогу формувати поле допустимих практик шляхом встановлення орієнтирів належної поведінки. Сертифікація ШІ-систем на відповідність вимогам захисту персональних даних може виконувати функцію своєрідного «фільтра», який відсіює очевидно ризиковані рішення ще на етапі впровадження. Водночас ефективність такого підходу залежить від авторитетності органу сертифікації та довіри до критеріїв оцінювання, що знову повертає до питання інституційної спроможності [124].

Регуляторні пісочниці дають змогу поєднати експериментальний характер інновацій з контролем з боку держави. Вони створюють простір для апробації нових ШІ-рішень без негайного застосування санкцій, але за умови постійної взаємодії з регулятором. З методологічної позицій це змінює логіку правового регулювання: замість жорсткого розмежування дозволеного й забороненого формується процес спільного пошуку прийнятних моделей використання технологій [60; 64]. Міжнародний вимір інституційного нагляду створює значення зв’язку з транскордонним характером ШІ-систем. Алгоритми, що обробляють персональні дані, нерідко розробляють в одній юрисдикції, навчаються на даних з кількох країн, їх і використовують глобальні платформи. Це ускладнює застосування виключно національних механізмів контролю і потребує координації між регуляторами, обміну інформацією та визнання рішень один одного. Для України цей аспект є важливим не лише з позицій захисту прав громадян, а й у контексті інтеграції в європейський правовий простір [102; 106].

Інституційний нагляд у сфері ШІ неминуче постає перед проблемою меж втручання держави в технологічний розвиток. Надмірно деталізований контроль може стримувати інновації, натомість надто м’який підхід створює ризик формалізації вимог і втрати довіри до системи захисту персональних даних. Методологічний баланс між цими крайнощами залишається рухомою точкою, що потребує постійного коригування з огляду на практику застосування та еволюції технологій [63].

У цьому сенсі інституційний і регуляторний нагляди слід оцінювати не як завершені елементи системи, а як процеси, що знаходяться на етапі становлення. Їх ефективність визначатимуть не лише текстами нормативних актів, а й здатністю регуляторів навчатися, адаптуватися та взаємодіяти з іншими учасниками алгоритмічної екосистеми. Саме така динамічна модель нагляду створює передумови для того, щоб правова охорона персональних даних у сфері ШІ залишалася релевантною в умовах стрімкої технологічної трансформації.

Технічні й організаційні гарантії захисту персональних даних у середовищі штучного інтелекту формуються не як додаток до правового регулювання, а як його практичне продовження. У сучасних алгоритмічних системах саме на рівні технічних рішень визначають реальний ступінь втручання в приватну сферу, оскільки навіть формально правомірна обробка може створювати непропорційні ризики через спосіб реалізації. Це зумовлює зміщення уваги з абстрактних заборон на конкретні архітектурні вибори, які або стримують поширення даних, або, навпаки, сприяють їх неконтрольованому використанню [60; 118].

Значна частина вже наявних ШІ-систем працює в режимі постійного навчання, коли дані не лише використовують одноразово, а повторно залучають для коригування моделей, тестування гіпотез й оптимізації результатів. У таких умовах особливої ваги набуває питання обмеження доступу та внутрішнього розмежування ролей. Якщо персональні дані є доступними широкому колу осіб або підсистем, ризик їх нецільового використання зростає незалежно від формальної наявності правової підстави. Тому організаційні рішення, пов’язані з управлінням доступом, записом дій і внутрішнім контролем, фактично стають елементом правової охорони приватності, навіть якщо їх прямо не описано в законі [64].

У практиці розроблення та експлуатації ШІ-систем дедалі частіше застосовують принцип мінімальної достатності не лише щодо обсягу даних, а й щодо їх функціонального використання. Це означає, що систему проєктують так, аби окремі компоненти отримували лише ту інформацію, яка є критично необхідною для виконання конкретного завдання. Такий підхід знижує ймовірність масштабних витоків або вторинного використання даних у разі збоїв чи зловживань. Водночас він ускладнює архітектуру систем і потребує додаткових ресурсів, що нерідко сприймають розробники як надмірний тягар. Саме тут виявляється напруження між економічною доцільністю та вимогами захисту прав людини [103].

Технічні гарантії у сфері ШІ дедалі частіше пов’язують з концепцією privacy-enhancing technologies, що сприяє зменшенню імовірності ідентифікації осіб навіть за умови активної аналітичної обробки даних. Ідеться не про повне усунення персональних елементів, а про контрольований рівень втручання, коли результати аналізу зберігають корисність, але не дають змоги відновити індивідуальні характеристики конкретної людини [58, с. 1–23]. У цьому контексті диференційну приватність розглядають не як універсальне рішення, а як інструмент, придатний для певних сценаріїв, зокрема статистичного аналізу й агрегованого навчання моделей [58; 105].

Водночас застосування технічних механізмів не може бути відірване від організаційних процесів, у межах яких ухвалюють рішення щодо використання ШІ. Навіть найпросунутіші засоби шифрування або знеособлення втрачають ефективність, якщо немає внутрішніх процедур контролю, політики зберігання даних або чітко визначених правил реагування на інциденти. Саме тому в європейських підходах увагу спрямовують на внутрішню документацію, опис потоків даних і фіксацію рішень, що приймають на різних етапах життєвого циклу системи [106].

Організаційний вимір охорони персональних даних у сфері ШІ тісно пов’язаний з питанням відповідальності. У складних алгоритмічних екосистемах складно однозначно встановити, на якому етапі виникла шкода або хто саме має нести юридичні наслідки. Тому дедалі важливішими стають внутрішні механізми розподілу відповідальності, які дають змогу простежити ланцюг рішень і дій. Такий підхід не усуває потреби в зовнішньому нагляді, але створює підґрунтя для ефективнішого правозастосування в разі порушень [46].

Окремим викликом є забезпечення захисту персональних даних у сценаріях транскордонної обробки, які є типовими для сучасних ШІ-сервісів. Дані можуть зберігати в одній юрисдикції, обробляти в іншій, а результати використовувати глобально. За таких умов технічні гарантії, зокрема

шифрування та сегментація доступу, виконують функцію універсального запобіжника, який частково компенсує відмінності в правових режимах. Водночас організаційні рішення щодо вибору провайдерів, умов передачі даних і договірних зобов'язань набувають самостійного правового значення [102; 118].

В українському контексті питання технічних й організаційних гарантій набуває особливої актуальності з огляду на процес реформування законодавства. Формальне наближення до європейських стандартів не гарантує їх реального впровадження без розвитку практик внутрішнього управління даними. У цьому сенсі запозичення моделей, що поєднують правові вимоги з конкретними інженерними рішеннями, може відігравати роль каталізатора для підвищення загального рівня захисту персональних даних у сфері ШІ [37; 90]. Слід також ураховувати, що технічні гарантії мають властивість швидко старіти в умовах стрімкого розвитку алгоритмічних методів. Те, що сьогодні вважають достатнім рівнем захисту, завтра може виявитися вразливим через регулярні технологічні оновлення. Це зумовлює потребу в динамічному підході, за якого системи регулярно переглядають, оновлюють та адаптують до нових загроз. У правовому вимірі це означає, що вимоги до захисту персональних даних не можуть бути повністю статичними, вони мають враховувати технологічну мінливість середовища [64; 86].

Отже, технічні й організаційні гарантії у сфері застосування штучного інтелекту виконують роль практичного містка між нормативними приписами й реальними процесами обробки персональних даних. Вони дають змогу трансформувати абстрактні принципи захисту приватності в конкретні рішення, що впливають на архітектуру систем, поведінку учасників і рівень ризику для прав людини. Поєднані з правовими й інституційними механізмами, ці гарантії формують основу для стійкої моделі охорони персональних даних в умовах алгоритмічного розвитку, де ефективність

захисту визначають не деклараціями, а реальною здатністю обмежувати шкоду.

Окремий пласт методологічних підходів пов’язаний з використанням технічних засобів захисту персональних даних, які в сучасному дискурсі розглядають не як допоміжний інструмент, а як структурний елемент правової охорони. Ідеться про ситуацію, коли норми права більше не можуть ефективно працювати без технологічного підкріплення, тому технічні рішення фактично стають способом реалізації юридичних вимог. У сфері штучного інтелекту це вкрай відчутно, оскільки логіка машинного навчання передбачає опрацювання значних обсягів інформації, багаторазове використання даних і формування похідних результатів, які складно контролювати виключно через формальні приписи [58; 118].

Диференційна приватність посідає особливе місце серед цих технологій, адже вона пропонує формалізований, математично обґрунтований спосіб обмеження інформації про конкретну особу в межах загального масиву даних. Її логіка ґрунтується на тому, що результат аналізу або навчання моделі не має дозволяти дійти достовірного висновку про наявність або відсутність даних конкретної людини у вибірці. Для правового аналізу важливо, що такий підхід надає можливість поєднати вимоги мінімізації даних із потребами розвитку алгоритмічних систем, не вдаючись до повної відмови від використання персональної інформації. Інтеграція диференційної приватності в практику використання ШІ змінює уявлення про допустимі межі обробки даних. Якщо раніше правова оцінка часто зводилася до питання законності збору та зберігання інформації, то тепер з’являється додатковий вимір – оцінювання того, чи здатна система гарантувати, що навіть в разі доступу до результатів обробки особа не буде ідентифікована. Це створює підґрунтя для розвитку гнучких моделей регулювання, де правові вимоги узгоджуються з конкретними технічними параметрами системи, а не лише з її формальним описом [105].

Істотне методологічне значення має напрям, пов’язаний із децентралізацією процесів навчання моделей. Федеративне навчання змінює логіку обробки даних, оскільки усуває необхідність створення єдиного сховища персональної інформації. З правової позиції це означає зниження концентрації ризиків: навіть у разі компрометації окремого вузла система не розкриває повного набору даних про суб’єктів. Такий підхід поступово розглядають як альтернативу традиційним моделям масового збирання інформації, передусім у чутливих сферах, пов’язаних зі здоров’ям, фінансами або соціальними послугами [86]. Проте децентралізація не усуває всіх правових проблем, а радше змінює їх конфігурацію. Постають питання щодо розподілу відповідальності між учасниками системи, контролю за коректністю локального навчання, а також можливості аудиту результатів. Методологічно це означає, що використання федеративного навчання не можна розглядати як автоматичне виконання вимог захисту персональних даних, воно потребує доповнення організаційними та процедурними гарантіями [46; 64].

Криптографічні методи включно з гомоморфним шифруванням і багатосторонніми обчисленнями формують ще один вимір технічного забезпечення приватності. Їх значення полягає в можливості здійснювати аналіз або обчислення без розкриття вихідних даних у відкритому вигляді. Для правового регулювання це відкриває перспективу переосмислення поняття доступу до персональних даних: якщо інформація залишається зашифрованою протягом усього процесу обробки, традиційні уявлення про володіння та розпорядження даними потребують корекції [105].

Водночас використання складних криптографічних рішень висуває нові вимоги до інституційної спроможності суб’єктів, які застосовують ШІ. Висока обчислювальна вартість таких технологій, потреба в спеціалізованих знаннях і складність перевірки їх коректності означають, що вони не можуть бути універсальним рішенням для всіх сценаріїв. З методологічної позиції це

засвідчує необхідність пропорційного підходу, коли вибір технічних засобів захисту узгоджується з рівнем ризику та характером обробки даних [118].

Важливою є і взаємодія технічних засобів захисту з правовими принципами прозорості та підзвітності. З одного боку, застосування складних технологій може ускладнювати розуміння того, як саме функціонує система. З іншого – відмова від таких технологій під приводом складності позбавляє суб'єктів даних реального захисту. Методологічний виклик полягає в тому, щоб забезпечити баланс між технічною ефективністю та можливістю юридичної оцінки, не спрощуючи ані технологію, ані право [93].

У сучасному європейському дискурсі технічні засоби дедалі частіше розглядають як критерій оцінювання належної поведінки оператора ШІ-системи. Наявність або відсутність відповідних механізмів може впливати на висновок про дотримання принципів мінімізації, безпеки й обмеження мети обробки. Для України це означає, що подальший розвиток правової охорони персональних даних неминуче включатиме поступове зближення правових вимог із технічними стандартами та рекомендаціями міжнародних організацій [60; 103]. Унаслідок цього технічні засоби захисту персональних даних у сфері штучного інтелекту постають не як факультативне доповнення до правового регулювання, а як його практичний інструмент. Вони формують міст між абстрактними правовими принципами та реальними алгоритмічними процесами, у межах яких ці принципи повинні працювати. Саме крізь таку призму технології підвищення приватності можна розглядати як складову методології правової охорони персональних даних, а не як зовнішній технічний фактор.

У сучасній методології захисту персональних даних у сфері застосування штучного інтелекту вагомим стає етичний вимір. В умовах, коли право об'єктивно не встигає оперативно реагувати на технологічні зрушення, етичні принципи фактично виконують функцію проміжного регулятора, який визначає орієнтири допустимої поведінки ще до появи формалізованих норм [65; 116]. Саме в цій площині етика вже не є зовнішнім

щодо права явищем, вона поступово інтегрується в методологію правової охорони персональних даних.

Особливість етичного підходу у сфері ШІ полягає в тому, що він фокусується не лише на факті обробки персональних даних, а на ширших наслідках алгоритмічного впливу на автономію людини. Персональні дані в таких системах є не просто об’єктом зберігання чи передачі, а матеріалом для формування висновків, прогнозів і рішень, які можуть визначати доступ до ресурсів, можливостей або соціальних ролей. У цьому контексті приватність розглядають як умову збереження людської гідності та свободи самовизначення, а не як технічне обмеження доступу до інформації [63]. Такий підхід суттєво змінює методологічну логіку регулювання, оскільки переносить акцент із формальних процедур на оцінку реального впливу технологій на людину.

У міжнародному дискурсі етичні засади захисту персональних даних у ШІ формуються навколо кількох стабільних ідей, серед яких центральне місце посідає людиноцентричність. Вона означає, що автоматизовані системи не можна розглядати як нейтральні інструменти, позбавлені ціннісного виміру. Навпаки, кожне рішення щодо архітектури моделі, вибору навчальних даних або сценаріїв застосування містить припущення про допустимий рівень втручання в приватне життя. Методологічно це зобов’язує розробників й операторів ШІ оцінювати не лише юридичну коректність обробки, а й те, чи не призводить система до знеособлення людини або редукції її до сукупності статистичних характеристик.

Виразним є зміщення від суто нормативного регулювання до поєднання права з організаційними й технічними гарантіями. Зазначене зумовлено тим, що алгоритмічні системи функціонують у середовищі постійної зміни: моделі донавчаються, джерела даних розширюються, завдання використання можуть трансформуватися вже після введення системи в експлуатацію. За таких умов правові приписи, сформульовані як статичні правила, не завжди здатні адекватно охопити реальний характер

обробки персональних даних. Саме тому захист приватності дедалі більше залежить від того, які технічні рішення закладено в архітектуру системи та які внутрішні процедури супроводжують її функціонування [118]. Значна частина ризиків для прав суб'єктів даних виникає не на етапі формального збору інформації, а в процесі її подальшого використання. Алгоритмічні системи здатні формувати нові знання шляхом інференцій, поєднання різнорідних масивів і створення похідних профілів, які можуть бути чутливими. У такому контексті персональні дані не є лише «вхідним матеріалом», вони стають динамічним ресурсом, що постійно змінює свою правову якість. Це ускладнює застосування традиційних підходів, ґрунтованих на разовій згоді або формальній законності первинної обробки [64].

Тож набувають значення технічні механізми захисту, які дають змогу обмежити рівень втручання в приватну сферу не шляхом заборони, а через зміну способу обробки інформації. Ідеться про технологічні рішення, які знижують імовірність ідентифікації конкретної особи навіть за умови активного аналізу даних. Такі підходи поступово формують нову логіку правового мислення, у межах якої ефективність захисту оцінюють не лише за формальними критеріями, а й за фактичним рівнем ризику, що залишається для суб'єкта даних [58].

Одним із найпоказовіших прикладів такого зміщення є диференційована приватність. Її значення полягає в тому, що вона дає змогу зберігати аналітичну цінність великих масивів інформації, водночас обмежуючи можливість виокремлення записів. Для правового аналізу важливо, що такий підхід не усуває обробку персональних даних повністю, але знижує ймовірність шкоди до рівня, який можна вважати прийнятним з позицій пропорційності [58; 105].

Утім застосування диференційованої приватності не є нейтральним рішенням. Воно впливає на точність результатів, якість рішень, які приймають на основі ШІ. Це відчутно передусім у сферах, де помилка може

мати вагомі наслідки для людини. Отже, вибір параметрів такої технології фактично перетворюється на юридично значущий акт, який має враховувати баланс між інтересами інновацій і захистом прав [86]. Аналогом постає федеративне навчання. Відмова від централізованого збирання інформації знижує концентрацію ризиків і змінює розподіл відповідальності між учасниками системи. Персональні дані залишаються в межах організацій або пристроїв, а до розробника надходять лише агреговані параметри моделей. Для правової методології це означає можливість реалізації принципу мінімізації без радикального обмеження використання ШІ [64; 95].

Водночас навіть такі децентралізовані підходи не виключають можливості відновлення інформації за певних умов. Це засвідчує, що технічні механізми не можна розглядати як самодостатні гарантії. Їх ефективність залежить від того, чи супроводжуються вони організаційними процедурами контролю, внутрішнім розмежуванням доступу та регулярним переглядом архітектурних рішень [106].

Криптографічні методи, зокрема шифрування та багатосторонні обчислення, формують ще один рівень захисту. Вони дають змогу знизити ризики несанкціонованого доступу навіть у складних транскордонних сценаріях. Водночас розвиток таких технологій ставить перед правом нові питання щодо тлумачення доступу, володіння та відповідальності, адже традиційні категорії не завжди адекватно описують ситуації, коли дані ніколи не розкривають у відкритому вигляді [60]. Організаційний вимір захисту персональних даних у сфері ШІ тісно пов’язаний з технічними рішеннями. Навіть найскладніші засоби захисту втрачають сенс, якщо немає внутрішньої політики, процедури реагування на інциденти та чіткого розподілу ролей. У таких умовах відповідальність за приватність фактично розмивається, що ускладнює правозастосування. Саме тому сучасні підходи дедалі частіше акцентують на документації процесів і фіксації рішень як на елементі правової охорони [2; 46, с. 161–165; 64]. В українському контексті значення технічних й організаційних гарантій посилюється у зв’язку з гармонізацією

законодавства з європейськими стандартами. Формальне закріплення принципів захисту персональних даних не забезпечує їх реальної дії без розвитку практик управління даними. Запровадження технологій підвищення приватності може слугувати інструментом поступової адаптації до вимог ЄС, проте лише за умови, що вони інтегруються в ширшу методологію правового регулювання [37].

Тут знову вже неодноразово згаданий етичний вимір захисту персональних даних у сфері застосування штучного інтелекту виникає як відповідь на ситуацію, у якій формальна відповідність правовим вимогам не гарантує відсутності шкоди. Алгоритмічні системи можуть діяти в межах закону, водночас створювати стійкі ефекти втручання в приватне життя, які не фіксуються через класичні механізми правозастосування. Ідеться про випадки, коли персональні дані використовують не для прямої ідентифікації, а для формування статистичних профілів, прогнозів або категорій, що опосередковано визначають поведінку людини або її доступ до певних ресурсів. У таких умовах питання допустимості виходить за межі формального аналізу законності й потребує додаткових критеріїв оцінювання [116].

Особливість штучного інтелекту полягає в тому, що його вплив часто є кумулятивним і тривалим у часі. Окрема операція з обробки персональних даних може видаватися несуттєвою, однак коли поєднується з іншими даними та повторюваними алгоритмічними рішеннями, то формує цілісну картину приватного життя особи. Саме ця накопичувальна природа алгоритмічного впливу ускладнює правову оцінку, водночас актуалізує етичні підходи, які дають змогу враховувати не лише окремі дії, а й загальну траєкторію взаємодії людини із цифровими системами [63].

У сучасних міжнародних документах з етики ШІ простежується тенденція до розширеного розуміння приватності. Її трактують не лише як захист від несанкціонованого доступу до інформації, а як умову збереження автономії особи в умовах автоматизованого аналізу поведінки. Персональні

дані в цьому контексті є засобом конструювання реальності, а не просто відображенням фактів. Алгоритмічні системи визначають, які характеристики вважають значущими, які дії – типовими, а які – відхиленнями, що безпосередньо впливає на соціальне позиціонування людини [83].

Антропоцентричність як ключовий етичний орієнтир передбачає, що права й інтереси особи мають пріоритет над ефективністю автоматизації. Це не означає відмову від використання ШІ, однак потребує постійного зіставлення технологічної доцільності з потенційними наслідками для приватності. У практичному вимірі це виявляється, зокрема, у вимогах до обмеження сфер застосування автоматизованих рішень, які можуть істотно впливати на життєві шанси людини без належного людського контролю [65].

Водночас етичний підхід все-таки не зводиться до абстрактних декларацій. Його цінність полягає в здатності слугувати інструментом попереднього оцінювання ризиків ще до того, як постане необхідність правового втручання. Наприклад, навіть за наявності формальної згоди суб’єкта даних використання персональної інформації для побудови поведінкових прогнозів можна розглядати як етично проблематичне, якщо особа не усвідомлює масштабу й наслідків такої обробки. У цьому сенсі етичні критерії надають можливість виявляти дисбаланс між поінформованістю суб’єкта та реальними можливостями впливу на алгоритмічні процеси [127].

Це порушує питання прозорості обробки даних. З одного боку, є вимога пояснюваності рішень, яка пов’язана з правом людини розуміти, як обробляють її дані. З іншого боку, технічна складність сучасних моделей та комерційні інтереси розробників обмежують можливість повного розкриття алгоритмічної логіки. Етичний підхід не потребує абсолютної прозорості, але наполягає на достатньому рівні зрозумілості, який дає змогу оцінити потенційні ризики й оскаржити рішення, що має негативні наслідки для суб’єкта даних [138]. Також слід урахувати теоретичну можливість

упередженості даних, яка виникає під час використання систем штучного інтелекту. Алгоритмічні системи відтворюють закономірності, закладені в навчальних вибірках, які нерідко формувалися в умовах соціальної нерівності. Унаслідок цього ШІ може посилювати дискримінаційні ефекти, навіть якщо розробники не мали такої мети. Для прикладу можна й зараз порівняти використання будь-яких двох генеративних моделей між собою, умовно контраверсійним політичним запитанням. Залежно від того, якою саме мовою буде написано запит, відповідь буде варіюватися на правових основах держави, якій мова запиту буде належати. З правової позиції довести наявність дискримінації в таких випадках буває складно, оскільки шкода часто має непрямий характер, в окремих ізольованих випадках становить не таку істотну шкоду. Водночас слід урахувати, що це фактично є обмеженням доступу до інформації та своєрідною маніпуляцією. Етичний аналіз дає змогу виявити ці ризики на ранніх етапах і скоригувати підходи до добору даних або налаштування моделей [131].

Концепція справедливості тут є вкрай важливою. В етичних документах з ШІ розглядають як необхідність уникнення систематичного виключення або маргіналізації певних груп. Для методології захисту персональних даних це означає, що оцінювання допустимості обробки має враховувати не лише індивідуальні, а й групові наслідки. Навіть якщо права конкретної особи формально не порушено, алгоритмічні практики можуть створювати стійкі негативні ефекти для певних соціальних категорій, що потребує уваги регулятора й розробників [63].

Етичний вимір тісно пов’язаний із принципом підзвітності. Автоматизований характер прийняття рішень не можна використовувати як аргумент для уникнення відповідальності. Навпаки, складність алгоритмічних систем посилює потребу в чіткому визначенні суб’єктів, відповідальних за їх функціонування. З етичної позиції неприйнятною є ситуація, коли негативні наслідки для приватності пояснюють «помилкою

алгоритму» без можливості ідентифікувати відповідального учасника процесу [116].

Для національного контексту України етичні підходи мають особливе значення в умовах трансформації правової системи й упровадження європейських стандартів. Формальне запозичення норм без урахування їх ціннісного підґрунтя може призвести до ситуації, коли вимоги щодо захисту персональних даних виконують декларативно. Інтеграція етичних орієнтирів у методологію регулювання дає змогу наповнити правові норми реальним змістом і забезпечити їх адаптацію до конкретних соціальних і технологічних умов [90]. Водночас надмірна опора на етичні механізми становить ризик розмивання правових гарантій. Якщо етику використовують як заміну чітких правових вимог, це може створити простір для довільного тлумачення допустимості обробки персональних даних. Тому методологічно виправданим є підхід, за якого етичні принципи слугують орієнтиром для розвитку права, але не підміняють юридично обов'язкові норми [63].

Окремий вимір методології захисту персональних даних у сфері застосування штучного інтелекту пов'язаний з рівнем обізнаності учасників цифрових процесів і розвитком механізмів саморегуляції. Умови алгоритмічної обробки інформації вирізняються складністю, багаторівневістю та швидкою зміною технічних рішень, що об'єктивно ускладнює ефективність виключно нормативного впливу.

За відсутності належного розуміння принципів роботи ШІ навіть формально коректні правові конструкції залишаються недостатньо ефективними, оскільки не трансформуються в реальні практики використання даних. Проблема обізнаності виявляється насамперед на рівні розробників й операторів ШІ-систем. Значну частину рішень, які мають безпосередній вплив на приватність, ухвалюють не юристи, а інженери, аналітики даних і продуктові менеджери. Саме вони визначають, які дані будуть зібрані, як довго їх зберігатимуть, чи можливе повторне використання наборів для інших завдань, як результати обробки інтегрують у бізнес-

процеси. За відсутності базових знань у сфері захисту персональних даних ці рішення часто приймають з орієнтованістю на технічну ефективність або економічну доцільність, без належної оцінки правових і соціальних наслідків [64, с. 4–9]. Освітній компонент у цьому контексті набуває методологічного значення. Ідеться не лише про формальне навчання норм законодавства, а про формування у фахівців здатності мислити категоріями ризику, пропорційності й відповідальності. Програми підготовки у сфері ІТ дедалі частіше охоплюють елементи data protection й етики ШІ, проте їх зміст нерідко залишається фрагментарним. Несформованість системного підходу призводить до того, що захист персональних даних сприймають як зовнішню вимогу, а не як внутрішню характеристику якості технологічного рішення [59].

Обізнаність суб’єктів – постачальників даних є вкрай важливою. Умови використання ШІ-систем у повсякденному житті створюють ситуацію, у якій людина взаємодіє з алгоритмами постійно, але зрідка усвідомлює масштаби й наслідки такої взаємодії. Персональні дані збирають й аналізують у фоновому режимі, часто без чітко окреслених моментів прийняття рішень з боку користувача. Це знижує ефективність класичних механізмів контролю, ґрунтованих на активних діях суб’єкта, зокрема наданні або відкликанні згоди [127]. За таких умов підвищення обізнаності набуває значення не як формальна інформованість, а як здатність людини орієнтуватися в цифровому середовищі, розуміти базову логіку алгоритмічних рішень і потенційні ризики для приватності. Інформаційні кампанії, інструменти прозорості, доступні пояснення принципів роботи ШІ можуть виконувати компенсаторну функцію, частково зменшуючи інформаційну асиметрію між суб’єктом даних й оператором системи [106].

Саморегуляцію у сфері застосування штучного інтелекту розглядають як ще один елемент методології, здатний доповнювати правове регулювання.

На відміну від жорстких нормативних приписів, саморегулятивні механізми дають змогу враховувати галузеву специфіку та швидко

адаптуватися до технологічних змін. Кодекси поведінки, внутрішні стандарти компаній, галузеві рекомендації формують поле допустимих практик, яке може бути гнучкішим, ніж законодавство, водночас достатньо стабільним для забезпечення передбачуваності [118].

Ефективність саморегуляції безпосередньо залежить від наявності зовнішніх стимулів і контролю. Без ризику юридичної відповідальності або репутаційних втрат саморегулятивні документи можуть перетворюватися на формальність. Саме тому в європейських підходах саморегуляцію розглядають не як альтернативу праву, а як його продовження, що діє в межах, окреслених законодавством, і підлягає оцінюванню з боку наглядових органів [124].

Цікавим є розвиток моделей співрегулювання, у межах яких держава, бізнес і професійні спільноти спільно формують правила поведінки у сфері ШІ.

Такий підхід дає змогу поєднати експертні знання розробників із правовими вимогами та суспільними очікуваннями. Методологічно співрегулювання сприяє легітимації правил, оскільки їх сприймають не як нав’язані «згори», а як результат узгодження інтересів. У сфері захисту персональних даних це має важливе значення, адже чимало рішень потребують балансу між інноваціями й охороною приватності [103].

Для України розвиток саморегулятивних механізмів і культури обізнаності може стати важливим компенсатором обмежених інституційних ресурсів. В умовах реформування законодавства та поступової адаптації до європейських стандартів не всі вимоги можуть бути ефективно забезпечені через державний контроль. Саме тому залучення професійних спільнот, освітніх платформ і бізнес-асоціацій до формування практик захисту персональних даних у сфері ШІ набуває стратегічного значення [90].

Водночас слід уникати ідеалізації освітніх і саморегулятивних підходів.

Вони не здатні замінити правові гарантії та не можуть бути використані як виправдання для зниження стандартів захисту. Їх роль полягає в

підвищенні якості правозастосування, формуванні спільного розуміння ризиків і відповідальності, але остаточні межі допустимого втручання в приватність слід визначати на рівні права [22].

У межах цього дисертаційного дослідження методологічну основу становить комплексна ризик-орієнтована, антропоцентрична та міждисциплінарна модель, відповідно до якої правова охорона персональних даних у сфері штучного інтелекту розглядається не лише як сукупність нормативних заборон і дозволів, а як система превентивних, інституційних, технічних і процесуальних гарантій, спрямованих на запобігання шкоді правам людини.

Освітній, комунікаційний і саморегулятивний виміри формують завершальний елемент методології захисту персональних даних у сфері штучного інтелекту. Вони забезпечують зв’язок між нормативними приписами, технічними рішеннями та повсякденними практиками використання ШІ. Саме через поєднання цих елементів можливе формування стійкої культури захисту приватності, у межах якої персональні дані розглядають не як побічний ресурс цифрового розвитку, а як цінність, що потребує постійної уваги й відповідального ставлення.

Отже, за підрозділом 1.3 можна зробити такі висновки:

1. Методологія дослідження має комплексний характер.
2. Основою є поєднання юридичних, технічних, етичних та інституційних підходів.
3. Центральним є ризик-орієнтований підхід.
4. Правова охорона персональних даних у сфері ШІ повинна мати превентивний характер.
5. Правовий захист має забезпечувати реальне поновлення порушених прав, пояснення автоматизованих рішень, людське втручання та ефективне оскарження.

Висновки до розділу 1

У першому розділі сформовано теоретико-методологічне підґрунтя для подальшого аналізу правової охорони та захисту персональних даних у сфері застосування штучного інтелекту. Доведено, що використання ШІ істотно змінює характер інформаційних правовідносин, оскільки персональні дані виконують не допоміжну роль, а перетворюються на базовий ресурс алгоритмічних систем. Унаслідок цього зростає інтенсивність втручання в приватну сферу особи, а також підвищується складність прогнозування наслідків обробки даних для прав і свобод людини.

У межах аналізу понятійно-категоріального апарату встановлено, що брак універсального визначення штучного інтелекту у праві пов’язаний з динамічністю технологічного розвитку. Сучасні нормативні й доктринальні підходи акцентують не стільки на технічній природі ШІ, скільки на його функціональних характеристиках, зокрема автономності, адаптивності та здатності до генерації рішень й інференцій. Саме ці властивості визначають специфіку ризиків для персональних даних і потребують особливих правових запобіжників.

Дослідження історії розвитку штучного інтелекту дало змогу встановити, що еволюція алгоритмічних технологій відбувалася паралельно зі посиленням ролі даних у процесах навчання та прийняття рішень. Якщо ранні моделі ШІ були відносно не залежними від масових масивів інформації, то сучасні системи машинного та глибинного навчання безпосередньо залежать від великих наборів персональних даних. Це зумовлює посилення впливу ШІ на приватність й актуалізує необхідність переосмислення класичних правових підходів до захисту інформації.

У процесі аналізу генези правового регулювання захисту персональних даних в Україні встановлено, що національна модель формувалася під вирішальним впливом європейських стандартів першого покоління і протягом тривалого часу орієнтувалася на традиційні сценарії обробки

інформації. Доведено, що чинне законодавство хоча й містить базові принципи охорони персональних даних, не враховує специфіки алгоритмічної обробки, зокрема автоматизованого прийняття рішень, профілювання та повторного використання даних для навчання ШІ-систем.

Проаналізовано стан наукового розроблення проблеми захисту персональних даних у контексті застосування штучного інтелекту в Україні. Встановлено, що національна доктрина знаходиться на етапі становлення та вирізняється фрагментарністю, а також значною залежністю від міжнародних підходів і концепцій. Це засвідчує брак цілісної національної концепції правової охорони персональних даних у сфері ШІ й актуалізує потребу в подальших системних дослідженнях.

Обґрунтовано, що сучасний етап розвитку правового регулювання захисту персональних даних в Україні знаходиться у фазі активного реформування, зумовленого як євроінтеграційними зобов'язаннями, так і внутрішньою логікою цифрової трансформації публічного управління та економіки. Констатовано, що впровадження алгоритмічних систем у діяльність органів публічної влади посилює вимоги до правової визначеності, прозорості та підзвітності обробки персональних даних. У межах методологічного аналізу доведено, що ефективна правова охорона персональних даних у сфері застосування ШІ не може ґрунтуватися виключно на нормативних приписах. Сучасна модель захисту має поєднувати правові, технічні й організаційні механізми, які функціонують у взаємозв'язку та взаємному доповненні. Такий підхід дає змогу перейти від формального дотримання процедур до реального управління ризиками для прав людини.

Встановлено, що ризик-орієнтований підхід є ключовою методологічною основою сучасного регулювання захисту персональних даних у сфері ШІ. Його значення полягає в зміщенні акценту з формальної законності окремих операцій на оцінку потенційної шкоди, яка може виникати впродовж усього життєвого циклу алгоритмічної системи. У цьому

контексті важливе значення має оцінка впливу на захист персональних даних як інструмент превентивного виявлення та мінімізації ризиків.

Доведено, що принципи privacy by design і privacy by default виконують не лише нормативну, а й методологічну функції, визначаючи спосіб проєктування та використання ШІ-систем. Їх застосування сприяє переорієнтації правового регулювання з реактивної моделі реагування на порушення до проактивного формування безпечних технологічних рішень, інтегрованих в архітектуру систем ще на етапі розроблення.

Обґрунтовано значення технічних механізмів захисту персональних даних як практичного інструменту реалізації правових вимог у сфері застосування ШІ. З'ясовано, що технології підвищення приватності, децентралізовані моделі навчання та криптографічні засоби змінюють архітектуру обробки даних і знижують імовірність непропорційного втручання в приватне життя особи. Водночас акцентовано, що ефективність таких механізмів залежить від їх поєднання з організаційними та правовими гарантіями.

Встановлено, що інституційний нагляд у сфері захисту персональних даних під час застосування ШІ має еволюціонувати від постфактумного реагування на порушення до превентивних і супровідних форм контролю. Це потребує підвищення регуляторної спроможності органів державної влади, розвитку експертного потенціалу та впровадження механізмів аудиту й сертифікації алгоритмічних систем.

Акцентовано на значенні етичного виміру як складової методології правової охорони персональних даних у сфері ШІ. Доведено, що етичні принципи людиноцентричності, недискримінації, прозорості та підзвітності виконують компенсаторну функцію в умовах нормативної невизначеності та сприяють формуванню практик відповідального використання алгоритмічних технологій.

Узагальнюючи результати розділу, встановлено, що застосування штучного інтелекту зумовлює трансформацію парадигми захисту

персональних даних, у межах якої право дедалі більше орієнтується на управління ризиками та соціальними наслідками алгоритмічної обробки. Це потребує переосмислення традиційних правових категорій і формування комплексної моделі правової охорони, здатної забезпечити баланс між інноваційним розвитком і захистом прав людини.

Сформульовані в першому розділі теоретичні висновки та методологічні орієнтири створюють наукове підґрунтя для подальшого порівняльно-правового аналізу закордонних моделей регулювання захисту персональних даних у сфері штучного інтелекту й обґрунтування напрямів удосконалення національного законодавства.

РОЗДІЛ 2
АНАЛІЗ ЗАРУБІЖНОГО ДОСВІДУ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ШТУЧНОГО ІНТЕЛЕКТУ

2.1. Поняття та класифікація персональних даних у сфері штучного інтелекту (зарубіжний досвід)

Розвиток технологій штучного інтелекту безпосередньо зумовив перегляд традиційних підходів до розуміння персональних даних, що привело до суттєвого переосмислення поняття персональних даних у контексті застосування систем штучного інтелекту як у національних, так і зарубіжних правопорядках та міжнародних нормативно-рекомендаційних документах останнього десятиліття. Якщо класичні підходи пов’язували персональні дані насамперед із наявністю прямих ідентифікаторів фізичної особи, то сучасні моделі регулювання ґрунтуються на функціональному розумінні інформації та її здатності впливати на становище людини в алгоритмічному середовищі. У документах Європейської ради із захисту даних акцентовано, що вирішальними є не форма даних і не спосіб їх первинного отримання, а можливість їх використання для індивідуалізації особи або формування щодо неї значущих висновків у межах автоматизованих процесів [61; 106]. Це означає відхід від вузького формально-юридичного критерію ідентифікації та перехід до оцінювання реального технологічного потенціалу обробки.

У цьому контексті персональні дані в системах штучного інтелекту розглядають як динамічний об’єкт правового захисту. Вони охоплюють не лише інформацію, безпосередньо надану суб’єктом даних або зібрану про нього з визначеною метою, а й результати подальшої алгоритмічної обробки, збагачення та комбінування з іншими масивами інформації. Така позиція

простежується, зокрема, у рекомендаціях Ради Європи та ЮНЕСКО, де зауважено, що штучний інтелект змінює логіку інформаційних процесів, перетворюючи дані з пасивного ресурсу на активний елемент прийняття рішень і прогнозування [89; 116].

Закордонні правопорядки та міжнародні організації сформували розширене бачення змісту персональних даних у середовищі штучного інтелекту. Майже всі сучасні підходи до персональних даних не є ізольованим масивом відомостей, що має сталий обсяг і значення, його розглядають як інформаційну категорію, зміст якої зумовлений функціями алгоритмічної обробки. Це означає, що правова оцінка інформації дедалі частіше ґрунтується не на її формальних ознаках, а на тому, яку роль вона відіграє в автоматизованих процесах аналізу, прийняття рішень і прогнозування.

У документах Європейської ради із захисту даних зазначено, що штучний інтелект істотно знижує поріг ідентифікованості особи, оскільки дає змогу встановлювати зв’язок між даними та конкретною фізичною особою навіть за відсутності традиційних ідентифікаторів. Персональні дані в цьому контексті охоплюють не лише інформацію, яка безпосередньо стосується ідентифікації, а й будь-які відомості, здатні в алгоритмічному середовищі впливати на формування індивідуалізованих рішень або висновків щодо особи [61; 106]. Такий підхід відображає перехід від статичного до процесуального розуміння персональних даних, у межах якого вирішальними є не початковий зміст інформації, а результати її використання. Міжнародні рекомендації Ради Європи, ЮНЕСКО та OECD засвідчують, що в умовах застосування систем штучного інтелекту персональні дані набувають багаторівневої структури. Вони охоплюють первинні відомості, які були зібрані безпосередньо від суб’єкта даних, а також інформацію, що виникає внаслідок подальшої обробки, агрегування та аналітичного узагальнення. У такій моделі персональні дані розглядають як результат безперервного інформаційного процесу, а не як разово зафіксований об’єкт правовідносин

[103; 116]. Це зумовлює необхідність урахування повного життєвого циклу даних під час визначення обсягу правового захисту.

В іноземних системах персональні дані в системах штучного інтелекту оцінюють крізь призму потенційної шкоди для прав і свобод людини. У сучасних зарубіжних документах дедалі частіше використовують ризик-орієнтовану модель, відповідно до якої персональними визнають будь-які дані, здатні разом з алгоритмічними інструментами призвести до дискримінації, необґрунтованого обмеження прав або непрозорого прийняття рішень. Такий підхід закріплений у міжнародних стандартах управління ризиками штучного інтелекту та рекомендаціях з етики цифрових технологій, що орієнтують правове регулювання на фактичні наслідки використання даних, а не лише на їхні формальні характеристики [64; 86].

У такому випадку персональні дані втрачають виключно інформаційний вимір, їх розглядають як елемент соціально-правових процесів, у межах яких алгоритмічні системи впливають на реалізацію прав людини. Саме тому акцентують на необхідності забезпечення прозорості та підзвітності алгоритмічної обробки даних, що безпосередньо пов’язано з розширеним розумінням персональних даних у сфері штучного інтелекту. Така концепція створює підґрунтя для подальшого аналізу проблем ідентифікації та реідентифікації осіб у процесах автоматизованої обробки даних і машинного навчання. Закордонні дослідження та правозастосовна практика засвідчують, що навіть за відсутності прямих ідентифікаторів сучасні алгоритмічні системи здатні відновлювати зв’язок між даними та конкретною особою шляхом аналізу поведінкових патернів, просторово-часових характеристик або технічних параметрів цифрової взаємодії. Класичним і простим прикладом такої ситуації є використання великих масивів знеособлених даних для навчання генеративних моделей, коли поєднання різних джерел інформації створює умови для повторної ідентифікації користувачів.

Як розвиток концептуальних положень щодо динамічного характеру персональних даних, сформульованих у попередньому підрозділі, зазначимо, що в зарубіжних підходах увагу зосереджують на проблемі ідентифікації та реідентифікації осіб у процесах автоматизованої обробки даних і машинного навчання. У контексті застосування систем штучного інтелекту ідентифікацію більше не розглядають як разовий акт встановлення особи на підставі прямих ідентифікаторів, вона постає як безперервний алгоритмічний процес, що ґрунтується на аналізі сукупності ознак, поведінкових патернів і статистичних кореляцій. У сучасних міжнародних документах зазначено, що здатність алгоритмічних систем до ідентифікації осіб значно перевищує можливості традиційних інформаційних технологій. Машинне навчання дає змогу встановлювати зв’язки між фрагментами даних, які поодинці не мають ідентифікаційного значення, але в сукупності формують унікальний цифровий профіль фізичної особи. У цьому сенсі ідентифікація набуває імовірнісного характеру: достатнім визнають не абсолютне встановлення особи, а досягнення такого рівня точності, який дає змогу впливати на її правове або соціальне становище.

Особливої актуальності проблема ідентифікації набуває у зв’язку з повторним використанням даних для завдань, відмінних від тих, для яких їх було зібрано первинно. У міжнародній практиці дедалі частіше визнають, що дані, які на момент збору вважали анонімними або такими, що не дають змоги встановити особу, можуть набути персонального характеру внаслідок подальшої алгоритмічної обробки та поєднання з іншими масивами інформації. Саме тому в позиціях європейських наглядових органів зауважено, що оцінювання ідентифікованості слід здійснювати з огляду на фактичні технологічні можливості, а не формальні характеристики наборів даних [61; 106].

Іноземна правозастосовна практика має численні приклади того, як алгоритмічні системи створюють умови для реідентифікації осіб навіть за наявності заходів знеособлення. Використання великих обсягів відкритих

даних для навчання генеративних моделей продемонструвало, що поєднання текстових, поведінкових і контекстуальних ознак надає можливість відновлювати зв’язок між даними та конкретними користувачами. Судові спори, пов’язані з використанням контенту із цифрових платформ для машинного навчання, виявили, що публічна доступність інформації не усуває ризиків для приватності, якщо така інформація може бути повторно використана для створення індивідуалізованих профілів або прогнозних моделей [117].

Показовим прикладом регуляторного реагування на ці ризики є практика італійського наглядового органу із захисту персональних даних щодо діяльності сервісу ChatGPT. Тимчасова заборона на використання сервісу, а згодом дозвіл на його роботу за умови впровадження додаткових гарантій засвідчили, що проблему ідентифікації та реідентифікації розглядають регулятори як реальну й таку, що потребує превентивного правового втручання [99]. Подальше накладення значного штрафу за порушення вимог законодавства про захист даних підтвердило, що ризики, пов’язані з непрозорою обробкою інформації для навчання моделей, оцінюють як системні й такі, що впливають на права широкого кола осіб [98].

У закордонних підходах також акцентовано на тому, що реідентифікація може відбуватися не лише на рівні окремих осіб, а й на рівні груп, що об’єднуються за певними ознаками. Алгоритмічні системи здатні формувати групові профілі на основі статистичних закономірностей, які згодом використовують для автоматизованого прийняття рішень щодо конкретних осіб. Така групова ідентифікація створює ризики непрямої дискримінації та стирання меж між персональними й неперсональними даними, що визнано в міжнародних рекомендаціях з етики штучного інтелекту та захисту прав людини [62; 103].

Важливим аспектом зарубіжних підходів є також визнання того, що реідентифікація не завжди має на меті встановлення особи в класичному розумінні. У низці випадків достатнім є встановлення стійкого зв’язку між

даними й певним цифровим профілем, який використовують для прогнозування поведінки або оцінювання ризиків. У таких ситуаціях навіть відсутність імені чи інших традиційних ідентифікаторів не усуває необхідності застосування режиму правового захисту персональних даних, оскільки алгоритмічні рішення безпосередньо впливають на реалізацію прав і свобод людини.

Отже, в іноземному досвіді ідентифікацію та реідентифікацію осіб у процесах автоматизованої обробки даних і машинного навчання розглядають як ключовий фактор, що визначає межі правового захисту персональних даних у сфері штучного інтелекту. Зміщення фокуса від формального підходу до ідентифікації та перехід до оцінювання реальних алгоритмічних можливостей дає змогу адекватно враховувати ризики для приватності та прав людини, що виникають у сучасних цифрових екосистемах.

Розвиток алгоритмічних технологій призвів до якісної зміни характеру інформації, яку використовують для прийняття рішень: поряд із первинними персональними даними дедалі важливішими стають результати їх аналітичної обробки. У зарубіжних підходах цю трансформацію осмислюють не як технічну деталь, а як фундаментальний виклик традиційним моделям правового регулювання, побудованим на уявленні про дані як про фіксований і порівняно стабільний об’єкт правовідносин.

У міжнародних нормативних й аналітичних документах похідні дані розглядають переважно як інформацію, що виникає внаслідок обробки первинних масивів, але не зводиться до їх простого агрегування. Ідеться про нові знання, закономірності або характеристики, які не були безпосередньо відомі до застосування алгоритмічних методів. Інференційні дані є різновидом таких похідних відомостей і є висновками щодо властивостей, поведінкових схильностей або ймовірних дій особи, сформованих на основі статистичних моделей і машинного навчання. Прогнозовані дані своєю чергою орієнтовані на майбутній вимір, їх використовують для передбачення

результатів, ризиків або сценаріїв розвитку подій щодо конкретної особи або групи осіб.

Ключова особливість інференційних і прогнозованих даних полягає в тому, що їх не надає суб'єкт персональних даних безпосередньо і часто він їх не усвідомлює як такі, що існують. Водночас саме ці дані дедалі частіше стають підґрунтям для автоматизованого прийняття рішень у сферах кредитування, страхування, зайнятості, соціального забезпечення, цифрових платформ і державного управління. У зарубіжних дослідженнях акцентовано, що вплив інференційних даних на реалізацію прав людини може бути значно глибшим, ніж вплив первинної інформації, оскільки такі дані формують основу для оцінювання надійності, платоспроможності, ризиків або соціального статусу особи [83; 131].

Така обставина зумовлює активну дискусію щодо правового статусу інференційних і прогнозних даних. У традиційних моделях захисту персональних даних правова охорона пов'язана з фактом ідентифікації особи або походженням інформації. Проте у випадку інференційних даних такі критерії виявляються недостатніми, оскільки алгоритмічні висновки можуть суттєво впливати на права та свободи людини навіть тоді, коли вони формально не підпадають під класичне визначення персональних даних. У закордонних рекомендаціях дедалі частіше пропонують керуватися функціональним підходом, відповідно до якого правовий режим визначають з огляду на наслідки використання інформації, а не лише на її формальні ознаки [103; 104].

Позиції європейських і міжнародних інституцій засвідчують поступове визнання того, що інференційні дані слід розглядати як об'єкт правового захисту у випадках, коли їх використовують для індивідуалізованого впливу або автоматизованого прийняття рішень. У висновках Європейської ради із захисту даних зауважено, що алгоритмічні висновки, сформовані щодо конкретної особи, не можуть бути виведені з-під дії режиму захисту лише на тій підставі, що вони є результатом аналітичної обробки, а не

безпосереднього збору інформації [106]. Аналогічна логіка простежується в рекомендаціях Глобальної асамблеї з питань приватності, де акцентовано на необхідності поширення принципів захисту персональних даних на весь ланцюг алгоритмічної обробки [62].

Посилену увагу в зарубіжному дискурсі привертає питання прозорості інференційних і прогнозних даних. На відміну від первинних персональних даних, джерело яких може бути чітко визначеним, алгоритмічні висновки часто формуються на основі складних моделей, логіка роботи яких є непрозорою навіть для їх розробників. Це створює суттєві складнощі для реалізації прав суб'єктів даних, зокрема права на доступ до інформації, права на виправлення та права на заперечення проти автоматизованого прийняття рішень. У міжнародних рекомендаціях з управління ризиками штучного інтелекту зазначено, що непрозорість алгоритмічних інференцій підвищує ризик помилкових або дискримінаційних рішень, тожі вимагає додаткових правових та організаційних гарантій [64; 86].

Практичні приклади використання інференційних даних у діяльності великих цифрових платформ і розробників генеративних моделей підтверджують ці ризики. Алгоритмічні системи, навчені на великих масивах відкритих і напіввідкритих даних, здатні відтворювати та посилювати соціальні стереотипи, формуючи висновки щодо осіб або груп на основі непрямих ознак. Згідно із закордонними аналітичними звітами, такі інференції можуть призводити до непрямої дискримінації навіть у тих випадках, коли чутливі категорії даних формально не використовують [83; 116]. Це знову ж таки ставить під сумнів ефективність формального підходу до класифікації інформації.

Саме тому розглядають проблему відмежування інференційних даних від статистичних або узагальнених результатів аналізу. У міжнародних документах зазначено, що вирішальне значення має не ступінь узагальнення інформації, а можливість її застосування щодо конкретної особи або чітко визначеної групи осіб. Якщо результати алгоритмічного аналізу

використовують для прийняття рішень, які мають індивідуалізовані наслідки, такі дані слід розглядати як такі, що потребують правового захисту, незалежно від їх статистичного характеру [59].

Зарубіжний досвід також засвідчує тісний зв'язок інференційних і прогнозованих даних із проблемою групової ідентифікації. Алгоритмічні системи часто оперують не індивідуальними профілями, а типовими моделями поведінки, які застосовують до широких категорій осіб. Унаслідок цього окремі індивіди можуть зазнавати правових або соціальних наслідків на підставі характеристик, приписаних їм як членам певної групи. Міжнародні рекомендації з етики штучного інтелекту спрямовують увагу на те, що такий підхід створює ризики колективної дискримінації та розмиває традиційні межі між персональними й неперсональними даними [62; 116].

У регуляторних документах після 2023 року дедалі чіткіше простежується тенденція до включення інференційних і прогнозних даних у сферу ризик-орієнтованого регулювання. Міжнародні стандарти управління ризиками штучного інтелекту пропонують оцінювати алгоритмічну обробку даних з огляду на ймовірність шкоди, масштаб впливу й можливість ефективного людського контролю. У межах такого підходу інференційні дані розглядають не як другорядний продукт обробки, а як ключовий фактор, що визначає рівень ризику для прав і свобод людини [60; 64; 86].

Отже, у зарубіжних підходах похідні, інференційні та прогнозні дані поступово визнають самостійним об'єктом правового захисту у сфері штучного інтелекту. Відхід від формального критерію походження інформації та перехід до функціонально-наслідкового аналізу надає можливість адекватніше враховувати специфіку алгоритмічних процесів і забезпечувати ефективний захист прав людини в умовах розвитку сучасних цифрових технологій.

У межах іноземних підходів до правового регулювання штучного інтелекту класифікацію персональних даних також дедалі частіше здійснюють з огляду на життєвий цикл алгоритмічних систем, а не виключно

на підставі формальних ознак інформації. Такий підхід є логічним продовженням функціонального розуміння персональних даних і відображає прагнення регуляторів адаптувати правові механізми до реальних практик розроблення, упровадження та експлуатації систем штучного інтелекту. У міжнародних рекомендаціях зазначено, що ризики для прав і свобод людини виникають на різних етапах функціонування ШІ, а отже, правова оцінка обробки персональних даних має враховувати контекст і мету їх використання [59; 64; 86].

Одним із базових елементів такої класифікації є розмежування персональних даних, що використовують на стадії навчання алгоритмічних моделей. Навчальні дані охоплюють великі масиви інформації, зібраної з різних джерел, зокрема з відкритих цифрових платформ. У зарубіжних документах акцентовано, що саме на цій стадії постають підвищені ризики непрозорого використання персональних даних, оскільки обробку часто здійснюють у масштабах, які ускладнюють забезпечення принципів мінімізації та цільового обмеження. Практика навчання генеративних моделей продемонструвала, що навіть фрагментарні або знеособлені відомості можуть у сукупності формувати персональні профілі, що потребує поширення на навчальні дані режиму правового захисту [59; 106].

Окрему категорію становлять вхідні дані, які надходять до систем штучного інтелекту в процесі їх безпосереднього використання. Ідеться про інформацію, яку вводять користувачі або отримує система в реальному часі для виконання конкретних функцій. Такі дані часто мають високий ступінь персоналізації, оскільки безпосередньо пов’язані з поведінкою, запитами або рішеннями конкретних осіб. Саме на цьому етапі значущими є питання прозорості, інформування суб’єктів даних і забезпечення можливості контролю за алгоритмічною обробкою інформації [64; 86]. Експлуатаційні дані охоплюють результати функціонування систем штучного інтелекту, зокрема лог-файли, метадані, згенеровані висновки й інші відомості, що виникають у процесі взаємодії користувачів із системою. У міжнародних

документах зазначено, що експлуатаційні дані часто залишаються поза увагою традиційних моделей захисту персональних даних, хоча саме вони можуть містити детальну інформацію про поведінкові патерни та цифрові звички осіб. Зарубіжний досвід засвідчує, що ігнорування правового режиму таких даних створює ризики повторного використання інформації для нових, неочікуваних завдань, зокрема для донавчання алгоритмічних моделей або профілювання користувачів [59].

У межах життєвого циклу систем штучного інтелекту виокремлюються дані, що використовують на стадіях тестування та валідації. Хоча ці дані формально можуть не використовувати для прийняття рішень щодо конкретних осіб, у зарубіжних підходах визнано, що вони також можуть містити персональну інформацію та впливати на якість і наслідки подальшої експлуатації системи. Належну правову оцінку таких даних розглядають як необхідну умову запобігання системним помилкам й упередженням, які згодом можуть мати дискримінаційний характер.

Класифікація персональних даних у контексті життєвого циклу ШІ тісно пов’язана з ризик-орієнтованими моделями регулювання, запропонованими в міжнародних стандартах і рекомендаціях. Одна й та сама інформація може створювати різний рівень ризику залежно від того, на якому етапі та з якою метою її використовують. Такий підхід надає можливість відмовитися від універсальних правил і перейти до диференційованого правового регулювання, орієнтованого на фактичний вплив алгоритмічної обробки на права людини [64; 60]. Зарубіжний досвід також засвідчує поступове розширення класифікаційних критеріїв за рахунок урахування ролі персональних даних у формуванні алгоритмічних моделей. Дані, які безпосередньо впливають на параметри моделі або її поведінку в реальному середовищі, розглядають як такі, що потребують підвищеного рівня правового контролю. Зазначене пов’язано з тим, що помилки або упередження, закладені на стадії навчання, можуть відтворювати протягом усього періоду експлуатації системи, впливаючи на невизначене коло осіб.

Отже, класифікація персональних даних у системах штучного інтелекту в зарубіжних підходах виходить за межі традиційних поділів і набуває процесуального характеру. Орієнтованість на життєвий цикл ШІ та рівень ризику дає змогу точніше визначати обсяг правового захисту і створює підґрунтя для побудови комплексних механізмів регулювання, здатних реагувати на динаміку сучасних алгоритмічних технологій.

В іноземних підходах до правового регулювання штучного інтелекту одним із центральних елементів є питання чутливих категорій персональних даних, використання яких в алгоритмічних системах пов’язане з підвищеними ризиками для прав і свобод людини. На відміну від класичних моделей захисту персональних даних, де перелік спеціальних категорій мав порівняно стабільний характер, сучасні міжнародні документи фіксують тенденцію до його розширення та функціонального переосмислення з огляду на специфіку автоматизованої обробки [62; 89; 116]. У цьому контексті біометричні дані розглядають як одну з найпроблемніших категорій інформації в системах штучного інтелекту, бо їх використання в технологіях розпізнавання облич, голосу, ходи або інших фізіологічних характеристик створює умови для постійної ідентифікації та моніторингу осіб у публічному й приватному просторі. У міжнародних рекомендаціях акцентовано, що масштабованість й автоматизований характер таких технологій істотно змінюють баланс між публічними інтересами та правом на приватність, оскільки біометричні системи дають змогу здійснювати масове спостереження без необхідності індивідуального втручання людини [70; 116].

Зарубіжна регуляторна практика засвідчує, що біометричні дані в контексті ШІ розглядають не лише як інформацію, що безпосередньо ідентифікує особу, а й як інструмент поведінкового аналізу та прогнозування. Системи, що використовують біометричні параметри, здатні формувати висновки щодо емоційного стану, рівня уваги або потенційної небезпеки особи, що значно розширює сферу впливу таких даних. Саме тому в міжнародних документах дедалі частіше засвідчують необхідність

посиленого правового режиму для біометричної інформації незалежно від конкретної мети її використання [61; 106].

Генетичні дані хоча й використовують у системах штучного інтелекту не так масово, однак привертають увагу іноземних дослідників і регуляторів. Алгоритмічний аналіз генетичної інформації надає можливість формувати висновки не лише щодо окремої особи, а й щодо її родичів або груп населення. У цьому сенсі генетичні дані мають колективний вимір, що ускладнює застосування традиційних індивідуалізованих механізмів захисту. Міжнародні рекомендації з етики штучного інтелекту зауважують, що використання генетичних даних разом з алгоритмічними системами створює довгострокові ризики дискримінації та соціальної стигматизації [51; 62; 116].

Чутливою категорією даних у контексті штучного інтелекту є поведінкові дані, які формуються в процесі цифрової взаємодії осіб з інформаційними системами. До них належать відомості про навігацію в мережі, шаблони користування сервісами, реакції на контент, часові та просторові параметри активності. У зарубіжних підходах зазначено, що саме поведінкові дані стають ключовим ресурсом для побудови алгоритмічних моделей прогнозування та профілювання, оскільки дають змогу доходити висновку щодо схильностей, інтересів і майбутніх дій осіб [83; 131].

Поведінкові дані мають особливу чутливість з огляду на те, що вони часто збираються пасивно, без активної участі або усвідомленої згоди суб’єкта даних. У міжнародних документах увагу зосереджено на тому, що поєднання поведінкових відомостей з методами машинного навчання дає змогу створювати детальні цифрові профілі, використання яких може призводити до маніпуляції поведінкою, інформаційного впливу або непрямої дискримінації [59; 131]. Це зумовлює необхідність поширення на такі дані посиленого режиму правового захисту, навіть якщо вони формально не підпадають під класичні категорії спеціальних даних.

Профілювальні дані посідають проміжне місце між первинною інформацією та інференційними висновками. Вони формуються як результат

систематичного аналізу різних джерел інформації, їх використовують для сегментації осіб, оцінювання ризиків або автоматизованого прийняття рішень. У зарубіжних підходах акцентовано, що профілювання в умовах ШІ виходить за межі традиційного маркетингового інструменту й дедалі частіше впливає на доступ до соціальних благ, фінансових ресурсів або публічних послуг. Саме тому міжнародні організації спрямовують увагу на правових гарантіях у сфері профілювання, зокрема щодо забезпечення прозорості й можливості людського втручання [59; 138].

Зарубіжний досвід також демонструє, що межі між різними чутливими категоріями персональних даних у контексті штучного інтелекту є дедалі менш чіткими. Біометричні, поведінкові та профілювальні дані часто поєднуються в межах однієї алгоритмічної системи, створюючи кумулятивний ефект для приватності та прав людини. У міжнародних рекомендаціях зазначено, що саме такий комбінований характер обробки інформації потребує комплексного підходу до правового регулювання, орієнтованого на сукупний ризик, а не на ізольовані категорії даних [62; 89; 116]. У зарубіжних підходах чутливі категорії персональних даних у контексті штучного інтелекту розглядають значно ширше, ніж у класичних моделях захисту інформації. Розширення переліку таких даних і зміна критеріїв їх ідентифікації відображають усвідомлення того, що алгоритмічні системи здатні трансформувати навіть формально нейтральну інформацію на ресурс підвищеного ризику для прав і свобод людини.

Проблему анонімізації та псевдонімізації персональних даних у системах штучного інтелекту в іноземних підходах розглядають як один із ключових вузлів сучасного правового регулювання. Якщо в класичних моделях захисту персональних даних ці інструменти протягом тривалого часу сприймали як ефективний спосіб виведення інформації з-під дії режиму правової охорони, то розвиток алгоритмічних технологій суттєво змінив оцінку їх реальної спроможності забезпечувати приватність. У міжнародних документах після 2018 року простежується чітка тенденція до критичного

переосмислення ролі анонімізації з огляду на можливості машинного навчання, кореляційного аналізу та повторного використання даних [89; 105; 116].

Анонімізація не є бінарним станом, за якого дані або повністю втрачають персональний характер, або зберігають його. Натомість її розглядають як контекстуально зумовлений процес, ефективність якого залежить від конкретних технологічних умов, доступних допоміжних даних і завдань подальшої обробки. Саме такий підхід закріплено в позиціях європейських наглядових органів, які акцентують, що оцінку анонімності слід здійснювати з огляду на «всі розумно ймовірні засоби» повторної ідентифікації [61; 106].

Псевдонімізація в зарубіжних підходах посідає окреме місце, оскільки її безпосередньо визнають як технічний захід захисту, що не усуває персональний характер даних, але може знижувати ризики для прав суб'єктів. У міжнародних рекомендаціях зазначено, що псевдонімізовані дані зберігають зв'язок із конкретною особою, хоча й опосередкований, а отже, залишаються в межах правового режиму захисту персональних даних. У контексті ШІ це має важливе значення, оскільки псевдонімізацію часто використовують на стадіях навчання і тестування моделей як компроміс між потребами інновацій та вимогами приватності [59; 83].

Критичний аналіз ефективності анонімізації в умовах розвитку штучного інтелекту ґрунтується на емпіричних дослідженнях можливостей реідентифікації. У зарубіжній доктрині доведено, що поєднання різних наборів знеособлених даних дає змогу відновлювати індивідуальні профілі з високим ступенем точності, передусім коли такі дані використовують для навчання алгоритмічних моделей. Ця проблема набуває особливої гостроти у випадках повторного використання даних для нових завдань, які не враховували під час первинної оцінки ризиків [105].

У міжнародних стандартах управління ризиками штучного інтелекту зазначено, що формальне застосування методів анонімізації не можна

розглядати як достатню гарантію захисту прав людини. Натомість пропонують оцінювати ризики з огляду на ймовірність повторної ідентифікації, масштаби потенційної шкоди й можливості ефективного контролю за подальшим використанням даних. Такий підхід відображено в документах NIST та ISO, де анонімізацію розглядають як один з елементів багаторівневої системи управління ризиками, а не як універсальне рішення [60; 64].

Увагу в зарубіжних підходах спрямовано на проблему анонімізації в контексті навчання генеративних моделей. Алгоритми, що працюють з великими корпусами текстових, візуальних або аудіоданих, здатні відтворювати фрагменти персональної інформації навіть у тих випадках, коли навчальні набори вважали знеособленими. У звітах міжнародних експертних центрів зазначено, що такі явища підривають традиційне уявлення про безпечність анонімізованих даних і вимагають перегляду критеріїв їх правової оцінки [59]. Іноземна регуляторна практика також засвідчує обмеженість анонімізації як інструменту захисту персональних даних у сфері ШІ. Розслідування та рішення наглядових органів у справах, пов’язаних із використанням даних для навчання великих мовних моделей, засвідчують, що навіть за відсутності прямих ідентифікаторів обробка інформації може створювати неприйнятні ризики для приватності. У таких випадках регулятори керуються тим, що факт можливості повторної ідентифікації є достатньою підставою для застосування режиму правового захисту [61; 98; 106].

Дедалі важливішими стають альтернативні й додаткові підходи до захисту даних, зокрема технології підвищення приватності. У міжнародних документах зазначено, що використання диференційної приватності, обмеження доступу до даних й організаційних заходів контролю може бути ефективнішим, ніж спроби досягти повної анонімності. Водночас ураховують, що жоден із цих інструментів не є самодостатнім і їх слід застосовувати в комплексі з правовими й інституційними гарантіями [54; 64].

Отже, у зарубіжних підходах анонімізацію та псевдонімізацію персональних даних у системах штучного інтелекту розглядають не як способи виведення інформації з-під дії правового регулювання, а як елементи ширшої системи управління ризиками. Усвідомлення обмеженості цих інструментів разом з алгоритмічними можливостями сучасних ШІ-систем формує підґрунтя для переходу до комплексних і контекстуально чутливих моделей захисту персональних даних.

Закордонний досвід правового регулювання штучного інтелекту свідчить про системну трансформацію класичних підходів до класифікації персональних даних, яка зумовлена зміною логіки обробки інформації в алгоритмічному середовищі. Традиційні моделі, що ґрунтувалися на відносно стабільному поділі даних за їх природою або формальними ознаками, виявилися недостатніми для опису процесів, у межах яких персональна інформація безперервно модифікується, комбінується та використовується для прийняття автоматизованих рішень. В умовах застосування ШІ персональні дані не є статичним об’єктом регулювання, вони набувають процесуального характеру [62; 89; 116].

Одним із ключових виявів цієї трансформації є поступовий відхід від формального критерію походження даних як визначального для встановлення їх правового режиму. У класичних підходах вирішальне значення мало те, чи були дані безпосередньо надані суб’єктом або зібрані про нього з ідентифікованих джерел. У зарубіжних моделях регулювання натомість акцент зміщується на функцію, яку інформація виконує в алгоритмічних процесах, а також на наслідки її використання для прав і свобод людини. Саме такий функціонально-наслідковий підхід простежується в рекомендаціях OECD, ЮНЕСКО та Ради Європи, де засвідчено необхідність оцінювати персональні дані з огляду на їх роль у прийнятті рішень, а не лише на їхні формальні характеристики [89; 103; 116]. Важливим елементом трансформації є переосмислення меж між персональними та неперсональними даними. У зарубіжних підходах дедалі

частіше визнають, що навіть інформація, яка формально не дає змоги прямо ідентифікувати особу, може набувати персонального значення внаслідок алгоритмічного поєднання з іншими масивами даних або використання для профілювання та прогнозування. Така позиція закріплена у висновках європейських наглядових органів, які акцентують, що можливість повторної ідентифікації або індивідуалізованого впливу є достатньою підставою для застосування режиму правового захисту [61; 106]. Зміни зазнає і традиційний поділ персональних даних на загальні та спеціальні категорії. У контексті штучного інтелекту цей поділ дедалі частіше доповнюють або навіть заміщують класифікаціями, побудованими на рівні ризику та чутливості алгоритмічної обробки. Міжнародні стандарти управління ризиками пропонують оцінювати обробку даних з огляду на імовірність шкоди, масштаби впливу та можливість ефективного людського контролю. У межах такого підходу правове значення має не стільки вид даних, скільки контекст їх використання та потенційні наслідки для суб'єктів [60; 64; 86]. Трансформація класифікаційних підходів тісно пов'язана з розширенням сфери автоматизованого прийняття рішень. В іноземних правопорядках визнано, що алгоритмічні системи здатні формувати рішення, які мають юридично значущі або фактично обов'язкові наслідки для осіб, навіть за відсутності формального правового акта. У таких умовах класифікація персональних даних не може обмежуватися описом їх властивостей, а має враховувати характер впливу алгоритмічних рішень на реалізацію прав людини. Цей підхід простежується в міжнародних рекомендаціях щодо етики штучного інтелекту та захисту прав людини, де засвідчено необхідність забезпечення підзвітності й можливості оскарження автоматизованих рішень [62; 116].

Важливу роль у трансформації класичних підходів відіграє усвідомлення кумулятивного ефекту алгоритмічної обробки персональних даних. Зарубіжні дослідження засвідчують, що навіть правомірне використання окремих наборів даних може призводити до непропорційного

втручання в приватне життя в разі їх поєднання в межах комплексних систем штучного інтелекту. Це зумовлює необхідність переходу від ізольованої оцінки окремих операцій обробки до аналізу сукупного впливу алгоритмічних процесів, що відображено в рекомендаціях міжнародних організацій і наглядових органів [83; 89; 131].

Зарубіжна практика демонструє тенденцію до інтеграції правових і технічних критеріїв у процесі класифікації персональних даних. Регуляторні документи дедалі частіше враховують специфіку архітектури алгоритмічних систем, рівень автономності моделей і можливість їх самонавчання. Це означає, що класифікацію даних розглядають не лише як юридичну категорію, а й як інструмент управління технологічними ризиками, що потребує міждисциплінарного підходу [60; 64].

Отже, іноземний досвід засвідчує, що трансформація класичних підходів до класифікації персональних даних під впливом технологій штучного інтелекту має комплексний характер. Відхід від формальних і статичних моделей на користь функціонально-наслідкових і ризик-орієнтованих підходів створює підґрунтя для побудови сучасних систем правового регулювання, здатних реагувати на динаміку алгоритмічних процесів. Така трансформація логічно підводить до подальшого аналізу конкретних регуляторних механізмів захисту персональних даних у сфері штучного інтелекту, що становить предмет наступного підрозділу дисертаційного дослідження.

2.2. Міжнародні нормативно-правові акти щодо захисту персональних даних у сфері штучного інтелекту

Формування міжнародно-правових підходів до захисту персональних даних у сфері штучного інтелекту відбувається в умовах браку універсального договору, спеціально присвяченого алгоритмічним

технологіям, у зв’язку з чим виникають певні розбіжності. Водночас у межах системи універсального міжнародного права поступово складається комплекс норм, принципів і стандартів, які визначають базові орієнтири для держав у сфері цифрової трансформації та захисту прав людини. У цьому контексті регулювання штучного інтелекту розглядають не як ізольований технічний феномен, а як складову ширшого процесу забезпечення права на приватність і захист персональних даних у цифрову епоху.

Універсальні міжнародно-правові акти ґрунтуються на визнанні права на приватність як фундаментального права людини, що зберігає свою чинність незалежно від технологічних змін. Резолюції Генеральної Асамблеї ООН, присвячені праву на приватність у цифрову епоху, фіксують обов’язок держав забезпечувати ефективний захист персональних даних в умовах розвитку нових інформаційних технологій, зокрема систем штучного інтелекту. У цих документах акцентовано, що автоматизована обробка даних й алгоритмічний аналіз не можуть виправдовувати зниження стандартів захисту прав людини, а, навпаки, потребують їх посилення з огляду на масштаб і швидкість обробки інформації [125]. Значущим для формування міжнародних підходів є Глобальний цифровий пакт, який розглядає штучний інтелект як один із ключових чинників трансформації сучасного суспільства. У цьому документі засвідчено необхідність забезпечення людиноцентричного підходу до цифрових технологій, що передбачає інтеграцію принципів захисту персональних даних у всі етапи розроблення та впровадження систем штучного інтелекту. Посилену увагу спрямовано на питання прозорості алгоритмічних рішень, підзвітності розробників і користувачів ШІ-систем, а також міжнародної координації у сфері цифрового врядування [87].

Універсальні міжнародні акти також закладають основу для застосування принципу належної обачності держав у сфері штучного інтелекту. Відповідно до цього підходу держави мають не лише утримуватися від порушень права на приватність, а й створювати ефективні

правові й інституційні механізми запобігання таким порушенням з боку приватних суб'єктів. У контексті алгоритмічних технологій це означає необхідність контролю за діяльністю розробників й операторів ШІ-систем, які здійснюють обробку персональних даних у транскордонному масштабі.

Значущим елементом універсального рівня регулювання є також декларативні акти та заяви міжнародних об'єднань органів із захисту персональних даних. Декларація з питань штучного інтелекту й захисту даних, ухвалена в межах Глобальної асамблеї з питань приватності, фіксує спільне розуміння того, що використання алгоритмічних систем не має підривати основоположні принципи захисту персональних даних. У документі засвідчено необхідність забезпечення законності, пропорційності та підзвітності в процесі використанні ШІ для обробки персональної інформації, а також важливість ефективного наглядового контролю [62]. відмітною рисою універсальних міжнародно-правових актів є їх принциповий і рамковий характер. Вони не встановлюють детальних процедурних вимог до обробки персональних даних у системах штучного інтелекту, проте формують ціннісні та нормативні орієнтири, які слід ураховувати під час розроблення регіональних і національних моделей регулювання. Саме на цьому рівні закріплено ідею технологічної нейтральності прав людини, відповідно до якої розвиток штучного інтелекту не змінює сутності права на приватність, але потребує адаптації механізмів його реалізації.

Отже, універсальні міжнародно-правові акти створюють концептуальне підґрунтя для подальшого розвитку спеціалізованих регіональних і секторальних норм у сфері захисту персональних даних і штучного інтелекту. Вони не підміняють детального регулювання, однак виконують системоутворювальну функцію, визначаючи межі допустимого втручання в приватне життя та орієнтири для балансування між інноваційним розвитком і захистом основоположних прав. Універсальний рівень міжнародного регулювання також відіграє важливу роль у формуванні спільного розуміння

транснаціональної природи обробки персональних даних у системах штучного інтелекту. Алгоритмічні технології функціонують у глобальних цифрових екосистемах, де дані вільно переміщуються між юрисдикціями, а рішення, прийняті однією системою, можуть мати наслідки для осіб у різних державах. У цьому контексті універсальні міжнародні акти засвідчують необхідність міжнародної співпраці й узгодження підходів до захисту персональних даних, зокрема шляхом обміну найкращими практиками та координації регуляторних дій [87].

В універсальних документах увагу зосереджено на питанні відповідальності держав за наслідки використання штучного інтелекту приватними суб'єктами. У межах сучасного міжнародно-правового дискурсу визнано, що держава не може обмежуватися роллю пасивного спостерігача за діяльністю технологічних компаній. Натомість вона зобов'язана забезпечити належні правові умови, за яких розроблення та застосування алгоритмічних систем відбуватимуться відповідно до вимог захисту персональних даних і прав людини. Такий підхід відповідає загальній еволюції міжнародного права прав людини, у межах якого посилюється акцент на позитивних обов'язках держав. Універсальні міжнародні акти також формують підґрунтя для розвитку процедур оцінки впливу цифрових технологій на права людини. Хоча ці документи не встановлюють обов'язкових механізмів оцінки впливу штучного інтелекту на приватність, у них закладено ідею необхідності попереднього аналізу ризиків і потенційної шкоди, що може виникати внаслідок алгоритмічної обробки персональних даних. Цю ідею згодом було розвинуто в регіональних правових актах і рекомендаціях, де оцінювання впливу стає одним із ключових інструментів забезпечення правомірності використання ШІ.

Важлива особливість універсального рівня регулювання полягає в його гнучкості й здатності адаптуватися до швидких технологічних змін. Рамковий характер міжнародних актів надає можливість їм зберігати актуальність, попри стрімкий розвиток алгоритмічних технологій і появу

нових форм обробки персональних даних. Саме завдяки цьому універсальні норми виконують стабілізаційну функцію в системі міжнародного регулювання, забезпечуючи сталість базових принципів захисту прав людини незалежно від конкретних технологічних рішень.

Універсальні міжнародно-правові акти слугують вихідною точкою для формування багаторівневої системи регулювання захисту персональних даних у сфері штучного інтелекту. Вони визначають загальний нормативний вектор, у межах якого розвиваються регіональні моделі та національні правопорядки, створюють основу для подальшої конкретизації правових механізмів, спрямованих на мінімізацію ризиків алгоритмічної обробки персональної інформації.

Регіональний рівень правового регулювання в межах Ради Європи посідає своє місце у формуванні стандартів захисту персональних даних у сфері штучного інтелекту, оскільки саме тут уперше було створено юридично обов'язкову міжнародну модель захисту інформації, орієнтовану на права людини. На відміну від універсальних актів, документи Ради Європи мають вищий ступінь нормативної конкретизації та безпосередній вплив на національні правопорядки держав-учасниць, що зумовлює їхню ключову роль у розвитку європейського підходу до регулювання алгоритмічних технологій.

Центральним елементом цієї системи є модернізована Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108+), яка закріплює базові принципи обробки персональних даних у технологічно нейтральній формі. Її положення не містять прямих згадок про штучний інтелект, однак сформульовані так, що охоплюють будь-які форми автоматизованої обробки, зокрема алгоритмічний аналіз і машинне навчання. У цьому виявляється принципова особливість підходу Ради Європи, відповідно до якого розвиток технологій не змінює сутності правових гарантій, а лише потребує їх адаптивного застосування [102]. Конвенція 108+ керується розширеним розумінням ризиків для прав людини,

пов’язаних з автоматизованою обробкою даних. Вона закріплює вимоги щодо якості даних, пропорційності обробки, обмеження завдань і наявності ефективних засобів правового захисту, які мають важливе значення в умовах використання штучного інтелекту. Алгоритмічні системи, здатні до масштабної та безперервної обробки інформації, істотно підвищують ризик порушення цих принципів, що зумовлює необхідність їх посиленого тлумачення в практиці застосування Конвенції. Подальший розвиток підходів Ради Європи до регулювання штучного інтелекту відбувається через рекомендаційні акти та керівні настанови, присвячені взаємозв’язку між алгоритмічними технологіями й захистом персональних даних. У Guidelines on Artificial Intelligence and Data Protection увагу зосереджено на потребі оцінювання впливу систем штучного інтелекту на права людини, а також забезпечення прозорості та підзвітності в процесі їх використання. Ці документи конкретизують загальні принципи Конвенції 108+ і спрямовані на їх практичну реалізацію у сфері алгоритмічної обробки інформації [89].

Значним кроком у розвитку регуляторної рамки Ради Європи стало ухвалення Рамкової конвенції про штучний інтелект і права людини, демократію та верховенство права. Цей документ закріплює комплексний підхід до регулювання алгоритмічних технологій, у межах якого захист персональних даних розглядають як невіддільний елемент ширшої системи гарантій прав людини. На відміну від суто рекомендаційних актів, Рамкова конвенція спрямована на створення юридично зобов’язувальних стандартів, що мають бути імплементовані державами-учасницями в національне законодавство [70; 132].

Особливість підходу Ради Європи полягає в акценті на взаємозв’язку між автоматизованою обробкою даних і демократичними процесами. У документах організації зауважено, що використання штучного інтелекту для обробки персональних даних може мати системний вплив не лише на окремих осіб, а й на функціонування демократичних інститутів, зокрема через алгоритмічне профілювання, маніпуляцію інформаційними потоками й

автоматизоване прийняття рішень у публічній сфері. Саме тому регулювання ШІ Радою Європи виходить за межі вузькоінформаційного права й інтегрується в загальну архітектуру захисту прав людини. Акти Ради Європи виконують роль своєрідного «містка» між універсальними принципами міжнародного права та деталізованими режимами регулювання, сформованими на рівні Європейського Союзу. Вони забезпечують узгодженість підходів до захисту персональних даних у сфері штучного інтелекту, створюють нормативну основу для подальшої конкретизації вимог у галузевому й технологічному законодавстві.

Отже, документи Ради Європи формують цілісну регіональну модель захисту персональних даних у сфері штучного інтелекту, яка поєднує принциповість універсальних стандартів із підвищеним рівнем нормативної визначеності. Їх значення полягає не лише у встановленні загальних правил, а й у формуванні правозастосовної культури, орієнтованої на превентивне врахування ризиків алгоритмічної обробки персональної інформації.

Саме на рівні права Європейського Союзу вперше було сформовано комплексну, внутрішньо узгоджену та юридично обов’язкову модель регулювання, орієнтовану безпосередньо на алгоритмічні технології. На відміну від універсальних і регіональних актів рамкового характеру, право ЄС поєднує загальні принципи захисту персональних даних із деталізованими механізмами їх практичної реалізації, що додає йому значущості в контексті розвитку штучного інтелекту.

Центральним елементом європейської моделі залишається Загальний регламент про захист даних, який встановлює уніфікований правовий режим обробки персональних даних на території Союзу. Хоча цей акт ухвалено до появи сучасних генеративних і високоризикових систем штучного інтелекту, його положення сформульовано так, що охоплюють будь-які форми автоматизованої обробки інформації. Важливими є також принципи законності, обмеження завдань, мінімізації даних, точності й підзвітності, які в умовах алгоритмічної обробки набувають підвищеного регуляторного

навантаження [118]. У контексті застосування систем штучного це затверджує детальніше окреслений вище GDPR, який закріплює низку інструментів, спрямованих на запобігання непропорційному втручанню в приватне життя. Насамперед ідеться про спеціальні правила щодо автоматизованого прийняття рішень і профілювання, які встановлюють обмеження на використання алгоритмічних систем у випадках, коли їх результати мають юридично значущі або схожі наслідки для особи. Ці положення розглядають у європейській доктрині як один із ключових механізмів стримування надмірної автоматизації у сфері обробки персональних даних [138].

Важливим елементом європейського підходу є також інститут оцінки впливу на захист даних, який набуває особливої актуальності в умовах використання штучного інтелекту. Оцінювання впливу розглядають не як формальну процедуру, а як інструмент попереднього аналізу ризиків, пов’язаних з алгоритмічною обробкою інформації. У практиці застосування GDPR саме використання нових технологій, зокрема систем машинного навчання, визнають однією з підстав для обов’язкового проведення такої оцінки [72]. Подальший розвиток правового регулювання штучного інтелекту в Європейському Союзі пов’язаний з ухваленням спеціального регламенту, що встановлює гармонізовані правила щодо штучного інтелекту. Цей акт формує окремий нормативний шар, спрямований на управління ризиками, які виникають унаслідок використання алгоритмічних систем у різних сферах суспільного життя. На відміну від GDPR, який зосереджений на захисті персональних даних, новий регламент передбачає ширшу перспективу захисту прав людини, безпеки й основоположних цінностей Союзу [124].

Ключовою характеристикою регулювання штучного інтелекту в ЄС є ризик-орієнтований підхід, відповідно до якого алгоритмічні системи класифікують залежно від потенційного впливу на права і свободи осіб. У межах цього підходу системи, що використовують персональні дані у

високоризикових контекстах, підлягають посиленим вимогам щодо прозорості, управління даними та людського контролю. Захист персональних даних у таких системах розглядають не ізольовано, а як складову комплексної системи гарантій, спрямованих на мінімізацію алгоритмічних ризиків. Взаємодія між регламентом про захист даних і спеціальним регулюванням штучного інтелекту є одним із найдискусійніших аспектів європейського правопорядку. У наукових та експертних колах зазначають, що ці акти не знаходяться у відносинах конкуренції, а доповнюють один одного, утворюючи багаторівневу модель регулювання. GDPR встановлює базові правила обробки персональних даних, натомість спеціальний регламент щодо штучного інтелекту конкретизує вимоги до алгоритмічних систем з огляду на їх функціональне призначення та рівень ризику [93, с. 1–6; 97]. У забезпеченні узгодженого застосування цих актів важливу роль відіграють інституції Європейського Союзу й органи з нагляду за захистом даних. Практика Європейської ради із захисту даних і Європейського наглядового органу з питань захисту даних свідчить про прагнення сформувати єдині підходи до тлумачення норм, що регулюють алгоритмічну обробку персональної інформації. У відповідних висновках і рекомендаціях зауважено, що використання штучного інтелекту не звільняє контролерів від дотримання вимог щодо законності, пропорційності та захисту прав суб’єктів даних [61; 85; 106].

Європейський підхід також вирізняється активним залученням практичних кейсів до формування регуляторних стандартів. Рішення національних наглядових органів щодо використання великих мовних моделей та обробки персональних даних у контексті навчання алгоритмів засвідчують, що право ЄС застосовують до сучасних технологій не декларативно, а через реальні механізми примусу. Такі кейси демонструють, що вимоги захисту персональних даних залишаються обов’язковими незалежно від масштабу чи інноваційності технології [98; 99].

Загалом право Європейського Союзу формує найрозвиненішу нормативну модель регулювання захисту персональних даних у сфері штучного інтелекту. Поєднання загальних принципів, ризик-орієнтованого підходу та розгалуженої інституційної системи забезпечує можливість адаптації правового режиму до швидкого розвитку алгоритмічних технологій. Саме цю модель дедалі частіше розглядають як орієнтир для інших правопорядків і міжнародних організацій у процесі формування власних підходів до регулювання штучного інтелекту.

Слід зосередити увагу на позанормативних регуляторних механізмах, що формуються поза межами класичного джерельного складу права, однак фактично впливають на зміст і напрям розвитку регулювання у сфері штучного інтелекту й обробки персональних даних. Ідеться про рекомендаційні та рамкові документи, які виникають як відповідь на структурну асиметрію між швидкістю технологічних інновацій і темпами формального нормотворення. На відміну від обов’язкових міжнародних договорів або актів вторинного права, такі інструменти не встановлюють безпосередніх юридичних зобов’язань, проте виконують роль методологічної основи для формування регуляторних підходів на національному й наднаціональному рівнях. Функціонально ці акти спрямовані не на регламентацію окремих правовідносин, а на окреслення допустимих меж використання алгоритмічних систем, критеріїв оцінювання ризиків і стандартів відповідальної обробки даних. Саме через них відбувається інституціоналізація таких категорій, як пропорційність алгоритмічного втручання, підзвітність розробників й операторів ШІ, а також інтеграція вимог до захисту персональних даних у технічні й організаційні процеси. Одним із ключових прикладів міжнародного «м’якого права» у сфері штучного інтелекту є принципи Організації економічного співробітництва та розвитку щодо штучного інтелекту. Ці принципи ґрунтуються на людиноцентричному підході та визнають необхідність забезпечення поваги до прав людини й захисту персональних даних у процесі розроблення та

застосування алгоритмічних систем. Посилену увагу в них спрямовано на питання прозорості, підзвітності й управління ризиками, що безпосередньо пов’язані з обробкою персональних даних у високоризикових ШІ-системах [103; 104].

Рекомендації OECD мають значення не лише як програмний документ, а й як основа для гармонізації підходів держав до регулювання штучного інтелекту. Їх активно використовують як орієнтир під час розроблення національних стратегій і законодавчих ініціатив, а також формування регуляторної політики в інших міжнародних організаціях. У цьому сенсі «м’яке право» є інструментом непрямої уніфікації правових режимів у сфері захисту персональних даних і ШІ.

Свій внесок у формування міжнародних стандартів здійснила ЮНЕСКО, яка ухвалила Рекомендацію з етики штучного інтелекту. Цей документ має ширший гуманітарний і соціальний вимір, проте містить чіткі положення щодо захисту персональних даних, приватності та людської гідності. У рекомендації зауважено, що використання алгоритмічних систем має ґрунтуватися на принципах законності, необхідності та пропорційності, а обробка персональних даних – ураховувати потенційний вплив на вразливі групи населення [116]. Особливість рекомендацій ЮНЕСКО полягає в їх міждисциплінарному характері, орієнтованості на довгострокові соціальні наслідки розвитку штучного інтелекту. У них захист персональних даних розглядають не лише як юридичне питання, а і як елемент забезпечення довіри до технологій та сталого розвитку суспільства. Такий підхід розширює традиційні межі інформаційного права й засвідчує необхідність інтеграції етичних стандартів у правове регулювання алгоритмічних систем.

Глобальна асамблея з питань приватності, яка об’єднує наглядові органи із захисту персональних даних з різних юрисдикцій, відіграє одну з основних ролей у цьому питанні. У деклараціях і заявах цього органу відображено спільну позицію регуляторів щодо неприпустимості використання штучного інтелекту з порушенням базових принципів захисту

персональних даних. Ці документи мають практичне значення, оскільки впливають на підходи до правозастосування та інтерпретації норм у національних правопорядках [62].

Рекомендаційні акти та «м'яке право» дають змогу випробовувати нові регуляторні підходи без невідкладного запровадження жорстких юридичних зобов'язань, що є вкрай важливим у сфері швидкозмінних технологій.

Крім того, «м'яке право» відіграє важливу роль у формуванні стандартів належної корпоративної поведінки. Міжнародні рекомендації дедалі частіше використовують приватні компанії як основу для розроблення внутрішніх політик, кодексів поведінки та процедур управління ризиками, пов'язаними з використанням штучного інтелекту. У цьому аспекті рекомендаційні акти впливають на практику обробки персональних даних не лише через державне регулювання, а й через механізми саморегуляції.

Загалом міжнародні рекомендаційні акти й інструменти «м'якого права» формують динамічний і гнучкий пласт регулювання у сфері захисту персональних даних і штучного інтелекту. Їх значення полягає в здатності швидко реагувати на нові виклики, визначати напрям розвитку правових стандартів і забезпечувати узгодженість підходів різних правопорядків. Саме завдяки цьому «м'яке право» стає невіддільним елементом сучасної системи міжнародного регулювання алгоритмічних технологій.

Окремий рівень міжнародного регулювання захисту персональних даних у сфері штучного інтелекту формують техніко-нормативні та стандартизаційні документи, які спрямовані на практичну операціоналізацію правових й етичних принципів. На відміну від нормативно-правових актів, ці документи не встановлюють безпосередніх юридичних зобов'язань, однак відіграють ключову роль у впровадженні ризик-орієнтованих підходів до розроблення та використання алгоритмічних систем. Саме через стандарти й рамкові моделі управління ризиками відбувається трансформація абстрактних вимог щодо захисту персональних даних у конкретні технічні й організаційні процедури.

У міжнародній практиці стандартизаційні документи розглядають як інструмент забезпечення узгодженості між правовим регулюванням і технологічними процесами. Вони дають змогу подолати розрив між загальними нормами, закріпленими в міжнародних договорах або регламентах, і фактичною архітектурою систем штучного інтелекту. У цьому сенсі технічні стандарти виконують функцію перекладу правових вимог мовою інженерних рішень й управлінських процедур.

Провідне місце серед таких документів посідає Рамкова модель управління ризиками штучного інтелекту, розроблена Національним інститутом стандартів і технологій США. Цей документ пропонує структурований підхід до ідентифікації, оцінювання та зниження ризиків, пов’язаних із використанням алгоритмічних систем, зокрема ризиків для приватності та захисту персональних даних. Особливість моделі полягає в її модульному характері, що надає можливість адаптувати її положення до різних типів ШІ-систем і сфер застосування [64, с. 12–17]. У контексті захисту персональних даних рамкова модель NIST визнає, що ризики для приватності є складником загального профілю ризиків штучного інтелекту. Управління такими ризиками передбачає не лише застосування технічних заходів безпеки, а й інтеграцію принципів прозорості, підзвітності та людського контролю в усі стадії життєвого циклу системи. Цей підхід корелює з європейською моделлю оцінки впливу на захист даних, однак має універсальнішу й технологічно нейтральну форму.

Подальший розвиток стандартизаційних підходів відображено у спеціалізованих профілях і настановах, присвячених генеративним системам штучного інтелекту. У таких документах увагу спрямовано на ризики відтворення персональної інформації, неконтрольованого використання навчальних даних і непрозорості механізмів прийняття рішень. Рекомендації спрямовані на впровадження процедур тестування, моніторингу й аудиту, що мають запобігати порушенням прав суб’єктів персональних даних [86].

Вагоме значення у сфері технічної стандартизації мають також міжнародні стандарти, розроблені в межах ISO та IEC. Ці документи формують універсальну термінологічну й методологічну основу для управління ризиками штучного інтелекту, включно з ризиками, пов’язаними з обробкою персональних даних. Стандарти ISO/IEC пропонують системний підхід до оцінювання ризиків, який охоплює як технічні, так й організаційні аспекти функціонування алгоритмічних систем [60]. Особливість цих стандартів полягає в їх орієнтованості на інтеграцію управління ризиками ШІ в загальні системи управління організаціями. Захист персональних даних у цьому контексті розглядають як складову загальної стратегії управління інформаційними й технологічними ризиками, а не як ізольований обов’язок. Такий підхід сприяє впровадженню комплексних політик, що поєднують вимоги інформаційної безпеки, приватності й етичного використання технологій.

Техніко-нормативні документи відіграють дедалі важливішу роль у правозастосовній практиці. Регуляторні органи та суди постійно звертаються до стандартів і рамкових моделей як до джерела орієнтирів для оцінювання належності дій контролерів і розробників ШІ-систем. У цьому сенсі стандартизаційні документи набувають квазінормативного значення, впливаючи на формування практики застосування обов’язкових правових норм.

Водночас зарубіжні дослідники акцентують на обмеженні технічної стандартизації як інструменту захисту персональних даних. Стандарти не можуть замінити правове регулювання і не здатні самостійно гарантувати дотримання прав людини. Їх ефективність залежить від ступеня інтеграції в нормативні вимоги та від наявності механізмів контролю і відповідальності. Саме тому техніко-нормативні документи розглядають як допоміжний, але необхідний елемент багаторівневої системи регулювання.

Узагальнення міжнародної практики засвідчує, що техніко-нормативні й стандартизаційні документи формують практичний вимір регулювання

захисту персональних даних у сфері штучного інтелекту. Їхнє значення полягає не у створенні нових правових режимів, а в забезпеченні функціонального зв'язку між загальними правовими принципами та реальними процесами розроблення, упровадження й експлуатації алгоритмічних систем. Саме через такі документи правові вимоги поступово інтегруються в технологічні й організаційні практики, що дає змогу застосовувати ризик-орієнтовані підходи та підвищувати рівень фактичного захисту прав людини в умовах динамічного технологічного розвитку. Поряд із нормативними й стандартизаційними інструментами істотну роль у міжнародній системі захисту персональних даних у сфері штучного інтелекту відіграє діяльність наглядових і координаційних органів. На відміну від актів позитивного права, ці інституції формують регуляторну практику через ухвалення висновків, настанов, рекомендацій та рішень у конкретних справах. Саме на цьому рівні відбувається перехід від абстрактних положень законодавства до практичних механізмів захисту прав суб'єктів персональних даних у контексті використання алгоритмічних систем.

У межах європейського регуляторного простору функцію забезпечення однакового застосування правил захисту персональних даних у державах – членах Європейського Союзу виконує Європейська рада із захисту даних. Її діяльність має особливе значення для сфери штучного інтелекту, оскільки через відповідні висновки та настанови відбувається адаптація загального режиму захисту персональних даних до нових технологічних практик. У документах Ради послідовно закріплено підхід, згідно з яким використання штучного інтелекту не створює винятків із загальних правил обробки персональних даних і не звільняє контролерів від обов'язку дотримуватися принципів законності, пропорційності та мінімізації обробки [106].

Зміст практики Європейської ради із захисту даних демонструє, що значна частина її висновків стосується питань навчання та використання моделей штучного інтелекту, які оперують великими масивами персональної інформації. У відповідних документах зазначено, що залучення відкритих

джерел або загальнодоступних даних не усуває необхідності визначення належних правових підстав обробки та гарантування прав суб'єктів персональних даних. Такий підхід має принципове значення для оцінювання правомірності навчання великих мовних моделей та підтверджує поширення режиму захисту персональних даних на сучасні алгоритмічні практики. Контроль за обробкою персональних даних інституціями й органами Європейського Союзу здійснює Європейський наглядовий орган з питань захисту даних. У своїх орієнтаціях щодо використання генеративних систем штучного інтелекту цей орган зосереджується на необхідності проведення попереднього аналізу ризиків, забезпечення прозорості алгоритмічних процесів і впровадження ефективних механізмів людського контролю. Така регуляторна позиція спрямована на запобігання системним порушенням права на приватність у діяльності публічних органів [85]. Практика національних наглядових органів держав – членів Європейського Союзу також істотно впливає на формування міжнародних стандартів у сфері штучного інтелекту. Рішення та розслідування, здійснені, зокрема, французькою Комісією з інформатики та свобод або італійськими регуляторними органами, демонструють здатність системи захисту персональних даних реагувати на виклики, пов'язані з використанням нових алгоритмічних технологій. Такі кейси засвідчують, що регуляторний контроль у сфері штучного інтелекту реалізують через конкретні механізми примусу та корекції практик обробки даних [98; 99; 134].

Координацію діяльності наглядових органів на міжнародному рівні забезпечує Глобальна асамблея з питань приватності, яка об'єднує регуляторів з різних регіонів світу. Її документи відображають спільне розуміння базових викликів, пов'язаних із використанням штучного інтелекту для обробки персональних даних, і спрямовані на розроблення узгоджених підходів до їх вирішення. Значення таких актів полягає у формуванні єдиного регуляторного дискурсу, який впливає на національні

правопорядки незалежно від рівня їх формальної інтеграції в європейську правову систему [62].

Аналіз рекомендацій та практики міжнародних і національних наглядових органів дає змогу констатувати поступове формування комплексного підходу до оцінювання ризиків, пов’язаних із використанням штучного інтелекту. Таке оцінювання виходить за межі традиційних процедур і охоплює не лише технічні, а й організаційні та управлінські аспекти функціонування алгоритмічних систем, що сприяє інтеграції захисту персональних даних у ширшу систему управління ризиками штучного інтелекту. Здатність наглядових органів оперативно реагувати на нові технологічні виклики відрізняє їхню діяльність від законодавчих процесів, які за своєю природою потребують значно тривалішого проміжку часу. Коригування практики застосування норм через роз’яснення, орієнтації та рішення в конкретних справах забезпечує гнучкість системи захисту персональних даних і дає змогу адаптувати її до стрімкого розвитку алгоритмічних технологій.

У сукупності діяльність наглядових і координаційних органів формує завершальний елемент міжнародної системи регулювання захисту персональних даних у сфері штучного інтелекту. Саме на цьому рівні універсальні принципи, регіональні норми і технічні стандарти поєднуються в практику правозастосування, що забезпечує не лише формальну наявність правових вимог, а й їх реальну ефективність у захисті прав і свобод людини в умовах розвитку сучасних алгоритмічних технологій.

2.3. Аналіз правових засад регулювання захисту персональних даних у країнах ЄС і можливість імплементації зарубіжного досвіду в законодавчу практику України

У цьому підрозділі здійснимо порівняльний аналіз підходів до захисту персональних даних під час використання штучного інтелекту в декількох ключових юрисдикціях: Європейському Союзі (зокрема на прикладі Естонії як цифрового лідера ЄС), США, Великій Британії, Канаді та Японії. Мета цього аналізу – виявити спільні тенденції та специфіку правового регулювання, а також окреслити, які елементи зарубіжного досвіду можуть бути впроваджені в Україні. Українське законодавство знаходиться на етапі оновлення з огляду на євроінтеграційні прагнення та стрімкий розвиток цифрової сфери, тому використання найкращих іноземних практик є надзвичайно актуальним.

Європейський Союз та Естонія. У Європейському Союзі захист персональних даних є фундаментальним правом (ст. 8 Хартії ЄС про основоположні права), його регулює переважно Загальний регламент про захист даних (GDPR) з 2018 року [118]. GDPR встановлює єдині правила для всіх 27 держав-членів, що сприяє уніфікованому підходу до приватності, зокрема і щодо технологій ШІ [118]. Хоча текст GDPR не містить слів «штучний інтелект» чи «алгоритм», його норми застосовують до будь-якої обробки персональних даних незалежно від технології [8; 118]. Важливими є положення GDPR, які значущі в контексті ШІ й охоплюють:

– принципи обробки даних (законність, справедливість, прозорість; обмеження мети; мінімізація даних; точність; обмеження зберігання; цілісність і конфіденційність; підзвітність (ст. 5 GDPR)) [118]. Ці принципи адресують ключові виклики ШІ: наприклад, мінімізація даних обмежує надмірний збір для навчання моделей, принцип прозорості вимагає пояснювати суб’єктам, як їхні дані використовують в алгоритмах [118];

– правові підстави обробки – ШІ-системи повинні мати підставу для збору й аналізу персональних даних (згода, контракт, законний інтерес тощо, ст. 6 GDPR) [118]. Чимало застосунків ШІ у бізнесі чи державі посилаються на легітимний інтерес, але GDPR вимагає проводити тест на збалансування інтересів і гарантувати, що права суб’єкта не переважають (EDPB,

2020) [106]. Це стримує використання даних у ШІ без належного обґрунтування [118];

– спеціальні категорії даних – заборона обробки чутливих даних без виняткових умов (ст. 9 GDPR) [118]. Для ШІ це означає, що системи не можуть збирати або виводити расові, етнічні, щодо здоров'я чи інші делікатні відомості без належної підстави [118]. Наприклад, алгоритм аналізу фотографій не повинен визначати етнічність особи, якщо на це немає легальної потреби і згоди, інакше це порушення GDPR [118];

– автоматизоване прийняття рішень – ст.с22 GDPR надає суб'єкту право не підлягати рішенню, що ґрунтується виключно на автоматизованій обробці, яке має юридично значущі або схожі суттєві наслідки [118]. Це критично важлива норма, що безпосередньо стосується систем ШІ (передусім систем прийняття рішень без участі людини, наприклад, автоматична відмова у кредиті, профілювання для страхування) [118]. Вона фактично забороняє такі рішення, якщо тільки не виконують додаткових вимог: або це необхідно для договору, або дозволено законом за наявності гарантій, або є явна згода суб'єкта [118]. Навіть коли автоматизоване рішення допустиме, особа має право на людське втручання, висловлення своєї позиції та оскарження рішення [118]. Цей механізм забезпечує захист від «black box» алгоритмів, хоча на практиці його інтерпретація досі є дискусійною (Almada, 2025) [138]. 2023 року Суд ЄС у справі SCHUFA Holding AG (C-634/21) підтвердив широкий підхід: кредитний скоринг, навіть якщо рішення про кредит формально приймає людина, але вона практично не впливає на автоматичний бал, підпадає під дію ст. 22, і громадяни мають право отримати значущу інформацію про логіку скорингу (CJEU, 2023; IAPP, 2023) [118]. Це прецедент, який задає вектор для всієї Європи у сфері алгоритмічної прозорості [118];

– Privacy by design/default – вимагає, щоби контролер упроваджував технічні й організаційні заходи для вбудованого захисту даних на початку розроблення систем [118]. Для ШІ це означає, що розробники мають

врахувати приватність на етапі проєктування моделей: наприклад, використовувати анонімізацію чи федеративне навчання там, де можливо, встановлювати суворі доступи до навчальних даних тощо [58, с. 1–23]. Також налаштування систем мають за замовчуванням бути максимально приватними (minimal data) [118];

– оцінки впливу (DPIA) – ст. 35 GDPR зобов'язує здійснювати оцінювання впливу на захист даних для видів обробки, які можуть призвести до високого ризику для прав осіб [118]. Європейський комітет із захисту даних (EDPB) роз'яснив, що використання ШІ, зокрема для оцінювання чи прогнозування аспектів життя, масове спостереження, обробка біометрії – це приклади, де потрібна DPIA (EDPB, Guidelines 2019) [106]. Унаслідок цього компанія чи установа перед запуском алгоритму має описати його процеси, оцінити ризики (наприклад, витоку даних, дискримінації) і запланувати заходи з пом'якшення [72]. DPIA стає дієвим інструментом виявлення небезпек ШІ для приватності завчасно [118].

GDPR як регламент прямої дії встановив однакові вимоги в усіх державах ЄС [118]. Це створило єдиний стандарт [118]. Проте механізми імплементації та контролю можуть різнитися [118]. Деякі держави, як-от Франція або Іспанія, активніше видають специфічні настанови: французька CNIL випустила 2017 року посібник «Алгоритми: рекомендації для прозорості, суспільного дебату та управління» (CNIL, 2017) [134], а іспанська AEPD – звіт «ШІ та захист даних» (AEPD, 2020) [89]. Ці документи пояснюють, як саме дотримуватися GDPR під час розроблення ШІ (наприклад, CNIL рекомендувала методику оцінювання алгоритмічної справедливості) [134].

Естонія впровадила GDPR через власний Закон про захист даних (2019), водночас функції наглядового органу виконує Естонська інспекція із захисту даних [118]. Як країна, що активно впроваджує електронне урядування та елементи ШІ в держпослуги, Естонія розробила цікаві практики [96]. 2019 року уряд Естонії розглядав концепцію «роботизованого

судді» для малих позовів – ШІ-системи, що приймала б рішення в спрощеному порядку [118]. Одразу постало питання: як узгодити це з GDPR стосовно автоматизованих рішень [118]. Виявилося, що навіть якщо сторони погодяться на такий порядок, усе одно слід передбачаити можливість перегляду рішення людиною-суддею (інакше це порушення ст. 22 GDPR) [118]. Проєкт знаходиться на експериментальній стадії, але приклад демонструє, що навіть у судочинстві ЄС правила приватності є запобіжником від неконтрольованого ШІ [118].

Інший приклад з Естонії – система попередження дитячої небезпеки, яка аналізувала дані про сім'ї (доходи, соціальний статус) для прогнозу можливого неналежного догляду за дітьми [118]. Цей алгоритм критикували за непрозорість і ризик стигматизації [118]. Естонська інспекція із захисту даних втрутилася, вимагаючи провести DPIA і забезпечити, щоб будь-яке негативне рішення (наприклад, примусове втручання соціальних служб) не було прийнято виключно автоматично [118]. Унаслідок цього систему доопрацьовано, додано елемент обов'язкової оцінки соціальним працівником: людина приймає кінцеве рішення, а алгоритм лише радить [118]. Цей кейс підтверджує застосування принципів GDPR на практиці: високоризиковий алгоритм допустимий лише за умови прозорості, пропорційності та контролю людини [118]. Естонія також відома проєктом X-Road – це державна платформа, що з'єднує бази даних різних відомств. У X-Road зберігаються не дані, а налаштування доступу – хто і яку інформацію може отримати [96]. Усі звернення до персональних даних журналюють, а громадяни можуть бачити, хто переглядав їхні дані. Така архітектура забезпечує принцип підзвітності й мінімізації доступу, передбачений GDPR [118]. Під час використання ШІ на базі X-Road (наприклад, аналітика для виявлення шахрайства) права доступу все одно обмежують обробку [96]. Отже, технічні рішення в Естонії втілюють юридичні вимоги: приватність за замовчуванням і контроль суб'єкта за власними даними [118].

У масштабах усього ЄС практику забезпечення GDPR у сфері ШІ можна проілюструвати резонансним випадком 2023 року – діями італійського регулятора проти ChatGPT [99]. Наприкінці березня 2023 року Італійська служба із захисту даних (Garante) видала наказ про тимчасове блокування сервісу ChatGPT на території Італії [99]. Підставами стали: 1) відсутність прозорого повідомлення користувачам про те, як їхні персональні дані (включно з розмовами) збирають і використовують для навчання моделі; 2) брак правової підстави для масового витягування особистих даних з інтернету (web scraping); 3) недостатній захист дітей – відсутність перевірки віку, хоча сервіс допускає потенційно шкідливий контент (Garante, 2023) [99]. Цей випадок став першим у світі блокуванням великої мовної моделі з причин приватності [99]. Після переговорів OpenAI (розробник ChatGPT) ввів низку змін: опції відмови від використання розмов для навчання, повідомлення про обробку даних, упровадження механізму перевірки віку [95]. У квітні 2023 року Garante зняв блокування, проте продовжив розслідування і в грудні 2024 року оштрафував OpenAI на 15 млн євро за порушення GDPR [98]. У рішенні регулятора зазначено, що компанія незаконно опрацювала персональні дані мільйонів інтернет-користувачів для навчання ШІ, без належної на те підстави й без інформування, а також не реалізувала права суб’єктів на виправлення або видалення їхніх даних із моделі [98]. OpenAI з цим не погоджується і оскаржує, але прецедент важливий: ЄС довів, що навіть новітні генеративні ШІ підпадають під GDPR, і компанії повинні знаходити способи забезпечити дотримання вимог приватності (Transparency, opt-out, age-gating) або не зможуть працювати на єврринку [118]. Інші країни ЄС (Франція, Іспанія, Німеччина) також почали перевірки аналогічних сервісів [106].

У ЄС склався комплексний правовий і регуляторний режим – GDPR як основа, доповнена секторними актами (DSA, AI Act) й активним наглядом з боку незалежних органів [118; 124]. Цей режим прагне гарантувати, що впровадження ШІ не вийде за межі, накреслені правом на приватність. Для

України досвід ЄС є визначальним, адже курс на євроінтеграцію передбачає гармонізацію з європейськими правовими документами (GDPR тощо). Крім того, уже в жовтні 2022 року в парламенті України прийнято Закон «Про захист персональних даних», метою якого є імплементація норм GDPR (Ministry of Digital Transformation of Ukraine, 2022) [37; 107]. Цей Закон розширює права суб'єктів, встановлює принципи «privacy by design/default», посилює відповідальність за порушення, тобто фактично наближає українське законодавство до європейського рівня [37; 108]. Його прийняття – вимога Плану дій щодо лібералізації візового режиму з ЄС та Угоди про асоціацію [107]. Важливо, що в пояснювальній записці до нормативного акта безпосередньо зазначено про необхідність урахування сучасних викликів, включно з обробкою даних в інформаційних системах, які приймають рішення автоматично [37]. Отже, інтеграція європейських стандартів захисту даних створює основу і для регулювання ШІ в Україні [43; 115].

США та секторний підхід, нові закони штатів і регуляторні дії щодо ШІ. Сполучені Штати Америки історично дотримуються секторного підходу до захисту персональних даних, тобто не мають єдиного всеосяжного федерального закону на кшталт GDPR [65]. Замість цього діє мозаїка галузевих норм (наприклад, HIPAA для медичних даних, FERPA для освітніх, FCRA для кредитної інформації, GLBA для фінансових установ) і є закони окремих штатів [65]. Проте розширення масштабів застосування цифрових технологій та ШІ спричинило в США дискусії про необхідність реформування приватності [65]. На федеральному рівні приватність регулюють такі нормативні акти:

– ст. 5 Закону про Федеральну комісію з торгівлі (FTC Act), яка забороняє «несправедливі та оманливі практики» [69]. FTC трактує порушення приватності як потенційно несправедливу практику [69]. Хоч це не прямий закон про дані, FTC з 2010-х років активно застосовує його для покарання компаній за витоки даних, порушення політик приватності тощо [69]. У контексті ШІ FTC чітко заявила, що якщо алгоритм треновано

на даних, зібраних обманним шляхом або з порушеннями, використання такого алгоритму вважатимуть продовженням порушення (FTC, 2021) [69]. Прецедент – справа Everalbum (2021): стартап, що пропонував фотосервіс, використав завантажені користувачами зображення для навчання алгоритму розпізнавання облич без належної згоди [69]. FTC кваліфікувала це як оманливу практику та наказала видалити не лише дані, а й алгоритми, створені на їх основі [69]. Це важливий сигнал: компанії в США можуть бути змушені знищувати ШІ-моделі, якщо ті збудовано на «брудних» з позицій приватності даних [69];

– закони про захист прав споживачів штатів [66; 67]. З 2018 року Каліфорнія запустила процес прийняття законів, схожих на GDPR за духом. California Consumer Privacy Act (CCPA) набрав чинності 2020 року, а із січня 2023 року діє поправки CPRA. Аналогічні закони ухвалили штати Вірджинія, Колорадо, Коннектикут, Юта [66; 67]. Ці закони надають споживачам права доступу, видалення, заборони продажу даних, а компаніям – обов'язки прозорості й безпеки [66; 67]. Хоча вони не настільки всеосяжні, як GDPR (вужче охоплення за суб'єктами, немає загальної вимоги мінімізації або обмеження завдання, вимоги реєструвати DPO тощо), але запроваджують поняття, критичні для ШІ: право відмовитися від профілювання [66; 67]. Наприклад, Каліфорнія CPRA згадує право обмежити використання sensitive personal information, що охоплює заборону використання таких даних для певних вторинних завдань, зокрема таргетингової реклами та профайлінгу (CPRA, §1798.121) [67]. Закони Вірджинії та Колорадо прямо зобов'язують проводити оцінку впливу (Data Protection Assessment) для діяльності з профілювання, що мають високий ризик для споживачів (Virginia Consumer Data Protection Act, 2021) [66]. Отже, уперше в США на рівні штатів з'явилося поняття «профілювання високого ризику», близьке за змістом до ст. 22 GDPR [66; 67]. Компанії мають документувати ризики дискримінації, порушення приватності, шкоди споживачу від таких алгоритмів [65]. Це витоки подальшого регулювання ШІ [65];

– біометричні закони штатів. Іллінойс 2008 року прийняв закон BIPA, який містить вимогу отримувати письмову згоду для збирання біометричних ідентифікаторів (відбитків, сканів обличчя), вводить право позову за порушення [66]. Цей закон став основою серії позовів проти технологічних компаній [66]. Найвідоміший – Rosenbach v. Six Flags (2019), де суд постановив, що навіть технічне порушення BIPA (збір відбитків пальців дітей без повного інформування) дає право на компенсацію, навіть якщо шкоду не доведено [66]. У контексті ШІ BIPA порушив справи проти Facebook (який 2020 року виплатив 650 млн доларів США за функцію розпізнавання облич у фото без згоди) та проти компанії Clearview AI (стартапу, що зібрав три мільярди фото з інтернету для розпізнавання облич) [66]. Clearview AI програла в суді Іллінойсу й погодилася не продавати свій сервіс приватним компаніям, сплатити штраф [66]. Аналогічні біометричні закони діють у Техасі й Вашингтоні [66]. Тож технологія розпізнавання облич опинилася під юридичним тиском у США, її використання звузилося [66]. Деякі міста (Сан-Франциско, Портленд) навіть заборонили місцевій поліції використовувати FR-технології, посилаючись на приватність і ризик расових упереджень;

– регулювання у фінансовій сфері. Оскільки чимало рішень ШІ пов’язані з кредитами, страхуванням, роботою з фінансовими даними, слід згадати Закон про чесну кредитну звітність (FCRA). Він дає споживачам право знати логіку будь-якої автоматизованої відмови в кредиті [66]. У контексті сучасних FinTech-алгоритмів це означає, що якщо модель ШІ скорингує позичальника, компанія зобов’язана повідомити ключові фактори, що вплинули на скоринг (наприклад, недостатній дохід, стисла кредитна історія тощо) [66]. Отже, explainability частково вбудована в законодавство США через окремі нормативні документи [65];

– акти про штучний інтелект (законопроєкти) [65]. На федеральному рівні поки немає прийнятого закону про ШІ, але було кілька ініціатив [65]. Наприклад, Algorithmic Accountability Act (законопроєкт 2019 року, повторно

– 2022 року) – пропонував зобов’язати компанії проводити оцінку впливу алгоритмів на приватність, точність, упередженість [65]. Він не пройшов Конгрес, але ідеї підхопили штати: Нью-Йорк 2021 року прийняв закон, що визначає обов’язковість аудиту на упередженість для алгоритмів найму персоналу (набрав чинності 2023 року) [65]. Це опосередковано пов’язано із захистом даних: якщо ШІ для рекрутингу використовує персональні дані кандидатів, його мають щорічно перевіряти незалежні фахівці, а результати (рівень точності й відхилень для різних груп) публікують [65]. Такий підхід стимулює компанії збирати менше чутливих даних (наприклад, інформацію про расу чи вік), аби уникнути потенційної дискримінації, або принаймні прозоро звітувати [65];

– Керівні принципи ШІ виконавчої влади [65]. У вересні 2022 року Білий дім оприлюднив «Рекомендації щодо прав людини в епоху ШІ: Стратегічний план», а в жовтні 2022 року – «Blueprint for an AI Bill of Rights» [65]. Ці документи не створюють нових законів, але формують політичну рамку [65].

Зазначений проєкт містить п’ять принципів:

1) безпечні й ефективні системи;

2) захист алгоритмічної дискримінації;

3) приватність даних:;

4) пояснюваність;

5) альтернативи та можливість відмовитися.

З позицій приватності в документі чітко визначено: «Ви маєте право на захист від порушення приватності через зловживання даними… і право контролювати збирання ваших персональних даних» [65]. Рекомендовано мінімізувати збір даних, використовувати лише потрібні для функції ШІ дані, вбудовувати механізми захисту (шифрування, диференційна приватність) і пропонувати людям опцію не надавати дані, коли можливо [65]. Хоча це все декларативно, проте уряд США почав упроваджувати ці принципи в практику закупівель. 2023 року видано Меморандум, згідно з яким

федеральні органи, закуповуючи технології ШІ, мають перевіряти їх на відповідність зазначеним принципам, включно з privacy. Отже, хоча федерація не має GDPR-аналога, через ринкові механізми й політику державних закупівель США також рухаються до стандартів privacy by design.

В американській правовій системі регулювання здійснюють переважно через прецеденти та справи, порушені споживачами чи генпрокурорами штатів. Уже йшлося про позови щодо Facebook (біометрія) і Clearview AI [66]. Ще один гучний випадок – FTC vs. Facebook (2020): унаслідок скандалу Cambridge Analytica Facebook сплатив рекордний штраф 5 млрд доларів США й зобов'язався впровадити комплексну програму конфіденційності [69]. Це показник того, що навіть без GDPR американські компанії під тиском регуляторів перебудовують свої політики, упроваджують комітети з етики даних, регулярні перевірки [65]. Колективні позови споживачів стали дієвим інструментом. 2023 року висунуто позови проти OpenAI та Google щодо порушення приватності під час навчання моделей на даних з інтернету (користувацьких постах, чатах), тобто увага до цього постійно посилюється [117].

Велика Британія: від GDPR до власного курсу. Велика Британія до 2020 року як член ЄС цілком підпорядковувалася GDPR і зберегла його у своєму законодавстві навіть після Brexit (через UK GDPR і Закон про захист даних 2018 року) [118; 73]. Тож базові правила в Британії ті самі, що описані вище для ЄС [118]. Однак зараз ця держава розглядає можливість деяких відхилень. 2023 року уряд вніс законопроєкт Data Protection and Digital Information, який пропонує пом'якшити деякі вимоги GDPR задля «скорочення бюрократії», наприклад, передбачити оцінювання впливу та призначення DPO опційними для компаній на основі ризиків [73]. Попри це, британські посадовці запевняють, що рівень захисту даних залишиться еквівалентним європейському (що важливо для взаємної адекватності передачі даних) [73].

Щодо штучного інтелекту Велика Британія обрала цікаву позицію: вона не планує поки єдиного закону про ШІ (на відміну від AI Act в ЄС), а хоче регулювати його через наявні органи – Управління з конкуренції (CMA), Управління із захисту даних (ICO), Управління з безпеки (MHRA) тощо [73]. В «AI Regulation Policy Paper» британський уряд окреслив принципи: безпека, прозорість, чесність, підзвітність, конкуренція. Щодо приватності там зазначено, що ICO продовжить стежити за використанням персональних даних в ШІ в межах повноважень [73].

І справді, британський Офіс Уповноваженого з інформації (ICO) – один з найактивніших у світі регуляторів, що видає детальні настанови. 2020 року ICO спільно з Alan Turing Institute розробили Рекомендації з пояснення рішень, прийнятих ШІ, у яких визначили шість видів пояснень (раціональне, результат-орієнтоване, щодо процесу, про дані, запобіжне та контекстуальне) і як їх надавати суб'єктам даних. Це фактично розшифрування вимог прозорості й ст. 22 GDPR для розробників [6; 8]. Також ICO протягом 2022–2023 років опублікував серію рекомендацій: щодо використання ШІ для біометричної класифікації осіб, щодо синтетичних даних, приватності дітей в алгоритмах [73].

2019 року ICO наклав умовний штраф 99 млн фунтів стерлінгів на готельну мережу Marriott за витік даних, 183 млн – на British Airways за хакерську атаку, продемонструвавши, що великим фірмам слід інвестувати в захист даних, інакше штрафи будуть відчутними [73]. Хоча зрештою штрафи зменшили, сигнал був очевидний. 2022 року ICO оштрафував Clearview AI на 7,5 млн фунтів стерлінгів і наказав видалити всі фото мешканців Британії зі своєї бази [73]. Clearview подав апеляцію до трибуналу, який 2023 року несподівано скасував штраф, вирішивши, що ICO не довела свою юрисдикцію (бо компанія не працювала безпосередньо в Британії) [73]. ICO оскаржує це рішення [73]. Але навіть без стягнення штрафу Clearview майже витіснено з британського ринку, і більшість держорганів відмовилися з нею працювати [73].

Ще один напрям – саморегуляція за стимулом регулятора. ICO 2021 року провела розслідування щодо рекламних технологій («AdTech») і виявила, що система реального аукціону реклами (RTB) порушує принципи приватності (дані про користувачів передають сотням компаній без їх відома). ICO погрожувала санкціями, тож галузь частково реформували: Google заявив про поетапну відмову від сторонніх cookies (Privacy Sandbox), інші впроваджують моделі таргетингу без передачі «сирих» персональних даних [73]. Це стосується ШІ опосередковано, адже рекламні алгоритми – вид ШІ, що профілює користувачів. Британський підхід полягає в тому, щоб через конструктивний тиск стимулювати нові технічні рішення, сумісні з приватністю.

Отже, Велика Британія дотримується парадигми GDPR, але розглядає більш гнучкі методи регулювання ШІ – через керівництва галузевих регуляторів і стимулювання відповідальної інновації [73; 118]. Для України британський досвід цікавий поєднанням жорсткого нагляду (штрафи, накази видаляти дані) з детальними роз'ясненнями для бізнесу, як виконувати вимоги закону на практиці [73]. У наших реаліях часто бракує саме таких практичних гайдів. Створення, наприклад, рекомендацій для державних органів щодо використання алгоритмів або настанов для ІТ-компаній з поясненнями щодо ШІ – завдання, яке міг би реалізувати український уповноважений з прав людини (як орган контролю за даними) або Мінцифри спільно з експертним середовищем [43].

Канада: модернізація підходів до захисту приватності та формування окремого регулювання штучного інтелекту. Канаду традиційно розглядають як державу з розвиненою правовою культурою захисту приватності. Канадські фахівці брали участь у формуванні глобальних принципів захисту персональних даних, зокрема в межах розроблення рекомендацій Організації економічного співробітництва та розвитку 1980 року [103]. Прийняття 2000 року Закону про захист персональної інформації та електронні документи (PIPEDA) стало одним із

перших прикладів комплексного національного регулювання в цій сфері [81]. Водночас після набуття чинності Загальним регламентом про захист даних Європейського Союзу канадську модель стали сприймати як таку, що потребує суттєвого оновлення, і це зумовило ініціювання законодавчої реформи [118].

У червні 2022 року уряд Канади вніс до парламенту законопроєкт C-27, який передбачає комплексне оновлення регулювання та охоплює три взаємопов'язані акти: новий Закон про приватність споживачів (Consumer Privacy Protection Act, CPPA), Закон про трибунал з питань даних, Закон про штучний інтелект і дані (Artificial Intelligence and Data Act, AIDA) [81]. Станом на 2025 рік цей законопроєкт знаходився на стадії парламентського розгляду, однак його зміст дає змогу окреслити напрям, у якому трансформується канадська модель правового регулювання.

Проєкт CPPA спрямований на суттєве посилення вимог до обробки персональних даних. Він закріплює підхід відповідальної обробки, який за змістом наближається до принципу підзвітності, розширює перелік прав суб'єктів даних, зокрема шляхом запровадження права на перенесення та вилучення інформації, а також передбачає значні фінансові санкції за порушення. У проєкті закону виокремлено чутливу персональну інформацію як самостійну категорію, для обробки якої є вимога щодо отримання явної згоди. Важливою новелою є обов'язок організацій надавати особі інформацію про використання автоматизованих систем ухвалення рішень і пояснювати загальні принципи їх функціонування, що наближається до підходу, закріпленого в ст. 22 GDPR [81; 118]. У такий спосіб CPPA створює нормативну основу для контролю алгоритмічних процесів у межах законодавства про приватність.

Проєкт Закону про штучний інтелект і дані (AIDA) є першою спробою запровадження в Канаді спеціального правового режиму, спрямованого безпосередньо на регулювання використання технологій штучного інтелекту.

Його положення орієнтовані на системи загального призначення, використання яких пов’язане з обробкою даних про людину та потенційною шкодою. Законопроєкт передбачає ідентифікацію високоризикових систем, запровадження обов’язкових процедур оцінювання відповідності й управління ризиками, а також заборону несанкціонованого збирання персональних даних для навчання алгоритмічних моделей. Запропонований підхід засвідчує про прагнення Канади розмежувати регулювання приватності та регулювання штучного інтелекту, не зводячи останнє виключно до інструментів захисту персональних даних [81].

Практика канадських наглядових органів демонструє активне застосування наявних регуляторних механізмів ще до прийняття нових законів. Показовим є розслідування Федерального комісара з приватності щодо діяльності компанії Clearview AI, здійснене спільно з провінційними регуляторами. Було встановлено, що масовий збір зображень із відкритих джерел для розпізнавання облич порушує вимоги щодо згоди та законної мети обробки. Компанія не має фізичної присутності в Канаді, регуляторний тиск і публічність висновків призвели до фактичного припинення її діяльності на канадському ринку [81].

Схожу логіку застосовано і у справі щодо використання біометричної аналітики в торговельних центрах компанією Cadillac Fairview, де прихований збір зображень відвідувачів для маркетингової мети було визнано не сумісним із вимогами законодавства про приватність. Унаслідок цього компанія була змушена припинити використання відповідних технологій [81]. Такі кейси свідчать про реальну дієвість регуляторного контролю навіть за умов обмежених формальних повноважень наглядового органу.

Канада також активно залучена до міжнародних ініціатив у сфері штучного інтелекту та прав людини, зокрема бере участь у роботі Глобального партнерства з питань ШІ й у переговорах щодо Конвенції Ради

Європи про штучний інтелект, що підтверджує орієнтованість держави на узгодження національного регулювання з глобальними стандартами [70; 116].

Для України канадський досвід є показовим з огляду на поєднання двох взаємодоповнюваних напрямів: модернізації законодавства про приватність і розроблення окремого правового режиму для штучного інтелекту. Важливим є і приклад активної ролі наглядового органу, який впливає на практику через розслідування та публічні висновки, що може бути корисним для посилення інституційної спроможності національних органів у сфері захисту персональних даних [43].

Японія: адаптація міжнародних стандартів і гнучкий підхід до регулювання штучного інтелекту. Японська модель захисту персональних даних ґрунтується на Законі про захист персональної інформації (APPI), який після низки законодавчих змін був визнаний Європейським Союзом таким, що забезпечує адекватний рівень захисту персональних даних. Це створило правову основу для транскордонного обміну інформацією, водночас дало змогу зберегти національну специфіку регулювання [54].

Підхід Японії до регулювання штучного інтелекту вирізняється перевагою загальних принципів і механізмів саморегуляції над жорстким нормативним контролем. Державні стратегії розвитку ШІ орієнтовані на поєднання інновацій із забезпеченням довіри до технологій, що відображено в програмі Society 5.0 й етичних принципах, розроблених за участю бізнесу й експертної спільноти [103]. Водночас Комісія із захисту персональних даних (PPC) активно використовує інструменти м’якого права, зокрема роз’яснення щодо створення та використання анонімізованої інформації, що стимулює інноваційну діяльність без зниження рівня захисту приватності [54].

Практика правозастосування засвідчує, що навіть без спеціального закону про штучний інтелект японські регулятори здатні реагувати на ризики, пов’язані з алгоритмічною обробкою даних. Інцидент із платформою LINE, пов’язаний із транскордонною передачею даних і доступом сторонніх підрядників, призвів до регуляторного втручання та коригування

корпоративних практик. Використання технологій розпізнавання облич у публічних просторах стало предметом суспільної дискусії та регуляторних заяв, що сформувало запит на дотримання балансу між безпекою і приватністю [54].

Для України японський досвід є показовим прикладом адаптації європейських стандартів без механічного копіювання. Запровадження спеціальних категорій даних, чітке регулювання обігу псевдонімізованої та анонімізованої інформації, а також створення стимулів для відповідального використання даних у сфері інновацій можуть бути враховані під час оновлення національного законодавства про захист персональних даних і штучний інтелект [37].

Узагальнення іноземного досвіду й імплементація для України. На основі здійсненого аналізу можна виокремити спільні риси правового регулювання персональних даних в епоху ШІ в різних державах [103; 116; 118]:

1. **Всеохопне законодавство про захист даних як фундамент.** Майже всі розвинуті країни мають або впровадили (ЄС, Британія, Японія, Канада), або активно рухаються до впровадження (США на рівні штатів) загальних норм щодо приватності, близьких за принципами до GDPR [54; 66; 67; 81; 118]. Це охоплює права суб'єктів, принципи обробки, регуляторні органи, штрафи [118]. Для України це означає нагальність прийняття нового закону № 8153 (GDPR адаптованого) [37; 107; 115]. Без міцного базового закону про дані говорити про захист приватності в ШІ буде неможливо [36].

2. **Визначення і захист спеціальних (чутливих) категорій даних.** Усі країни признають, що певні дані (біометрія, здоров'я, етнічність тощо) потребують підвищеного захисту [54; 81; 118]. У контексті ШІ це критично, бо алгоритми можуть ці дані й генерувати (як висновки) [105; 106]. Зарубіжний досвід полягає в тому, щоб вимагати явної згоди або законної необхідності для таких даних [118; 81]. Україна повинна зберегти та

розширити перелік чутливих даних у новому законі, урахувати нові види (генетичні, біометричні дані, дані дітей) [37; 69].

3. **Регулювання автоматизованих рішень і профілювання.** ЄС через ст. 22 GDPR дав імпульс і в законах Канади, і США: людям потрібні гарантії, що рішення ШІ не будуть їх утискати без можливості оскарження [66; 81; 118]. Отже, право на людський перегляд і на пояснення рішення – ключові інструменти [118; 138]. Україна може імплементувати аналог ст. 22 GDPR у своє законодавство [37]. У законопроєкті № 8153 уже є право не підлягати автоматизованому рішенню із суттєвими наслідками (ст. 20) [37]. Важливо потім розробити механізм реалізації цього права – процедури звернення суб'єкта, строки і форми надання пояснень [107].

4. **Privacy by design і оцінювання ризиків.** Усі юрисдикції безпосередньо або через рекомендації вимагають, щоб захист приватності було вибудовано в системах одразу [65; 103; 118]. Також поширеним є зобов'язання проводити оцінку впливу (DPIA) для високоризикових випадків (у ЄС прямо, у Канаді й деяких штатах США – вводять) [66; 81; 118]. Україна має включити вимогу DPIA до свого закону, передусім для таких випадків, як державні реєстри, великі системи відеоспостереження, системи автоматичного розпізнавання [37; 72]. Крім того, слід закріпити принцип «налаштувань приватності за замовчуванням» – щоб постачальники технологій ШІ надавали продукти з максимально захищеними опціями [118].

5. **Посилення відповідальності та нагляд.** Зарубіжний досвід демонструє реальні санкції: багатомільйонні штрафи (ЄС, Велика Британія), судові позови (США), вимоги видалити незаконно отримані дані й моделі (FTC, європейські DPA) [66; 69; 98; 118]. Для імплементації Україна повинна забезпечити дієвість санкцій [37]. У законопроєкті № 8153 запропоновано штрафи до 300 тис. грн – їх треба впровадити і забезпечити стягнення [37; 107]. Також необхідно підняти інституційну спроможність омбудсмена чи окремого органу: розширити кадри для проведення експертизи, щоб вони

могли проводити аудит алгоритмів [39]. Можливо, слід розглянути створення окремого підрозділу чи агентства із ШІ-етики, однак це на перспективу [43].

6. **Спеціальні правила для біометрії та відеоспостереження.** Чимало країн через скандали з Clearview, FR-технологіями зрозуміли необхідність посиленої уваги до цього [66; 73]. Україна також постає перед такими проблемами: в умовах війни застосовують технології розпізнавання осіб ворога, але після війни такі системи потребують перегляду [43]. Тому вже зараз слід закласти норми: хто і як може використовувати біометрію, передбачити гарантії (згода, альтернативні методи ідентифікації, заборона використання в реальному часі громадськими інституціями без дозволу суду, тощо) [116; 118; 124]. Європейський AI Act планує заборонити масове розпізнавання облич у реальному часі в публічних місцях – Україна може врахувати це і не рухатися до «state surveillance» [124].

7. **Міжнародна кооперація.** Для України важливо приєднуватися до міжнародних режимів: ратифікувати Конвенцію 108+, долучитися до нової Конвенції Ради Європи про ШІ [70; 102; 132]. Це не лише престиж, а й практична користь – доступ до найкращих практик, участь в обміні досвідом між регуляторами, можливість впливати на глобальні правила [87; 116]. Як країна – кандидат для вступу до ЄС Україна апріорі буде переймати законодавство ЄС, включно з AI Act, тож потрібно вже готувати експертів, бізнес, суспільство до цих змін [43; 124].

8. **Освіта і просвіта.** У всіх країнах фокус на тому, що разом із законами слід проводити просвітницькі заходи – як для компаній (про відповідність вимогам), так і для громадян (про їхні права) [65; 103; 116]. Регулятори типу ICO, OPC публікують у відкритому доступі [73; 81]. Українському регулятору слід створити схожі матеріали українською, проводити семінари для IT-сектору про вимоги приватності, залучати громадські організації до моніторингу випадків порушень [42; 43].

Можливості імплементації в Україні можна звести до конкретних кроків:

– прийняти новий рамковий Закон про захист персональних даних (гармонізований з GDPR) – це надасть Україні статус країни з адекватним рівнем захисту, відкриє обмін даними з ЄС і надасть інструменти протидії зловживанням [37; 107; 115];

– внести зміни до суміжних законів і підзаконних актів: про електронні комунікації (щодо cookie і метаданих), про банківську таємницю (щодо скорингу), про охорону здоров'я (щодо телемедицини і даних пацієнтів для ШІ-діагностики), про державні послуги онлайн (Дія та інші – щоб відповідали privacy by design) [36; 43].;

– створити при уряді або Раді національної безпеки робочу групу з AI-етики, яка розробила б національні принципи використання ШІ (можливо, на основі ЮНЕСКО чи ОЕСР, адаптовані до українського контексту) [43; 103; 116];

– посилити інституційну незалежність і ресурсне забезпечення органу захисту даних. Без сильного наглядача навіть досконалий закон не працюватиме [39]. Можливо, слід розглянути створення окремого агента (Data Protection Authority) замість покладання всіх обов'язків на Омбудсмена або принаймні створити окрему експертну службу в його структурі [39];

– запровадити практику проведення тестів на захист даних і права під час упровадження нових технологій державою [72]. Наприклад, у разі введення систем відеонагляду з аналітикою – обов'язковими є консультація з Омбудсменом, громадські слухання щодо необхідності та пропорційності [116];

– урахувати досвід і помилки інших: наприклад, провести аудит наших державних баз, чи не передають дані необдумано третім сторонам (як у випадку LINE) [54]. Або оцінити, чи немає в нас аналогів Clearview (можливо, якісь компанії збирають фото із соцмереж – слід відстежити і зупинити це) [66];

– підтримати бізнес у впровадженні відповідального ШІ: розробити добровільні кодекси практики для ІТ-компаній, стартапів з AI [43; 103].

Можна за прикладом Сінгапуру (Model AI Governance Framework) створити в Україні пілотний проєкт з декількома компаніями, щоб ті випробували внутрішні політики прозорості, справедливості алгоритмів, а потім поширити це далі [103].

Наостанок слід зазначити, що імплементація зарубіжного досвіду має враховувати українські реалії [43]. У період дії правового режиму воєнного стану є намір розширити державне спостереження заради безпеки [43]. Проте зарубіжний досвід (приклад США після 2001 року чи Європи з її дискусією про «справедливий баланс») демонструє: це підриває довіру громадян і в довгостроковій перспективі шкодить демократії [116; 125]. Тому захист персональних даних повинен лишатися одним з пріоритетів навіть у складні часи [22, с. 141; 125]. Україна, яка виборює європейське майбутнє, має демонструвати відданість європейським цінностям, а право на приватність належить до базових [22, с. 141; 102].

Закордонний досвід пропонує Україні багатий набір інструментів – від правових норм до організаційних практик – для регулювання захисту персональних даних у сфері ШІ [103; 116; 118]. Імплементація цього досвіду потребує політичної волі, законодавчих змін і просвітницької роботи [43]. Проте вигода очевидна: утвердження довіри до цифрових технологій, захист громадян від нових ризиків, а також відкриття можливостей для участі у глобальній цифровій економіці як рівноправний партнер [87].

Висновки до розділу 2

У другому розділі дисертаційного дослідження здійснено комплексний порівняльно-правовий аналіз іноземного досвіду нормативно-правового регулювання захисту персональних даних у сфері штучного інтелекту, що надало можливість виявити як спільні тенденції розвитку відповідного правового регулювання, так і національні особливості підходів окремих

держав та регіонів. Дослідження засвідчило, що інтенсивне впровадження штучного інтелекту в публічну та приватну сфери зумовлює трансформацію традиційних моделей захисту персональних даних і потребує формування нових правових механізмів, орієнтованих на запобігання ризикам, пов'язаним з автоматизованою та алгоритмічною обробкою інформації про особу.

Аналіз підходів Європейського Союзу дає підстави стверджувати, що саме модель, побудована на Загальному регламенті про захист даних, сформувала найсистемніший і цілісний режим правової охорони персональних даних у контексті застосування штучного інтелекту. Хоча GDPR не містить спеціального регулювання штучного інтелекту, його принципи, інститути та гарантії, зокрема принципи законності, прозорості, мінімізації даних, підзвітності, а також механізми оцінки впливу на захист даних, права на заперечення проти автоматизованих рішень і вимоги щодо privacy by design і privacy by default, фактично виконують функцію універсального правового фільтра для алгоритмічних систем. Судова та регуляторна практика ЄС, передусім рішення Суду Європейського Союзу та діяльність національних органів захисту даних, підтверджує, що навіть найновітніші форми генеративного та прогнозного штучного інтелекту не виводяться за межі дії законодавства про персональні дані.

Розгляд національних практик держав – членів ЄС, зокрема Естонії, продемонстрував, як європейські правові стандарти імплементуються у високодиджиталізованих адміністративних системах. Естонський досвід засвідчив, що навіть за активного використання алгоритмічних рішень у публічному управлінні ключовими умовами їх допустимості залишаються прозорість, можливість людського контролю та підзвітність. Практика поєднання технічних архітектурних рішень із правовими вимогами GDPR дає змогу стверджувати про ефективність інтегрованого підходу, у межах якого правові принципи безпосередньо впливають на дизайн цифрових систем.

Дослідження американської моделі регулювання виявило її фрагментарний, водночас динамічний характер. Брак єдиного федерального закону про захист персональних даних компенсується розвитком галузевого законодавства, активною роллю регуляторних органів і судовою практикою. Посилену увагу привертає підхід, за якого порушення правил обробки персональних даних може тягнути за собою не лише санкції, а й обов'язок знищення алгоритмів, створених на незаконно зібраних даних. Така практика формує превентивний ефект і нерозривний зв'язок між легальністю даних та легітимністю систем штучного інтелекту.

Аналіз підходу Великої Британії демонструє збереження загальної логіки GDPR за одночасного прагнення до гнучкішого та принципо орієнтованого регулювання штучного інтелекту. Акцент на регуляторних настановах, практичних рекомендаціях і міжінституційній координації дає змогу британській моделі поєднувати високий рівень захисту персональних даних із підтримкою інновацій. Діяльність національного органу із захисту даних у сфері алгоритмічної прозорості та пояснюваності рішень свідчить про важливість не лише формальних норм, а й ефективних інструментів їх практичної реалізації.

Канадський досвід продемонстрував тенденцію до модернізації правового регулювання через поєднання оновленого законодавства про персональні дані з розробленням спеціального правового режиму для штучного інтелекту. Запропонована модель, у межах якої окремо врегульовують високоризикове використання алгоритмічних систем, засвідчує поступовий перехід від виключно приватнісного підходу до ширшого регулювання соціальних і правових наслідків застосування штучного інтелекту. Важливим є також активна роль наглядових органів, які через розслідування та публічні висновки впливають на поведінку суб'єктів навіть без максимальних санкційних повноважень.

Японський підхід до захисту персональних даних у сфері штучного інтелекту вирізняється прагненням до балансу між регуляторними гарантіями

та стимулюванням інновацій. Гармонізація національного законодавства з європейськими стандартами поєднується з розвитком механізмів саморегуляції та використанням знеособлених і псевдонімізованих даних. Такий підхід демонструє можливість адаптації міжнародних стандартів без їх механічного копіювання та врахування національних особливостей правової культури.

Узагальнюючи результати аналізу зарубіжного досвіду, можна констатувати, що ключовими елементами ефективного захисту персональних даних у сфері штучного інтелекту є: наявність базового всеохопного законодавства про захист персональних даних; спеціальні гарантії щодо автоматизованого прийняття рішень і профілювання; обов'язкове врахування ризиків для прав людини на етапі проєктування та впровадження алгоритмічних систем; дієвий і незалежний нагляд. Ці елементи в різних комбінаціях простежуються в правових системах більшості досліджених юрисдикцій.

Для України результати другого розділу мають принципове значення, оскільки підтверджують необхідність гармонізації національного законодавства із сучасними міжнародними стандартами захисту персональних даних, з огляду на специфіку використання штучного інтелекту. Іноземний досвід засвідчує, що ефективне регулювання в цій сфері можливе лише за умови поєднання правових, організаційних і технічних механізмів, а також за наявності політичної волі до забезпечення реальної, а не декларативної охорони прав людини. Отримані висновки створюють основу для подальшого аналізу сучасного стану правового регулювання в Україні та формування практичних пропозицій з його вдосконалення, що і становить предмет дослідження наступного розділу дисертації.

Важливим результатом дослідження є також виявлення посилення ролі наглядових органів і судової практики у формуванні стандартів допустимого використання штучного інтелекту. Зарубіжний досвід демонструє, що саме через інтерпретацію загальних принципів захисту даних, прийняття

обов’язкових приписів, застосування санкцій та оприлюднення рекомендацій відбувається фактична конкретизація вимог до алгоритмічних систем. Це засвідчує, що ефективне регулювання у сфері штучного інтелекту неможливе без інституційно спроможного й незалежного органу контролю, здатного поєднувати правову, технічну й етичну експертизи.

РОЗДІЛ 3
СУЧАСНИЙ СТАН І ШЛЯХИ ВДОСКОНАЛЕННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ШТУЧНОГО ІНТЕЛЕКТУ В УКРАЇНІ З ОГЛЯДУ НА МІЖНАРОДНИЙ ДОСВІД

3.1. Сучасний стан і тенденції розвитку національного законодавства щодо захисту персональних даних у сфері штучного інтелекту

Сучасний стан національного законодавства України у сфері захисту персональних даних характеризується браком спеціалізованого нормативного регулювання, орієнтованого безпосередньо на використання технологій штучного інтелекту, що зумовлює застосування загальних правових конструкцій до принципово нових способів обробки інформації. Правові норми, які нині використовують для регламентації обробки персональних даних, були сформовані на підставі традиційних інформаційних процесів і не передбачали появи автономних, самонавчальних і масштабованих систем, здатних здійснювати комплексний аналіз великих масивів даних без безпосереднього людського втручання. Чинна модель захисту персональних даних сформована переважно в умовах традиційних інформаційних відносин і ґрунтується на уявленні про лінійну, прогнозовану та контрольовану обробку даних, що не відповідає реальним практикам функціонування сучасних ШІ-систем [101; 126].

Використання алгоритмічних систем машинного навчання, зокрема генеративних моделей, порушує класичну логіку правового регулювання, у якій суб’єкт обробки даних здатен повністю визначити завдання, обсяг і наслідки відповідної обробки. У національному законодавстві немає норм, що враховували б такі властивості ШІ, як стохастичний характер результатів,

самонавчання, непрозорість внутрішніх процесів прийняття рішень і можливість вторинного використання даних у масштабах, які не передбачали на момент їх первинного збирання [68; 84]. Унаслідок цього правозастосування ґрунтується переважно на формальному тлумаченні загальних принципів, таких як законність, справедливість і прозорість обробки, що не забезпечує належного рівня превентивного захисту прав суб'єктів персональних даних. Брак у національному праві спеціальних вимог до алгоритмічних систем призводить до ситуації, за якої оцінювання правомірності обробки здійснюють уже після виникнення негативних наслідків, а не на етапі проєктування та впровадження ШІ-рішень.

Фрагментарність чинного регулювання виявляється також у відсутності системного підходу до співвідношення норм про захист персональних даних із суміжними галузями цифрового права, зокрема регулюванням інформаційної безпеки, кібербезпеки та використання автоматизованих рішень у публічному управлінні. Така ізольованість правових режимів ускладнює комплексну оцінку ризиків, пов'язаних із використанням ШІ, і не дає змоги сформувати цілісну модель захисту приватності в цифровому середовищі, де персональні дані є одночасно об'єктом правової охорони та ключовим ресурсом функціонування алгоритмічних систем. У науковій літературі обґрунтовують, що така роз'єднаність нормативних масивів створює ситуацію, за якої навіть формально коректне дотримання вимог щодо персональних даних не гарантує реального захисту приватності в умовах комплексних цифрових систем [23; 49].

Орієнтованість на інститут згоди як центральний елемент легітимації обробки персональних даних становить також частину проблемних питань. У національному законодавстві згоду традиційно розглядають як універсальний механізм балансування інтересів суб'єкта даних і суб'єкта обробки, однак у контексті використання ШІ-систем така конструкція дедалі частіше втрачає свою регулятивну ефективність. У контексті ШІ-систем згода дедалі частіше набуває декларативного характеру, оскільки суб'єкт

даних об’єктивно не здатен усвідомити всі можливі сценарії використання інформації, включно з повторним навчанням моделей, агрегацією даних і потенційними ризиками відновлення персональної інформації з моделей [53; 77]. Така ситуація засвідчує кризу класичної моделі згоди та потребу переосмислення її ролі в національному праві, з огляду на технологічні обмеження та асиметрію знань між суб’єктами обробки й суб’єктами даних [101].

Наявні прогалини національного регулювання посилюються браком чітких вимог до організаційних і технічних заходів захисту персональних даних у процесі розроблення та впровадження ШІ. Законодавство не встановлює обов’язкових стандартів щодо інтеграції принципів захисту даних у життєвий цикл алгоритмічних систем, що створює правову невизначеність для розробників і користувачів ШІ та знижує рівень відповідальності за потенційні порушення прав суб’єктів даних. На відміну від сучасних міжнародних підходів, які керуються необхідністю інтеграції правових принципів безпосередньо в дизайн й архітектуру технологічних систем, українське законодавство зберігає переважно постфактум орієнтований характер, зосереджений на відповідальності за порушення, а не на запобіганні ризикам [110; 112]. Це обмежує ефективність правового регулювання в умовах швидкого розвитку штучного інтелекту та зумовлює потребу його подальшої еволюції.

Поточний стан національного законодавства щодо захисту персональних даних у сфері штучного інтелекту можна схарактеризувати як перехідний. Воно знаходиться на етапі поступової трансформації від універсальної, технологічно нейтральної моделі регулювання до спеціалізованого підходу, здатного враховувати особливості алгоритмічної обробки даних і пов’язані з нею ризики. Водночас несформованість чіткої законодавчої стратегії у сфері ШІ спричиняє фрагментарність реформ і залежність національного правового розвитку від зовнішніх орієнтирів та міжнародних стандартів. Саме ця обставина визначає подальші тенденції

розвитку національного правового регулювання, орієнтовані на поступову спеціалізацію норм, запозичення міжнародного досвіду й упровадження ризик-орієнтованих підходів до захисту персональних даних у сфері ШІ [80; 97].

Однією з ключових змін, зумовлених розвитком штучного інтелекту, є переосмислення ролі персональних даних у правовому регулюванні. Дані вже не розглядають виключно як об’єкт правової охорони, дедалі частіше вони функціонують як стратегічний ресурс для навчання, оптимізації та масштабування алгоритмічних систем. У цьому сенсі персональні дані можуть використовувати багаторазово, у різних комбінаціях і для завдань, які не завжди є передбачуваними на етапі їх первинного збирання. Така практика вступає в напружене співвідношення з принципом цільового обмеження, який є основою національного законодавства про захист персональних даних, оголює його обмежену адаптивність до умов алгоритмічної обробки інформації [53; 77].

Увагу на себе перебирає питання правової кваліфікації обробки персональних даних у процесі навчання та донавчання моделей штучного інтелекту. У національному праві немає чітких критерії, які дозволяли б відмежувати допустиме повторне використання даних від такої обробки, що виходить за межі первісної правової підстави. Це створює правову невизначеність як для розробників ШІ-систем, так і для суб’єктів даних, права яких можуть порушувати без явного порушення формальних вимог законодавства. Унаслідок цього ефективність правового захисту безпосередньо залежить від добросовісності суб’єктів обробки, що не відповідає сучасним уявленням про належний рівень гарантій прав людини в цифровому середовищі [101].

Подальший розвиток генеративних моделей та великих мовних систем посилює зазначені проблеми, оскільки результати їх функціонування можуть містити інформацію, яка дає змогу ідентифікувати конкретних осіб або формувати висновки про їхні персональні характеристики. Наукові

дослідження демонструють, що навіть за умов формальної анонімізації навчальних наборів даних є ризик відновлення персональної інформації шляхом атак на моделі або аналізу їхніх вихідних даних [68; 84]. Це підриває звичні підходи до знеособлення інформації, які досі активно використовують у національній правозастосовній практиці як універсальний засіб мінімізації ризиків для приватності.

Використання штучного інтелекту для автоматизованого прийняття рішень і профілювання осіб додатково ускладнює забезпечення ефективного захисту персональних даних. Алгоритмічні рішення дедалі частіше впливають на доступ до послуг, можливості реалізації соціальних і економічних прав, а також на правове становище особи загалом. Водночас обмежена пояснюваність низки ШІ-систем створює ситуацію, за якої суб'єкт даних не має реальної можливості зрозуміти логіку прийнятого щодо нього рішення або ефективно його оскаржити. Без спеціальних національних механізмів контролю та нагляду зростає ризик непропорційного втручання в права людини та підривається довіра до цифрових технологій [101; 137].

Важливим аспектом впливу розвитку штучного інтелекту є поглиблення асиметрії інформації між суб'єктами обробки персональних даних і суб'єктами даних. Складність алгоритмічних моделей, багаторівнева структура ланцюгів постачання ШІ-рішень і використання транснаціональних технологічних платформ фактично унеможливлюють повну реалізацію принципу прозорості в його класичному розумінні. Це ставить під сумнів практичну здійсненність таких прав, як право на доступ до персональних даних, право на виправлення та право на заперечення проти обробки, які залишаються декларативними без відповідних організаційних і технічних гарантій [49; 101].

У сукупності зазначені фактори свідчать про те, що розвиток технологій штучного інтелекту змінює не лише інструментарій обробки персональних даних, а й логіку правового регулювання в цій сфері. Національна модель захисту персональних даних постає перед необхідністю

адаптації до умов, у яких ризики для приватності мають системний, а не поодинокий характер, а наслідки обробки даних можуть виявлятися непрямо, з часовою затримкою. Це зумовлює потребу переходу до комплексного, ризик-орієнтованого підходу в правовому регулюванні, що враховуватиме як технологічні особливості ШІ-систем, так і міжнародні тенденції розвитку права у сфері захисту персональних даних [80; 97].

Європейський Союз посідає основне місце у формуванні сучасних стандартів захисту персональних даних у цифровому середовищі, пропонуючи комплексну модель правового регулювання, що поєднує жорсткі нормативні вимоги з ризик-орієнтованим підходом. У цьому контексті Регламент ЄС про штучний інтелект (AI Act) є не лише спеціальним актом, спрямованим на регулювання ШІ-систем, а й важливим орієнтиром для подальшого розвитку національного законодавства держав, які прагнуть правової сумісності з європейським простором. Хоча AI Act формально не є частиною національної правової системи України, його концептуальні підходи дедалі активніше використовують як модель для формування внутрішніх політик і законодавчих ініціатив у сфері ШІ та захисту персональних даних [80; 97]. Значущою стає ідея комплексного регулювання, за якої захист персональних даних розглядають не як ізольований інститут, а як елемент ширшої екосистеми цифрового права. Європейська модель передбачає узгоджене застосування норм про захист даних, регулювання цифрових сервісів, відповідальність технологічних платформ і забезпечення прав людини в алгоритмічному середовищі. Для національного законодавства України це означає необхідність поступового відходу від фрагментарного запозичення окремих положень і перехід до системного врахування європейських стандартів як взаємопов’язаного нормативного комплексу [47; 49].

Водночас інтеграція європейських підходів у національне регулювання не може зводитися до формальної імплементації окремих принципів або термінології. Особливості правової системи України, рівень інституційної

спроможності й стан розвитку цифрової інфраструктури зумовлюють потребу адаптації міжнародних стандартів з огляду на національний контекст. У науковій літературі обґрунтовано, що механічне копіювання європейських норм без належного інституційного забезпечення може призвести до декларативності правового регулювання та зниження його практичної ефективності [49; 101].

Орієнтири для розвитку національного законодавства у сфері захисту прав людини в умовах цифровізації формуються, зокрема, у документах Ради Європи та Організації Об'єднаних Націй, які закріплюють універсальні підходи до відповідного правового регулювання. Рамкова конвенція Ради Європи щодо штучного інтелекту, прав людини, демократії та верховенства права формує ціннісну основу для оцінювання допустимості використання ШІ з погляду фундаментальних прав і свобод. Для України ці документи мають особливе значення як інструменти зближення з європейським правовим простором і водночас як джерело гнучких принципів, які можуть бути інтегровані в національне законодавство без надмірного регуляторного навантаження [70; 80; 132].

Поряд з обов'язковими міжнародно-правовими актами дедалі важливішого значення набувають документи «м'якого права», зокрема рекомендації міжнародних організацій, етичні кодекси та керівні принципи у сфері штучного інтелекту. Вони відіграють важливу роль у формуванні практик правозастосування та слугують своєрідним мостом між правовими вимогами й технологічними реаліями. Для національного законодавства України такі документи є джерелом концептуальних підходів до побудови ризик-орієнтованої моделі регулювання, яка дає змогу враховувати швидкі темпи розвитку ШІ без постійного внесення змін до законодавства [56; 101; 116].

Отже, інтеграція міжнародних і європейських стандартів у національне регулювання захисту персональних даних у сфері штучного інтелекту є багатовимірним процесом, що охоплює не лише запозичення окремих

правових норм, а й трансформацію логіки правового регулювання. Для України цей процес є одночасно викликом і можливістю: викликом – через необхідність адаптації складних нормативних моделей до національних реалій, можливістю – завдяки формуванню сучасної, системної та ефективної моделі захисту персональних даних, здатної відповідати викликам алгоритмічної епохи та забезпечувати належний рівень захисту прав людини [80; 97; 101].

Процеси розвитку національного законодавства України у сфері захисту персональних даних у контексті використання штучного інтелекту неможливо розглядати ізольовано від міжнародних і європейських правових тенденцій. В умовах глобалізації цифрових ринків, транснаціонального характеру обробки даних й активного використання алгоритмічних систем національні правопорядки дедалі частіше змушені орієнтуватися на зовнішні нормативні моделі, які формують загальні стандарти допустимої обробки персональної інформації. Для України така орієнтованість має не лише техніко-правове, а й стратегічне значення, оскільки інтеграцію міжнародних підходів розглядають як складову європейського вектору розвитку та гармонізації національного законодавства [47, с. 149–156; 80].

Інтеграція міжнародних стандартів передбачає використання підходів до оцінювання впливу алгоритмічних систем на права людини та захист персональних даних. У міжнародній практиці дедалі активніше застосовують механізми попереднього оцінювання ризиків, спрямовані на ідентифікацію потенційних загроз ще на етапі розроблення та впровадження ШІ. Для України це відкриває можливість переходу від реактивної моделі правового захисту до превентивної, у якій ключову роль відіграють не санкції за порушення, а запобігання їм шляхом належного правового й організаційного планування [101; 112].

Водночас інтеграція міжнародних і європейських стандартів у національне регулювання супроводжується низкою викликів. Серед них – ризик нормативної фрагментації, коли різні міжнародні підходи

імплементують без належної координації, а також небезпека формального виконання зобов’язань без реального впливу на практику обробки персональних даних. У таких умовах ключове значення має формування узгодженої державної політики у сфері штучного інтелекту й захисту персональних даних, здатної поєднати міжнародні стандарти з національними пріоритетами розвитку [47, с. 149–156; 49, с. 15–18].

Додатково слід зауважити, що європейський підхід до регулювання штучного інтелекту й захисту персональних даних ґрунтується на поєднанні правових, інституційних і політичних інструментів, що в сукупності формують багаторівневу систему гарантій. Для України це означає необхідність усвідомлення того, що інтеграція міжнародних стандартів не може обмежуватися рівнем формального законодавчого запозичення. Вона потребує створення відповідного нормативного середовища, у межах якого принципи захисту персональних даних будуть функціонувати як обов’язкові орієнтири для всієї екосистеми розроблення та використання ШІ, включно з приватним сектором, публічним управлінням і науково-дослідною діяльністю [47; 49].

У цьому контексті важливе значення мають питання нормативної узгодженості між різними міжнародними документами, що регулюють суміжні аспекти цифрових відносин. Міжнародні стандарти у сфері прав людини, рекомендації щодо етики штучного інтелекту, документи з питань цифрового врядування та захисту персональних даних формують складний і багатопластовий регуляторний ландшафт. Для національного законодавця це створює ризик фрагментації правового регулювання, коли імплементація окремих стандартів відбувається без урахування їх системного взаємозв’язку. У наукових дослідженнях зауважують, що така фрагментація може знизити передбачуваність правозастосування та ускладнити реалізацію прав суб’єктів персональних даних у цифровому середовищі [101].

Міжнародні та європейські стандарти у сфері штучного інтелекту дедалі частіше виходять за межі суто правових приписів і формують

комплексні рамки поведінки для учасників цифрових ринків. Такі рамки поєднують юридично обов'язкові норми з рекомендаційними положеннями, етичними принципами й технічними стандартами, що спільно визначають допустимі межі використання алгоритмічних систем. Для України це відкриває можливість використання гнучких інструментів регулювання, які дають змогу реагувати на технологічні зміни без постійного перегляду законодавства, водночас потребують високого рівня інституційної координації та експертного забезпечення [56; 116].

У сферах оборони, правоохоронної діяльності та публічного адміністрування взаємодія міжнародних стандартів і національних підходів до безпеки набуває практичного виміру, оскільки застосування штучного інтелекту потребує узгодження вимог захисту персональних даних із завданнями державної безпеки. Міжнародний досвід засвідчує, що надмірне звуження стандартів захисту даних під приводом безпекових міркувань може призвести до ерозії довіри до державних інститутів і порушення фундаментальних прав людини. Для України, яка знаходиться в умовах підвищених безпекових викликів, інтеграцію міжнародних стандартів слід здійснювати з особливою обережністю та з огляду на принцип пропорційності [101; 125; 135].

Складним є питання практичної імплементації міжнародних стандартів у діяльність суб'єктів приватного права, насамперед технологічних компаній і розробників ШІ. У міжнародній практиці дедалі поширенішим є підхід, за яким дотримання стандартів захисту персональних даних розглядають як елемент корпоративної відповідальності та конкурентної переваги. Для національного правового поля це означає необхідність формування стимулів до добровільного впровадження міжнародних стандартів, зокрема через механізми саморегулювання, сертифікації та публічної звітності. Водночас без належного державного нагляду такі інструменти можуть залишатися суто декларативними і не забезпечувати реального підвищення рівня захисту персональних даних [56; 101].

У цьому зв’язку інтеграція міжнародних і європейських стандартів має супроводжуватися розвитком національної експертизи у сфері штучного інтелекту й захисту персональних даних. Міжнародні документи часто оперують складними техніко-правовими категоріями, коректне застосування яких потребує міждисциплінарних знань. Брак достатньої кількості фахівців, здатних поєднувати правовий аналіз із розумінням технологічних процесів, істотно ускладнює ефективну імплементацію стандартів і підвищує ризик формального підходу до їх застосування [49; 112].

Подальшу інтеграцію міжнародних і європейських стандартів у національне регулювання захисту персональних даних у сфері штучного інтелекту слід розглядати не як одноразовий акт законодавчого запозичення, а як тривалий і багаторівневий процес. Його успішність залежить від здатності національної правової системи забезпечити узгодженість між різними нормативними джерелами, адаптувати міжнародні підходи до національного контексту і створити ефективні механізми їх практичної реалізації. Саме в такому вимірі інтеграція міжнародного досвіду може стати основою для формування сучасної та стійкої моделі захисту персональних даних в Україні в умовах активного розвитку штучного інтелекту [80; 97; 101].

Однією з ключових тенденцій розвитку сучасного правового регулювання у сфері захисту персональних даних є поступовий перехід від формально-нормативної моделі до ризик-орієнтованого підходу, у центрі якого – не факт обробки даних, а потенційні наслідки такої обробки для прав і свобод людини. У контексті використання штучного інтелекту ця тенденція ж вкрай важливою, оскільки алгоритмічні системи здатні породжувати складні, непрямі та кумулятивні ризики, які не можуть бути адекватно оцінені за допомогою традиційних юридичних критеріїв [101; 126]. Ризик-орієнтований підхід ґрунтується на тому, що не всі операції з персональними даними є однаково небезпечними з погляду втручання в приватність, а отже, потребують диференційованого правового реагування. Така логіка поступово

витісняє універсальні вимоги, орієнтовані на формальне дотримання принципів, натомість передбачає оцінку конкретного контексту використання даних, масштабів обробки, характеру застосованих технологій та вразливості суб'єктів даних. У національному законодавстві України зазначений підхід поки що реалізований фрагментарно і не має системного характеру, що відчутно передусім у сфері застосування ШІ [49; 112].

Центральним елементом ризик-орієнтованої моделі у сфері захисту персональних даних є механізм попереднього оцінювання ризиків, спрямований на ідентифікацію можливих негативних наслідків ще до початку обробки. У міжнародній практиці таку оцінку розглядають як обов'язковий інструмент відповідального використання алгоритмічних систем, здатний забезпечити превентивний характер правового захисту. Для національного правопорядку України імплементація таких механізмів означає зміну акцентів із реактивного реагування на порушення до управління ризиками на етапах проєктування, розроблення та впровадження ШІ-систем [101; 112].

Використання штучного інтелекту суттєво ускладнює процес ідентифікації та оцінювання ризиків, оскільки наслідки обробки персональних даних можуть виявлятися не одразу, а з плином часу, а також мати опосередкований характер. Алгоритмічні системи здатні формувати профілі, робити прогностичні висновки та впливати на поведінку осіб у спосіб, який складно передбачити на етапі їх упровадження. Це ставить під сумнів ефективність традиційних правових гарантій і зумовлює необхідність використання міждисциплінарних підходів до оцінювання ризиків, що поєднують правовий аналіз із технічними та соціальними аспектами функціонування ШІ [68; 84; 101].

Увагу в межах ризик-орієнтованого підходу привертає питання автоматизованого прийняття рішень і профілювання. Такі форми обробки персональних даних потенційно здатні призводити до дискримінаційних ефектів, помилкових висновків або непропорційного обмеження прав

людини. Без спеціальних процедур оцінювання ризиків і належного нагляду застосування ШІ в цих сферах може мати системний негативний вплив, який не обмежується окремими випадками порушень. У цьому контексті ризик-орієнтований підхід розглядають як інструмент забезпечення справедливого балансу між інноваційним розвитком і захистом фундаментальних прав [101; 137]. Важливим аспектом формування ризик-орієнтованої моделі є переосмислення ролі згоди суб'єкта персональних даних. У традиційній моделі згоду розглядають як ключовий елемент легітимації обробки, однак у випадку складних ШІ-систем вона часто не здатна забезпечити реальний контроль особи за своїми даними. Ризик-орієнтований підхід зміщує акцент із формального отримання згоди на відповідальність суб'єкта обробки за оцінювання та мінімізацію ризиків, незалежно від того, чи було надано згоду. Така трансформація відповідає сучасним міжнародним тенденціям розвитку права у сфері захисту персональних даних [101].

Формування ризик-орієнтованого підходу в національному праві також передбачає розвиток інституційних механізмів, здатних забезпечити належний рівень контролю за використанням штучного інтелекту. Це передбачає посилення ролі наглядових органів, запровадження спеціалізованих процедур аудиту алгоритмічних систем і створення умов для міжвідомчої координації у сфері цифрового регулювання. Без належного інституційного забезпечення ризик-орієнтована модель може залишатися декларативною і не мати реального впливу на практику обробки персональних даних [49; 112].

Водночас реалізація ризик-орієнтованого підходу постає перед низкою викликів, серед яких важливе місце посідає проблема визначення критеріїв оцінювання ризиків у сфері штучного інтелекту. Брак уніфікованих підходів до класифікації ризиків, а також швидкі темпи технологічних змін ускладнюють розроблення стабільних правових механізмів. Це підвищує значення міжнародного досвіду й стандартів як джерела орієнтирів для

національного законодавця, водночас зберігаючи потребу в адаптації таких підходів до українських реалій [80; 97; 101].

Узагальнюючи, зазначимо, що формування ризик-орієнтованого підходу в національному праві щодо захисту персональних даних у сфері штучного інтелекту слід розглядати як одну з базових тенденцій подальшого розвитку правового регулювання. Такий підхід дає змогу поєднати вимоги інноваційного розвитку з необхідністю забезпечення ефективного захисту прав людини, водночас створюючи підґрунтя для впровадження гнучкіших й адаптивних правових механізмів [126; 101].

Ефективність правового регулювання захисту персональних даних у сфері використання штучного інтелекту безпосередньо залежить не лише від якості нормативних приписів, а й від рівня інституційної спроможності органів, відповідальних за їх реалізацію та контроль. У сучасних умовах саме інституційний вимір дедалі частіше є визначальним фактором, який зумовлює реальний рівень захисту прав суб'єктів персональних даних у цифровому середовищі. Для національної правової системи України ця проблема набуває особливої актуальності з огляду на складність алгоритмічних технологій і трансформацію моделей управління даними [49; 101; 112]. Центральне місце в системі інституційного забезпечення захисту персональних даних посідають наглядові органи, призначені здійснювати контроль за дотриманням законодавства та реагувати на порушення. В умовах поширення ШІ їхня роль суттєво ускладнюється, оскільки традиційні інструменти нагляду, орієнтовані на перевірку формальної відповідності вимогам закону, виявляються недостатніми для оцінювання складних алгоритмічних процесів. Це вимагає від наглядових інституцій не лише правової, а й технічної експертизи, здатності аналізувати архітектуру ШІ-систем, логіку їх функціонування та потенційні ризики для прав людини [126; 101].

Інституційні виклики посилюються фрагментацією компетенцій між різними органами державної влади, які опікуються питаннями захисту

персональних даних, цифрової трансформації, кібербезпеки й інформаційної політики. Брак чітких механізмів координації між цими суб'єктами призводить до розосередженості відповідальності й ускладнює формування єдиної державної політики у сфері використання штучного інтелекту. Дослідники обґрунтовують, що така інституційна роз'єднаність знижує ефективність правозастосування і створює додаткові ризики для суб'єктів персональних даних [49; 112].

Проблему становить також кадрове та ресурсне забезпечення інституцій, відповідальних за реалізацію законодавства про захист персональних даних. Аналіз міжнародного досвіду засвідчує, що ефективний нагляд за використанням ШІ потребує залучення фахівців із міждисциплінарною підготовкою, які поєднують правові знання з розумінням принципів машинного навчання та аналізу даних. Для України дефіцит таких кадрів істотно ускладнює практичну імплементацію сучасних підходів до захисту персональних даних і підвищує ризик формального виконання регуляторних функцій [101].

Організаційний вимір реалізації законодавства у сфері захисту персональних даних під час використання ШІ охоплює також внутрішні механізми управління в організаціях, які розробляють або застосовують алгоритмічні системи. У сучасних умовах відповідальність за дотримання вимог законодавства дедалі частіше покладають не лише на формальних суб'єктів обробки, а й на внутрішні структури корпоративного управління, що забезпечують інтеграцію принципів захисту даних у процеси проєктування та експлуатації ШІ-рішень. Брак у національному праві чітких вимог до таких організаційних механізмів обмежує можливості превентивного захисту прав суб'єктів даних [101; 112].

Важливим аспектом інституційної реалізації законодавства є взаємодія державних органів із приватним сектором і громадянським суспільством. У сфері штучного інтелекту така взаємодія набуває стратегічного значення, оскільки саме приватні компанії часто є основними розробниками та

постачальниками алгоритмічних технологій. Міжнародний досвід демонструє, що без налагодженого діалогу між регуляторами й суб'єктами ринку запровадження жорстких нормативних вимог може призвести до їх формального виконання або спроб оминути. Для України актуальним є пошук балансу між регуляторним впливом держави та створенням умов для відповідального інноваційного розвитку [56; 101]. Важливу роль у забезпеченні ефективності інституційних і організаційних механізмів відіграють інструменти о «м'якого права», які доповнюють законодавче регулювання та сприяють формуванню єдиних стандартів правозастосовної практики. Рекомендації, керівні принципи й методичні матеріали дають змогу адаптувати загальні правові вимоги до конкретних технологічних контекстів і знижують рівень правової невизначеності для суб'єктів, що використовують ШІ. Водночас ефективність таких інструментів залежить від їх сприйняття на практиці та рівня довіри до інституцій, які їх розробляють [56; 101]. Інституційні й організаційні аспекти реалізації законодавства тісно пов'язані з питанням відповідальності за порушення у сфері захисту персональних даних. У контексті використання штучного інтелекту традиційні моделі відповідальності, орієнтовані на чітке визначення винного суб'єкта, постають перед складнощами через ланцюги розроблення та експлуатації ШІ-систем. Це посилює потребу в напрацюванні колективних і розподілених моделей відповідальності, здатних відобразити реальний характер взаємодії учасників алгоритмічних екосистем [101; 126].

Реалізація законодавства про захист персональних даних у сфері використання штучного інтелекту безпосередньо залежить від ефективності інституційних і організаційних механізмів, які забезпечують практичне втілення нормативних вимог. Без належної інституційної інфраструктури навіть найпрогресивніші правові норми залишаються декларативними та не здатні забезпечити реальний захист прав суб'єктів персональних даних. У цьому контексті інституційний вимір набуває самостійного значення, оскільки саме він визначає межі застосовності правових приписів у

складному технологічному середовищі штучного інтелекту [49, с. 14–18; 101; 112]. Ключовим елементом інституційної системи захисту персональних даних є наглядові органи, уповноважені здійснювати контроль за дотриманням законодавства та реагувати на порушення. В умовах поширення ШІ функції таких органів істотно ускладнюються, оскільки перевірка відповідності алгоритмічних систем правовим вимогам виходить за межі традиційного документального контролю. Нагляд у сфері ШІ потребує здатності аналізувати технічну архітектуру систем, оцінювати логіку алгоритмічних рішень і прогнозувати потенційні ризики для прав людини, що об’єктивно вимагає розширення компетенцій і ресурсів відповідних інституцій [101; 126].

Інституційні проблеми реалізації законодавства посилюються фрагментацією повноважень між різними органами державної влади. Питання захисту персональних даних, цифрової трансформації, інформаційної безпеки та регулювання штучного інтелекту часто знаходяться у віданні різних інституцій, що ускладнює формування узгодженої державної політики. За браку ефективних механізмів міжвідомчої координації виникає ризик дублювання функцій або, навпаки, прогалин у правозастосуванні, що негативно позначається на рівні захисту персональних даних у практиці використання ШІ [49, с. 3–9; 112].

Увагу слід спрямувати на кадрове й експертне забезпечення інституцій, відповідальних за реалізацію законодавства у сфері захисту персональних даних. Сучасні ШІ-системи вирізняються високим рівнем технічної складності, що зумовлює потребу в міждисциплінарній експертизі. Брак достатньої кількості фахівців, що мають правові знання та розуміють принципи машинного навчання, аналізу даних, істотно обмежує спроможність державних органів здійснювати ефективні нагляд і контроль. Унаслідок цього правозастосування ризикує обмежитися формальним аналізом, не охоплюючи реальних алгоритмічних ризиків [101]. Організаційні аспекти реалізації законодавства виявляються також на рівні

суб’єктів, які безпосередньо розробляють або використовують ШІ-системи. У сучасних умовах забезпечення дотримання вимог щодо захисту персональних даних дедалі істотнішими стають внутрішні механізми корпоративного управління, комплаєнсу й управління ризиками. Інтеграцію принципів захисту даних у процеси проєктування, розроблення та експлуатації ШІ-рішень розглядають як ключову умову превентивного захисту прав суб’єктів даних. Водночас національне законодавство України поки що не встановлює чітких вимог до таких внутрішніх організаційних структур, що обмежує потенціал їх практичного застосування [101; 112].

З огляду на те, що значна частина інновацій у сфері штучного інтелекту формується поза державним сектором, взаємодія публічних інституцій і приватних суб’єктів набуває практичного виміру. Міжнародний досвід демонструє, що ефективне регулювання ШІ неможливе без конструктивного діалогу між регуляторами й технологічними компаніями. Для України це означає необхідність формування таких моделей взаємодії, які поєднували б обов’язковість правових вимог із стимулюванням відповідальної інноваційної діяльності. Без цього балансу зростає ризик або надмірного регуляторного тиску, або формального дотримання норм без реального впливу на практику [56; 101]. Значну роль у забезпеченні інституційної ефективності відіграють інструменти «м’якого права», зокрема рекомендації, методичні настанови та стандарти правозастосовної практики. Вони дають змогу конкретизувати загальні вимоги законодавства з огляду на технологічні особливості ШІ-систем і сприяють уніфікуванню підходів до оцінювання ризиків. Водночас ефективність таких інструментів безпосередньо залежить від рівня довіри до інституцій, які їх розробляють, а також від готовності суб’єктів ринку сприймати їх як обов’язкові орієнтири поведінки [56; 101].

Аналізу потребує питання відповідальності у сфері захисту персональних даних під час використання штучного інтелекту. Складність ланцюгів створення та експлуатації ШІ-систем ускладнює застосування

традиційних моделей юридичної відповідальності, орієнтованих на індивідуалізацію вини. Це зумовлює необхідність переосмислення підходів до відповідальності та розроблення колективних або розподілених моделей, які відображали б реальний характер взаємодії учасників алгоритмічних екосистем [101; 126].

Узагальнюючи, зауважимо, що інституційні й організаційні аспекти реалізації законодавства у сфері захисту персональних даних під час використання штучного інтелекту є критичним елементом ефективності національної моделі правового регулювання. Без належної інституційної спроможності, розвитку експертного потенціалу, координації між органами влади та впровадження внутрішніх організаційних механізмів у приватному секторі правове регулювання може залишатися формальним. Саме тому вдосконалення інституційних й організаційних засад слід розглядати як необхідну умову подальшого розвитку законодавства України у сфері захисту персональних даних в умовах активного впровадження технологій штучного інтелекту [49; 101; 112].

Сукупний аналіз сучасного стану національного законодавства України у сфері захисту персональних даних, а також впливу технологій штучного інтелекту на правове регулювання дає змогу виокремити низку стійких тенденцій, які визначають вектор подальшої еволюції відповідної нормативної моделі. Ці тенденції не зводяться до окремих законодавчих змін або інституційних реформ, а відображають глибшу трансформацію підходів до правового регулювання в умовах алгоритмічної обробки даних і цифрової автоматизації суспільних процесів. Саме в цьому сенсі аналіз тенденцій набуває особливого значення як інструмент прогнозування напрямів удосконалення правового регулювання [101; 126].

З-поміж визначальних тенденцій виокремимо такі:

1. Першою ключовою тенденцією є поступовий відхід від універсальної, технологічно нейтральної моделі регулювання захисту персональних даних на користь диференційованого підходу, орієнтованого

на специфіку конкретних технологій. Якщо традиційно національне законодавство ґрунтувалося на припущенні про можливість застосування єдиних правових принципів до всіх форм обробки даних, то розвиток ШІ продемонстрував обмеженість такого підходу. Алгоритмічні системи створюють ризики, які не можуть бути адекватно врегульовані виключно за допомогою загальних норм, що зумовлює необхідність спеціалізації правового регулювання з огляду на рівень автономності, масштабності й потенційного впливу ШІ на права людини [49; 101; 112].

2. Другою важливою тенденцією є посилення значення ризик-орієнтованого підходу як методологічної основи правового регулювання. Національне законодавство дедалі активніше орієнтується не на формальні критерії правомірності обробки, а на оцінку фактичних і потенційних ризиків для прав і свобод суб'єктів персональних даних. У сфері штучного інтелекту такий підхід дає змогу враховувати складний, багатовимірний характер алгоритмічних впливів, а також їх можливі кумулятивні наслідки. Водночас несформованість усталених національних критеріїв оцінювання ризиків зумовлює залежність правового розвитку від міжнародних стандартів і практик [101; 126].

3. Третьою тенденцією є трансформація ролі суб'єкта персональних даних у системі правового регулювання. У традиційній моделі суб'єкт даних розглядали як активного учасника інформаційних відносин, здатного здійснювати контроль за обробкою своїх даних шляхом надання або відкликання згоди. В умовах використання складних ШІ-систем така модель втрачає свою ефективність, оскільки інформаційна і технологічна асиметрія між суб'єктом даних та суб'єктом обробки істотно обмежує можливості усвідомленого вибору. Це зміщує акцент з індивідуального контролю на інституційні й організаційні гарантії захисту персональних даних [101].

4. Четверта тенденція пов'язана з переосмисленням принципу прозорості як одного з базових елементів захисту персональних даних. У національному праві прозорість традиційно асоціювали з обов'язком

інформування суб’єктів даних про обробку їхньої інформації. Проте в контексті ШІ-систем, внутрішні механізми яких часто є непрозорими навіть для їх розробників, така інтерпретація виявляється недостатньою. Це стимулює розвиток нових підходів до прозорості, орієнтованих не лише на розкриття інформації, а й на забезпечення підзвітності, пояснюваності та можливості зовнішнього контролю за алгоритмічними процесами [101; 126; 137].

5. П’ятою тенденцією є поступове посилення ролі інституційного та міжвідомчого регулювання у сфері захисту персональних даних. Підвищення складності цифрових екосистем зумовлює необхідність координації дій між органами, відповідальними за захист персональних даних, цифрову трансформацію, інформаційну безпеку й інші суміжні сфери. У національному контексті це виявляється в прагненні сформувати узгоджену модель державної політики у сфері ШІ, здатну забезпечити баланс між інноваційним розвитком і захистом прав людини [49; 112].

6. Шостою тенденцією слід визнати зростання значення міжнародного та європейського досвіду як джерела орієнтирів для національного правового розвитку. Без власної усталеної практики регулювання ШІ Україна керується міжнародними стандартами, рекомендаціями та рамковими документами, які формують загальні підходи до захисту персональних даних у цифрову епоху. Така орієнтація сприяє гармонізації національного законодавства з європейськими моделями, водночас зберігаючи ризик формальної імплементації без належного врахування національних особливостей [80; 97; 101].

7. Сьома тенденція стосується поступового переходу від реактивної моделі правового захисту до превентивної. У традиційній парадигмі правове регулювання зосереджувалося на реагуванні на порушення, які вже відбулися, натомість сучасні підходи орієнтуються переважно на запобігання ризикам на ранніх етапах упровадження технологій. У сфері штучного інтелекту це означає посилення ролі попередньої оцінки впливу, внутрішніх

процедур управління ризиками й відповідальності розробників і користувачів ШІ за потенційні наслідки обробки персональних даних [101; 112].

8. Восьмою тенденцією є посилення значення міждисциплінарного підходу до правового регулювання захисту персональних даних. Складність алгоритмічних систем об'єктивно потребує поєднання правового аналізу з технічними, етичними та соціальними аспектами використання ШІ. Для національного законодавства України це означає необхідність розвитку нових форм експертної взаємодії та залучення фахівців різних галузей до процесу формування та реалізації правової політики у сфері ШІ [101].

9. Дев'ятою тенденцією є поступове усвідомлення обмеженості виключно правових засобів регулювання у сфері штучного інтелекту. Посилення ролі технічних стандартів, організаційних механізмів й інструментів «м'якого права» засвідчує формування гібридної моделі регулювання, у межах якої право взаємодіє з технологіями та саморегулюванням.

Така модель надає можливість забезпечити гнучкість правового впливу, водночас потребує чітких інституційних гарантій для запобігання зловживанням [56; 101].

Ця модель поєднує спеціалізацію норм, ризик-орієнтований підхід, посилення інституційної ролі держави й активне використання міжнародного досвіду. Саме в такому напрямі закладають підвалини для подальшого вдосконалення правового регулювання захисту персональних даних в Україні, що логічно зумовлює необхідність переходу до аналізу конкретних правових механізмів й інструментів їх реалізації [126; 101]. Також забезпечено логічну зміну аналітичного фокуса від загальних закономірностей розвитку правового регулювання до його прикладного виміру. Подальший розгляд конкретних правових механізмів дасть змогу оцінити, наскільки задекларовані тенденції знаходять реальне втілення в нормах, процедурах і практиках застосування, а також виявити наявні прогалини між нормативними моделями й фактичними інструментами їх

реалізації. Це створює підґрунтя для обґрунтованих висновків щодо ефективності національної системи захисту персональних даних у контексті використання технологій штучного інтелекту та перспектив її подальшого розвитку.

3.2. Проблеми національного законодавства щодо захисту персональних даних у сфері штучного інтелекту та шляхи їх подолання

Попри позитивні зрушення, українська нормативна база досі має низку прогалин і проблем у контексті захисту даних під час використання ШІ. Однією з ключових проблем національного законодавства щодо захисту персональних даних у сфері використання штучного інтелекту є його нормативна фрагментарність і брак спеціалізованого регулювання, здатного врахувати особливості алгоритмічної обробки інформації [110]. Чинна модель правового захисту персональних даних в Україні формувалася в умовах домінування традиційних інформаційних технологій і ґрунтується на припущенні про відносну передбачуваність процесів обробки даних, чітке розмежування ролей суб’єктів та лінійний характер інформаційних потоків. Застосування ШІ суттєво підважує ці припущення, що призводить до виникнення системних прогалин у правовому регулюванні [112].

Нормативна фрагментарність виявляється, зокрема, у відсутності єдиного підходу до правового визначення алгоритмічної обробки персональних даних. Законодавство оперує загальними категоріями «обробка», «використання» та «поширення» персональних даних, не розмежовуючи принципово різні за своєю природою технологічні процеси, такі як машинне навчання, профілювання, генерація нових даних або автономне прийняття рішень. Унаслідок цього правозастосування постає перед складнощами під час кваліфікації дій суб’єктів, що використовують ШІ-системи, а також для визначення меж допустимого втручання в

приватність [57]. Навіть звичні технології масового спостереження та розпізнавання обличчя на основі ШІ суттєво змінюють баланс між публічною безпекою та правами людини, оскільки вони дають змогу здійснювати приховану ідентифікацію осіб у публічних місцях без їх відома та згоди. Використання цих технологій має підвищений рівень ризику через незворотність таких даних і неможливість їх «заміни» в разі витоку, а в Україні наразі немає чітких правил щодо підстав застосування таких технологій, меж збору та зберігання даних, процедур судового контролю та незалежного нагляду [24, с. 317–321].

Відсутність спеціалізованого правового режиму для використання штучного інтелекту у сфері обробки персональних даних призводить до того, що загальні норми застосовують без урахування технологічної специфіки алгоритмічних систем. Такі норми формально залишаються чинними, однак їх практична ефективність істотно знижується, оскільки вони не охоплюють складні, багаторівневі й динамічні процеси обробки даних, притаманні сучасним ШІ-рішенням. Це передусім помітно у випадках, коли персональні дані використовують не для безпосереднього надання послуги, а для навчання моделей або формування статистичних залежностей. Проблемність фрагментарного підходу посилюється тим, що норми, які опосередковано стосуються використання штучного інтелекту, розміщені в різних нормативних актах і не утворюють внутрішньо узгодженої системи. Законодавство про захист персональних даних, інформаційну безпеку, електронні комунікації та цифрову трансформацію розвивається паралельно, без належної координації термінології та регуляторних підходів. За таких умов суб’єкти обробки даних отримують значний простір для довільного тлумачення правових вимог, що негативно впливає на рівень правової визначеності й передбачуваності.

Нормативна фрагментарність також ускладнює визначення обсягу обов’язків суб’єктів, які розробляють або використовують ШІ-системи. Загальні вимоги щодо забезпечення безпеки персональних даних і

дотримання принципів їх обробки не конкретизують, як ці обов’язки слід виконувати в умовах автономності алгоритмів, їх здатності до самонавчання та використання великих масивів даних. Унаслідок цього правове регулювання фактично відстає від технологічних реалій і не забезпечує належного рівня захисту персональних даних.

Отже, нормативна фрагментарність і відсутність спеціалізованого правового регулювання використання штучного інтелекту у сфері обробки персональних даних формують лише поверхневий вияв значно глибшої проблеми – структурної невідповідності чинної моделі правового регулювання реальним механізмам функціонування алгоритмічних систем. Ця невідповідність не зводиться до окремих прогалин або неточностей законодавчої техніки, а має системний характер і виявляється на концептуальному, інституційному та функціональному рівнях.

У національному праві бракує чітких критеріїв, які надавали б можливість відмежувати використання штучного інтелекту як допоміжного інструменту від випадків, коли алгоритмічні системи фактично виконують функцію прийняття рішень, що мають юридично значущі наслідки для суб’єктів персональних даних. За відсутності таких критеріїв правове регулювання не здатне адекватно реагувати на ситуації, у яких автоматизовані рішення впливають на реалізацію прав і свобод особи, зокрема у сфері доступу до послуг, працевлаштування чи соціального забезпечення. Така фрагментарність законодавства обумовлена збереженням класичної уявної моделі обробки персональних даних як контрольованого, локалізованого та цілеспрямованого процесу. У межах цієї моделі суб’єкта обробки сприймають як такого, що цілком усвідомлює обсяг, мету й наслідки обробки, натомість суб’єкт персональних даних формально зберігає можливість здійснювати індивідуальний контроль за своїми даними. Алгоритмічні системи штучного інтелекту, передусім ті, що ґрунтуються на машинному навчанні, порушують цю модель, оскільки процеси обробки набувають імовірнісного, розподіленого й частково непрозорого характеру

[111; 114; 128]. Чинне законодавство не містить інструментів, здатних адекватно описати та врегулювати такі процеси, що призводить до концептуального розриву між нормою та практикою.

Функціональний вимір нормативної фрагментарності виявляється у неспроможності загальних правових приписів охопити всі етапи життєвого циклу штучного інтелекту. Законодавство фактично фокусується на моменті використання персональних даних, залишаючи поза належною правовою увагою етапи їх збирання для навчання моделей, повторного використання, донавчання, тестування та подальшої адаптації алгоритмів. Унаслідок цього виникає ситуація, за якої значна частина обробки персональних даних відбувається в «сірих зонах» правового регулювання, де формально застосовують загальні норми, але немає спеціалізованих вимог, співмірних рівню потенційного втручання в приватність [71].

Нормативна фрагментарність також ускладнює застосування базових принципів захисту персональних даних у контексті використання штучного інтелекту. Принципи законності, мінімізації даних, обмеження мети та пропорційності залишаються декларативно закріпленими, однак їх практичне наповнення у випадку алгоритмічної обробки не має чітких орієнтирів. Зокрема, брак спеціалізованих норм не дає змоги однозначно визначити, як принцип мінімізації може бути реалізовано в системах, що функціонують на основі великих масивів даних, або як слід оцінювати відповідність між початковою метою збирання даних і подальшими, часто не передбачуваними способами їх використання в процесі навчання моделей. Увагу привертає проблема правової невизначеності щодо результатів алгоритмічної обробки персональних даних. Чинне законодавство переважно керується тим, що об’єктом правового захисту є первинні персональні дані, натомість похідні результати їх обробки, профілі, прогнозні висновки, оцінки ризиків залишаються на периферії правового регулювання. У контексті використання штучного інтелекту саме ці результати набувають вирішального значення для прийняття рішень, що впливають на правове становище особи. Відсутність

чіткої регламентації їхнього правового статусу є прямим наслідком фрагментарного підходу законодавця [82; 129].

Системний характер проблеми нормативної фрагментарності засвідчують також складнощі правозастосування [88]. Суди, наглядові органи й інші суб'єкти правозастосовної діяльності змушені інтерпретувати загальні норми в умовах браку спеціалізованих критеріїв, що призводить до неоднорідності практики та підвищення рівня правової невизначеності. За таких умов однакові за своєю технологічною сутністю ситуації можуть отримувати різну правову оцінку залежно від суб'єктивного тлумачення, що підриває принцип правової визначеності як складову верховенства права [55].

Це все також посилюється відсутністю чіткої ієрархії та взаємозв'язку між нормами, які регулюють захист персональних даних і суміжні сфери цифрових відносин. Законодавство про інформаційну безпеку, електронні комунікації, цифрові послуги й електронне урядування містить положення, що опосередковано стосуються використання алгоритмічних систем, однак ці положення не інтегровані в єдину регуляторну логіку. Унаслідок цього виникає багаторівнева фрагментація, яка охоплює не лише законодавство про персональні дані, а й систему цифрового права загалом.

З огляду на викладене, нормативна фрагментарність і брак спеціалізованого правового регулювання використання штучного інтелекту у сфері обробки персональних даних слід розглядати як базову, системоутворювальну проблему національного законодавства. Вона не може бути усунута шляхом точкових змін або ізольованого доповнення окремих норм, оскільки має глибоке коріння в логіці чинної правової моделі. На відміну від проблеми нормативної фрагментарності, що має переважно структурний характер, правова невизначеність алгоритмічної обробки персональних даних виявляється безпосередньо на рівні взаємодії між технологією та правом. Вона виникає не стільки через брак окремих норм, скільки через неспроможність чинних правових конструкцій адекватно описати і врегулювати процеси, у межах яких рішення щодо особи

формуються на основі складних алгоритмічних моделей. У такій ситуації право втрачає здатність виконувати свою базову функцію – забезпечувати передбачуваність і контрольованість втручання у сферу приватності [112].

Алгоритмічна обробка персональних даних у сучасних системах штучного інтелекту не зводиться до простого автоматизованого виконання наперед заданих інструкцій. Вона передбачає побудову моделей, що самостійно виявляють закономірності, формують прогностичні висновки й адаптуються до нових даних. Водночас чинне законодавство не містить критеріїв, які дали б змогу відмежувати використання алгоритмів як технічного засобу обробки інформації від ситуацій, у яких алгоритмічна система фактично здійснює інтелектуальне оцінювання та формує результат, що має значення для правового становища особи. Така невизначеність створює умови, за яких алгоритмічна обробка формально підпадає під дію загальних правил, не активуючи спеціальних гарантій захисту персональних даних [110].

Проблематичною також є сфера автоматизованого прийняття рішень. У практиці використання штучного інтелекту дедалі частіше застосовують моделі, результати яких безпосередньо впливають на доступ особи до послуг, ресурсів або можливостей. Без чітких правових орієнтирів автоматизовані рішення нерідко маскують під рішення, прийняті «за участю людини», хоча фактичний вплив людини на їх зміст є мінімальним або суто формальним. Чинне законодавство не забезпечує інструментів для виявлення таких ситуацій, що призводить до ерозії процесуальних гарантій захисту прав суб’єктів персональних даних [82].

Правова невизначеність алгоритмічної обробки тісно пов’язана з проблемою непрозорості функціонування штучного інтелекту. Низка сучасних моделей машинного навчання не дають змоги відтворити логіку прийняття конкретного рішення в зрозумілій для людини формі. За браку чітко закріплених правових вимог щодо пояснюваності алгоритмічних рішень суб’єкти персональних даних фактично позбавлені можливості

оцінити правомірність втручання у свою приватну сферу або ефективно реалізувати право на оскарження [57]. Прикладом є розпізнавання ходи, що слугує одним із сучасних методів ідентифікації. На відміну від класичних методів біометрії, таких як відбитки пальців чи розпізнавання обличчя, аналіз ходи можуть здійснювати дистанційно, непомітно для людини, а також у складних умовах відеоспостереження. Це суттєво підвищує потенціал масового збору біометричних даних, посилює ризики прихованого моніторингу, а також становить етичну загрозу, високу імовірність помилкових ідентифікацій, дискримінаційних наслідків у разі використання систем у правоохоронній сфері, проблем доведення законності отримання таких даних, а також складнощів реалізації права особи на доступ, виправлення та видалення інформації. Наше середовище не враховує специфіку цього виду біометричних даних і не містить достатніх гарантій проти неправомірного використання технологій [26].

Окремим аспектом цієї проблеми є невизначеність правового статусу результатів алгоритмічної обробки персональних даних. Чинна модель захисту персональних даних зосереджена переважно на первинній інформації, яку безпосередньо ідентифікує особу. Водночас у системах штучного інтелекту ключову роль відіграють похідні результати обробки – профілі, індекси, прогнозні оцінки, категорії ризику, які формуються на основі персональних даних, але не завжди прямо визнані такими.

Брак чіткої правової кваліфікації цих результатів призводить до того, що вони випадають з-під дії механізмів захисту, попри їх безпосередній вплив на правове становище особи [82; 129]. Правова невизначеність посилюється також технічними обмеженнями контролю за алгоритмічною обробкою персональних даних. Загальні вимоги щодо забезпечення безпеки інформації та захисту приватності не конкретизують, як вони мають реалізовуватися у випадку складних самонавчальних систем, що постійно змінюють свої параметри. За відсутності нормативного зв’язку між технічними стандартами та юридичними обов’язками суб’єктів обробки

даних забезпечення прозорості й підзвітності алгоритмів залишається декларативним [71]. Тож правова невизначеність алгоритмічної обробки персональних даних й автоматизованого прийняття рішень підриває принцип правової визначеності як складову верховенства права. Однакові за технологічною природою алгоритмічні процеси можуть отримувати різну правову оцінку залежно від контексту або інтерпретації, що знижує передбачуваність правового регулювання та рівень довіри до механізмів захисту персональних даних у цифровому середовищі [55]. Така ситуація засвідчує глибоку розбіжність між реальними практиками використання штучного інтелекту та чинними правовими інструментами їх регулювання, що зумовлює необхідність подальшого аналізу інших проблемних аспектів у межах цього розділу.

Водночас правова невизначеність алгоритмічної обробки персональних даних не зводиться виключно до проблеми автоматизованих рішень у вузькому сенсі. Вона охоплює ширший спектр правовідносин, у яких алгоритмічні системи опосередковано впливають на формування управлінських, комерційних або соціально значущих рішень, хоча їх формально не визнають суб’єкти правового регулювання. У таких випадках використання штучного інтелекту залишається «вбудованим» в організаційні процеси, що ускладнює ідентифікацію моменту виникнення юридично значущих наслідків для суб’єкта персональних даних. Додаткову складність становить відсутність у національному законодавстві чіткого розмежування між різними рівнями алгоритмічної автономності. Чинні норми не враховують, що ступінь впливу алгоритмічної системи на кінцевий результат може суттєво варіюватися – від допоміжного аналітичного інструмента до фактичного детермінанта рішення. Без такої диференціації однакові правові вимоги формально застосовують до принципово різних за ризиковим профілем технологічних рішень, що знижує ефективність правового захисту персональних даних [110; 112].

Рішення, сформовані на основі штучного інтелекту, нерідко мають кумулятивний характер і впливають на правове становище особи не одномоментно, а через послідовне накопичення оцінок, рейтингів або профілів. Чинне законодавство орієнтоване переважно на фіксацію окремих актів обробки персональних даних і не враховує довгострокові наслідки алгоритмічної оцінки, що додатково ускладнює реалізацію права на захист й ефективне оскарження [55; 57]. Правова невизначеність також виявляється у браку процесуальних механізмів, адаптованих до специфіки алгоритмічних систем. Традиційні інструменти доказування та контролю не завжди дають змогу встановити причиново-наслідковий зв'язок між використанням персональних даних і негативними наслідками для особи у випадку складних моделей машинного навчання. Унаслідок цього навіть за наявності формального порушення прав суб'єкта персональних даних можливість ефективного захисту таких прав залишається обмеженою [82; 129].

Отже, правова невизначеність алгоритмічної обробки персональних даних й автоматизованого прийняття рішень у національному законодавстві виходить за межі окремих дефініційних або технічних проблем. Вона формує багатовимірну зону правової невизначеності, у якій поєднуються концептуальні, функціональні та процесуальні прогалини, що в сукупності істотно знижують рівень захисту персональних даних у сфері застосування штучного інтелекту.

Національне правове регулювання захисту персональних даних у сфері застосування штучного інтелекту пов'язане не стільки зі змістом нормативних приписів, скільки з інституційними й наглядовими можливостями їх реалізації. Навіть за наявності формально чинних норм ефективність захисту персональних даних залежить від спроможності державних органів здійснювати контроль за алгоритмічною обробкою інформації, виявляти порушення та реагувати на них у спосіб, співмірний складності сучасних технологічних рішень [62; 89]. У цьому контексті ключовими стають питання організаційної компетентності, процесуальних

інструментів, експертних ресурсів і здатності до міжвідомчої координації, без яких формальні гарантії приватності втрачають практичну результативність [87].

Інституційна проблематика у сфері захисту персональних даних в умовах використання штучного інтелекту виявляється насамперед у розриві між традиційними моделями наглядової діяльності та фактичними характеристиками алгоритмічних систем. Механізми контролю, сформовані для перевірки лінійних і порівняно прозорих процесів обробки даних, виявляються недостатньо ефективними щодо систем, які функціонують на основі самонавчальних моделей, використовують розподілені обчислювальні інфраструктури та постійно змінюють параметри своєї роботи [57; 88]. У таких умовах наглядова діяльність набуває переважно формального характеру: акцент зміщується на перевірку документації та процедур, натомість фактичні ризики можуть приховуватися у внутрішній логіці моделі або в непрозорих ланцюгах передавання даних між постачальниками та користувачами ШІ-рішень [59; 85]. Складність алгоритмічних систем зумовлює також обмеженість експертних можливостей органів, уповноважених здійснювати нагляд у сфері захисту персональних даних. Чинна інституційна модель керується припущенням, що контролюючий орган здатен оцінити правомірність обробки персональних даних на підставі поданої документації або пояснень суб’єкта обробки. У випадку використання штучного інтелекту така оцінка потребує міждисциплінарної експертизи, яка поєднує правові, технічні й організаційні знання, а також розуміння ризикових сценаріїв для прав і свобод суб’єктів персональних даних [61; 106]. Брак достатнього інституційного ресурсу для проведення такої експертизи істотно знижує ефективність нагляду і створює асиметрію між суб’єктом регулювання (державним органом) і суб’єктом, який володіє технічними знаннями й інструментарієм (розробником або оператором системи) [55].

Окрему проблему становить відсутність процедурних інструментів, адаптованих до специфіки використання штучного інтелекту. Традиційні форми перевірок, приписів та санкцій не враховують того, що наслідки алгоритмічної обробки персональних даних можуть виявлятися не одразу, а мати відкладений або кумулятивний характер, а також бути розподіленими між кількома елементами ланцюга постачання (розробник моделі, інтегратор, оператор, постачальник даних) [59; 88]. За таких умов реагування на порушення часто відбувається вже після того, як негативні наслідки для суб'єктів персональних даних стали незворотними, а відновлення порушених прав ускладнюється доказовими бар'єрами й технічною складністю відтворення причиново-наслідкового зв'язку [85; 106].

Інституційна слабкість наглядових механізмів ускладнює також реалізацію превентивних форм захисту персональних даних. У контексті використання штучного інтелекту важливе значення має здатність державних органів виявляти потенційні ризики ще до масового впровадження алгоритмічних систем, оскільки масштабованість цифрових сервісів може призводити до швидкого та широкого поширення негативних ефектів [88; 89]. Проте чинна модель нагляду часто орієнтована переважно на реагування на вже вчинені порушення і не завжди передбачає достатньо процедур для раннього виявлення системних ризиків, передусім коли обробку персональних даних здійснюють у транснаціональних інфраструктурах або через хмарні сервіси [55; 114].

Важливим інституційним фактором є також співвідношення наглядових повноважень у сфері захисту персональних даних із суміжними режимами регулювання цифрового простору. У правопорядках, орієнтованих на європейську модель, контроль алгоритмічної обробки персональних даних перетинається з вимогами щодо цифрових послуг, прозорості платформ й управління даними, що формує складні міжрежимні взаємозв'язки [122; 123]. В українському контексті інституційні обмеження посилюються тим, що відповідні напрями державної політики розвиваються нерівномірно, а

наглядові повноваження можуть бути розподілені між органами з різними пріоритетами та рівнем технічної спроможності [40, с. 106–112; 76]. Зрештою інституційні та наглядові обмеження формують самостійний проблемний пласт у сфері захисту персональних даних в умовах використання штучного інтелекту. Вони посилюють нормативні та концептуальні прогалини правового регулювання і призводять до ситуації, у якій формальна наявність правових гарантій не супроводжується їх ефективною реалізацією [61; 89]. Це демонструє, що проблематику захисту персональних даних у сфері штучного інтелекту в Україні слід розглядати не лише як питання якості норм, а й як питання реальної інституційної спроможності забезпечити контроль, підзвітність й ефективний нагляд у цифровому середовищі [41, с. 132–142; 55].

Водночас інституційні обмеження не стосуються виключно дефіциту ресурсів або експертних знань. Вони також виявляються у невизначеності функціональної ролі наглядових органів у процесах, пов’язаних із впровадженням й експлуатацією систем штучного інтелекту. Чинна модель державного нагляду здебільшого орієнтована на постфактум-контроль, натомість алгоритмічні системи потребують безперервного моніторингу, здатного враховувати змінювану поведінку моделей у часі [57; 88]. Без такого моніторингу наглядові органи опиняються в позиції реактивних суб’єктів, що знижує превентивний потенціал правового регулювання.

Складність становить і транснаціональний характер значної частини алгоритмічних систем, які використовують для обробки персональних даних. Дані можуть зберігати й обробляти в хмарних інфраструктурах за межами національної юрисдикції, а ключові елементи системи – модель, дата-сети, програмні бібліотеки – знаходитися під контролем іноземних суб’єктів. У таких умовах можливості національних наглядових органів істотно обмежуються, а ефективний контроль залежить від рівня міжнародної координації та взаємного визнання регуляторних підходів [122; 123]. Інституційні обмеження виявляються також у складності застосування

санкційних механізмів у сфері алгоритмічної обробки персональних даних. Традиційні підходи до притягнення до відповідальності передбачають чітку ідентифікацію суб'єкта порушення та причиново-наслідкового зв'язку між його діями й негативними наслідками. У випадку використання штучного інтелекту відповідальність може бути розподіленою між кількома учасниками технологічного ланцюга, що ускладнює інституційне реагування та знижує стримувальний ефект правових санкцій [59; 88].

Додатковим чинником є обмеженість процедур доступу наглядових органів до інформації, необхідної для перевірки алгоритмічних систем. Навіть за наявності формальних повноважень отримання технічної інформації про функціонування моделей може наштовхуватися на комерційну таємницю, інтелектуальну власність або договірні обмеження. Без спеціалізованих процедур балансування між захистом конфіденційної інформації та публічним інтересом у забезпеченні прав людини інституційний контроль залишається фрагментарним і вибірковим [55; 85; 106]. Тож інституційні та наглядові обмеження у сфері використання штучного інтелекту формують кумулятивний ефект, який підриває дієвість механізмів захисту персональних даних. Вони взаємодіють із нормативними прогалинами та правовою невизначеністю алгоритмічної обробки, створюючи середовище, у якому ризики для приватності накопичуються швидше, ніж можливості їх правового стримування. Така ситуація виявляє глибоку залежність ефективності правового захисту персональних даних від інституційної архітектури та реальної спроможності держави здійснювати нагляд за складними цифровими процесами [55; 87; 89].

Використання штучного інтелекту в процесах обробки персональних даних актуалізує проблему ефективності засобів правового захисту, якими можуть скористатися суб'єкти персональних даних у разі порушення їхніх прав. Чинна модель захисту прав у цій сфері ґрунтується на припущенні про можливість ідентифікувати суб'єкта обробки, встановити факт порушення та довести причиново-наслідковий зв'язок між обробкою персональних даних і

негативними наслідками для особи. У контексті застосування алгоритмічних систем ці припущення виявляються нереалістичними, що зумовлює істотне звуження практичної доступності правових засобів захисту [55; 82]. Одним із ключових чинників обмеженості правового захисту є інформаційна асиметрія між суб'єктом персональних даних і суб'єктом, який використовує штучний інтелект. Суб'єкти персональних даних здебільшого не володіють інформацією про факт використання алгоритмічних систем, їхню роль у прийнятті рішень й обсяг персональних даних, залучених до обробки. В умовах, коли не забезпечено прозорість алгоритмічних процесів, особа не здатна ні своєчасно виявити порушення, ні сформулювати обґрунтовану правову позицію для захисту своїх прав [57]. Обмеженість засобів правового захисту виявляється також у складності реалізації права на доступ до персональних даних й інформації про їх обробку. Традиційні механізми доступу орієнтовані на надання формальної інформації про наявність і зміст персональних даних, однак у випадку використання штучного інтелекту ключове значення має розуміння логіки обробки, ролі алгоритмічних моделей і впливу похідних результатів на правове становище особи. Чинне законодавство не завжди забезпечує можливість отримання такої інформації у формі, придатній для ефективного захисту прав [57; 82].

Суттєвою перешкодою для реалізації засобів правового захисту є проблема доказування. У справах, пов'язаних з алгоритмічною обробкою персональних даних, суб'єкт персональних даних постає перед необхідністю довести не лише факт обробки, а й те, що саме ця обробка призвела до конкретних негативних наслідків. У випадку складних моделей машинного навчання встановлення такого причиново-наслідкового зв'язку може бути технічно неможливим або потребувати спеціальних знань, які виходять за межі доступних для пересічної особи ресурсів [84; 129].

Обмеженість засобів правового захисту посилюється також фрагментацією відповідальності між різними учасниками алгоритмічного ланцюга. Розробники моделей, постачальники даних, інтегратори та кінцеві

користувачі систем штучного інтелекту можуть перебувати в різних правових режимах і юрисдикціях. За таких умов визначення належного відповідача й обсягу його відповідальності стає складним завданням, що додатково знижує ефективність судового та позасудового захисту [86]. Проблему становить обмеженість процесуальних механізмів колективного захисту прав суб'єктів персональних даних. Алгоритмічна обробка переважно має масовий характер й однотипно впливає на значну кількість осіб, однак індивідуалізовані засоби захисту не завжди дають змогу адекватно реагувати на такі порушення. Без ефективних механізмів колективного захисту або представницьких позовів системні порушення можуть залишатися поза належною правовою оцінкою [62; 89].

Обмеженість правового захисту виявляється також у складності отримання відшкодування шкоди, завданої внаслідок алгоритмічної обробки персональних даних. Нематеріальний характер порушень приватності, а також кумулятивний ефект алгоритмічних рішень ускладнюють оцінку шкоди та її компенсацію в межах традиційних правових конструкцій. Унаслідок цього навіть встановлення факту порушення не завжди приводить до ефективного відновлення порушених прав [55]. Тож обмеженість засобів правового захисту суб'єктів персональних даних в умовах використання штучного інтелекту формує ще один системний елемент проблематики правового регулювання в цій сфері. Вона взаємодіє з нормативною фрагментарністю, правовою невизначеністю алгоритмічної обробки й інституційними обмеженнями нагляду, створюючи ситуацію, у якій формальні гарантії прав суб'єктів персональних даних не трансформуються в реальні можливості їх захисту [55; 82].

Суттєвою проблемою національного правового регулювання захисту персональних даних у сфері використання штучного інтелекту є його неповна узгодженість із міжнародними та європейськими підходами, які формують сучасні стандарти захисту приватності в цифровому середовищі. У той час як міжнародні організації та інституції Європейського Союзу

послідовно розвивають комплексні рамки регулювання, національне законодавство України знаходиться на етапі фрагментарної адаптації, що спричиняє виникнення нормативних колізій та прогалин у практиці правозастосування [87; 89]. Одним із виявів такої неузгодженості є відмінність у підходах до оцінювання ризиків, пов'язаних з алгоритмічною обробкою персональних даних. Міжнародні документи дедалі більше орієнтуються на ризик-орієнтовану модель регулювання, у межах якої інтенсивність правових вимог корелює з потенційним впливом технології на права і свободи людини. Натомість національне регулювання переважно зберігає формальний підхід, що не дає змоги диференціювати обов'язки суб'єктів обробки залежно від характеру й масштабів використання штучного інтелекту [56; 116].

Колізійність виявляється також у різному розумінні ролі й статусу суб'єкта персональних даних. У європейській правовій традиції посилюється акцент на активній участі особи в контролі за алгоритмічною обробкою, зокрема через розширення вимог до прозорості, пояснюваності й підзвітності автоматизованих систем. Водночас національне законодавство України залишається орієнтованим на модель формального інформування, яка не завжди забезпечує реальну можливість особи впливати на процеси обробки персональних даних у середовищі штучного інтелекту [82; 89].

Проблемним постає співвідношення національного регулювання з актами права Європейського Союзу, що мають міжгалузевий характер й опосередковано впливають на захист персональних даних у сфері штучного інтелекту. Регулювання цифрових послуг, управління даними та використання штучного інтелекту в ЄС формується як взаємопов'язана система, у межах якої захист персональних даних інтегрується з іншими режимами цифрового права. В українському правопорядку немає системної інтеграції, що створює ризик вибіркового або фрагментарного запозичення окремих норм без урахування їх місця в загальній регуляторній архітектурі [121–123].

Неузгодженість із міжнародними підходами виявляється також у сфері етичного та принципового регулювання штучного інтелекту. Міжнародні документи дедалі частіше закріплюють принципи людської гідності, справедливості, недискримінації та відповідальності як нормативні орієнтири для використання алгоритмічних систем. Водночас у національному законодавстві ці принципи не завжди отримують чітке правове наповнення та залишаються на рівні декларативних положень, що ускладнює їх практичне застосування у сфері захисту персональних даних [83; 116]. Колізійність регулювання посилюється також різним рівнем деталізації правових вимог. Європейські й міжнародні документи передбачають розвиток спеціалізованих інструментів контролю та оцінювання впливу алгоритмічних систем на права людини, натомість національне законодавство лише частково інтегрує такі механізми і не завжди забезпечує їх узгоджене застосування у сфері штучного інтелекту [89; 106]. Це створює ситуацію, у якій формальне запозичення окремих інститутів не супроводжується становленням цілісної моделі правового регулювання.

Тож колізії та неузгодженість національного регулювання з міжнародними та європейськими підходами формують додатковий рівень складності у сфері захисту персональних даних в умовах використання штучного інтелекту. Вони знижують передбачуваність правового середовища, ускладнюють адаптацію суб’єктів обробки до європейських стандартів і створюють ризики неповної або вибіркової імплементації міжнародних зобов’язань України в цифровій сфері [41; 56; 87].

Однією з найглибинніших проблем правового регулювання захисту персональних даних у сфері застосування штучного інтелекту є стійкий технологічно-правовий розрив між реальними механізмами функціонування алгоритмічних систем й інструментарієм, який пропонує чинне законодавство. Цей розрив не зводиться до відсутності окремих норм або недостатньої деталізації правових приписів, а має системний характер, оскільки право намагається регулювати динамічні, імовірнісні та

багаторівневі технологічні процеси за допомогою конструкцій, сформованих для статичних і передбачуваних моделей обробки інформації [112; 128].

Технологічно-правовий розрив виразно виявляється у сфері повторного використання даних та їх залучення для навчання алгоритмічних моделей. У практиці розроблення штучного інтелекту персональні дані можуть використовувати не лише для надання конкретної послуги, а й для вдосконалення моделей, тестування нових функцій або формування універсальних алгоритмічних рішень. Водночас правові механізми контролю за цими процесами залишаються обмеженими, оскільки чинні норми не завжди дозволяють чітко відмежувати первинну мету обробки від подальших способів використання даних у контексті машинного навчання [71; 110].

Окремий вимір проблеми становить невідповідність між швидкістю технологічних змін і темпами правового реагування. Алгоритмічні системи можуть оновлюватися в режимі реального часу, змінюючи свої параметри, джерела даних і логіку функціонування. Натомість правові інструменти контролю, зокрема оцінка відповідності або перевірка правомірності обробки персональних даних, переважно мають статичний характер і не пристосовані до постійної еволюції технології. Це призводить до ситуації, у якій формально правомірна на момент впровадження система з плином часу може генерувати нові ризики для приватності без належного правового реагування [56; 88].

Технологічно-правовий розрив виявляється також у складності інтеграції технічних стандартів і рекомендацій у правову площину. Міжнародні та галузеві стандарти з управління ризиками, безпеки та приватності пропонують деталізовані підходи до проєктування й експлуатації алгоритмічних систем, однак їх юридичний статус у національному правопорядку залишається обмеженим. Без чітких механізмів трансформації технічних вимог у юридично обов’язкові критерії право втрачає здатність адекватно реагувати на технічні аспекти ризиків, пов’язаних з обробкою персональних даних у системах штучного інтелекту

[71; 110; 113; 128]. Суттєвим аспектом технологічно-правового розриву є також проблема виявлення та запобігання витокам персональних даних у процесі навчання та функціонування моделей. Наукові дослідження демонструють, що сучасні алгоритмічні системи можуть відтворювати або розкривати фрагменти даних, використаних для навчання, навіть без прямого доступу до первинних дата-сетів. Чинне законодавство, орієнтоване на традиційні уявлення про зберігання та передачу даних, не завжди враховує такі ризики, що створює додаткові прогалини в захисті персональних даних [53; 68; 129]. Технологічно-правовий розрив посилюється також через складність ідентифікації моменту порушення прав суб'єкта персональних даних. У випадку алгоритмічної обробки негативні наслідки можуть виникати не в момент збирання або первинного використання даних, а на пізніших етапах функціонування системи, зокрема внаслідок донавчання моделі або зміни контексту її застосування. Така відкладеність ускладнює застосування традиційних правових засобів захисту та підвищує ризик того, що порушення залишаться поза сферою ефективного контролю [57; 129].

Окремим і водночас системоутворювальним проблемним виміром національного правового регулювання захисту персональних даних у сфері використання штучного інтелекту є обмежена придатність класичних принципів захисту персональних даних до алгоритмічних систем. Чинне законодавство ґрунтується на принципах, сформульованих у контексті традиційних моделей обробки інформації, де процеси збирання, зберігання та використання персональних даних мали відносно стабільний, контрольований і лінійний характер. Алгоритмічні системи штучного інтелекту, навпаки, функціонують у режимі постійної адаптації, взаємозалежності та масштабованості, що ставить під сумнів можливість прямого застосування класичних принципів без їх сутнісного переосмислення [111; 112]. Проблемність застосування класичних принципів виразно виявляється в реалізації принципу обмеження мети обробки персональних даних. У традиційній правовій моделі мету обробки

визначають до початку збирання даних, і вона залишається відносно незмінною протягом усього життєвого циклу обробки. У системах штучного інтелекту персональні дані часто використовують у багатоетапних процесах, де початкова мета може еволюціонувати або доповнюватися внаслідок донавчання моделей, оптимізації алгоритмів чи повторного використання дата-сетів. За таких умов формальне дотримання принципу обмеження мети не гарантує фактичного контролю за подальшими способами використання персональних даних [105; 110].

Проблематичним є і застосування принципу мінімізації даних. Алгоритмічні системи, передусім ті, що ґрунтуються на машинному навчанні, демонструють високу залежність від обсягу та різноманітності даних. Практика розроблення та впровадження штучного інтелекту часто ґрунтується на презумпції необхідності залучення максимально можливих масивів даних для підвищення точності й надійності моделей. Це створює опозицію з принципом мінімізації, який у класичному значенні передбачає обмеження обробки лише тими даними, що є необхідними для досягнення визначеної мети [71; 77]. Тож принцип мінімізації ризикує залишатися декларативним і втрачає свій стримувальний потенціал. Структурна непридатність класичних принципів виявляється також у застосуванні принципу прозорості. У традиційних моделях обробки прозорість передбачає можливість зрозуміти, які персональні дані обробляють, з якою метою та які суб’єкти. У випадку алгоритмічних систем цього виявляється недостатньо, оскільки ключове значення має не лише факт обробки, а й логіка функціонування моделей, механізми формування прогнозів і критерії прийняття автоматизованих рішень. Непрозорість або часткова непрозорість алгоритмів ускладнює реалізацію принципу прозорості в його класичному вигляді й обмежує здатність суб’єкта персональних даних усвідомлено реалізовувати свої права [82; 137]. Проблеми виникають також під час застосування принципу точності персональних даних. Алгоритмічні системи часто оперують не лише первинними даними, а й похідними показниками,

профілями та прогнозними оцінками, які можуть не відповідати фактичним характеристикам особи, водночас впливати на прийняття рішень щодо неї. Чинне законодавство переважно не розрізняє статус первинних персональних даних і результатів їх алгоритмічної обробки, що ускладнює реалізацію принципу точності та коригування даних у контексті штучного інтелекту [129; 137]. Структурне напруження між класичними принципами захисту персональних даних й алгоритмічними системами виявляється в застосуванні принципу пропорційності. У традиційній правовій логіці пропорційність оцінюють шляхом співвіднесення втручання в приватність із досягненням конкретної, чітко визначеної мети. Алгоритмічні системи можуть генерувати множинні ефекти, включно з непрямими й відкладеними наслідками, що ускладнює оцінку пропорційності в момент ухвалення рішення про використання персональних даних [101]. Це створює ризик системного недооцінювання впливу штучного інтелекту на права і свободи людини.

Проблемність класичних принципів захисту персональних даних у контексті штучного інтелекту посилюється також через їх формально-універсальний характер. Принципи застосовують однаково до різних типів обробки, незалежно від рівня ризику, масштабу впливу або ступеня автономності алгоритмічних систем. Такий підхід не дає змоги адекватно врахувати специфіку високоризикових застосувань штучного інтелекту й обмежує можливості диференційованого правового реагування [56; 116].

Отже, структурна непридатність класичних принципів захисту персональних даних до алгоритмічних систем штучного інтелекту виявляється не в їх повній непридатності, а в обмеженості їх регуляторного потенціалу за умов збереження традиційного тлумачення. Без переосмислення змісту та функцій цих принципів вони не здатні ефективно виконувати роль базових орієнтирів захисту приватності в цифровому середовищі.

Також слід акцентувати на обмеженій здатності чинного законодавства адекватно враховувати кумулятивні та непрямі наслідки алгоритмічної

обробки інформації. Традиційна модель правового захисту приватності керується припущенням, що втручання в права суб'єкта персональних даних має чітко окреслений характер, може бути ідентифіковане в конкретний момент часу та співвіднесене з визначеними діями конкретного суб'єкта обробки. Алгоритмічні системи штучного інтелекту порушують цю логіку, оскільки їх вплив на права і свободи особи формується поступово, через накопичення результатів обробки, перехресне використання даних і взаємодію кількох технологічних процесів [101; 105].

Кумулятивний характер алгоритмічної обробки персональних даних виявляється в тому, що деякі операції з даними можуть не створювати очевидного або негайного ризику для приватності, однак їх поєднання в межах складних систем призводить до істотного посилення втручання в особисту сферу. Профілювання, прогнозування поведінки, оцінка ризиків й автоматизоване прийняття рішень часто ґрунтуються на результатах попередніх етапів обробки, що робить загальний вплив алгоритмічної системи значно інтенсивнішим, ніж сума окремих операцій. Чинне законодавство, орієнтоване на оцінювання окремих актів обробки, не завжди здатне охопити такий накопичувальний ефект [82; 137]. Непрямі наслідки алгоритмічної обробки персональних даних становлять ще складнішу проблему для правового регулювання. Вони можуть виявлятися у формі опосередкованого впливу на доступ особи до ресурсів, послуг або можливостей, без прямого прийняття рішення щодо неї. Алгоритмічні системи можуть змінювати інформаційне середовище, у якому перебуває особа, формувати її цифровий профіль або впливати на поведінку інших суб'єктів, що зрештою позначається на реалізації прав і свобод людини. Такі ефекти часто залишаються поза сферою прямого правового контролю, оскільки не підпадають під класичні уявлення про обробку персональних даних [83; 116].

Обмеженість національного законодавства у врахуванні кумулятивних і непрямих наслідків тісно пов'язана з домінуванням індивідуалізованого

підходу до захисту персональних даних. Правові механізми переважно орієнтовані на захист окремого суб'єкта в конкретній ситуації, натомість алгоритмічні системи часто створюють системні ефекти, що впливають на широкі групи осіб або суспільство загалом. За відсутності інструментів оцінювання колективного та суспільного впливу алгоритмічної обробки персональних даних значна частина ризиків залишається невидимою для правозастосування [62; 89]. Кумулятивні наслідки алгоритмічної обробки ускладнюють також застосування принципу пропорційності й оцінку правомірності втручання в приватність. Втручання, яке на початковому етапі може виглядати мінімальним і виправданим, з плином часу набуває якісно іншого характеру внаслідок повторного використання даних, їх поєднання з іншими джерелами та використання в нових контекстах. Чинні правові механізми не завжди дають змогу врахувати цю динаміку, що призводить до заниження реального рівня ризику для прав суб'єктів персональних даних [101; 105]. Кумулятивні та непрямі наслідки алгоритмічної обробки часто стають очевидними лише на пізніх етапах функціонування системи. На момент упровадження або первинної оцінки правомірності обробки персональних даних такі наслідки може бути неможливо передбачити з достатнім рівнем точності. Тож правове регулювання, орієнтоване на попередню оцінку ризиків, не забезпечує належного захисту від довгострокових або емерджентних ефектів використання штучного інтелекту [56; 88].

Нездатність законодавства повністю враховувати кумулятивні та непрямі наслідки алгоритмічної обробки персональних даних впливає також на ефективність механізмів відповідальності. У випадках, коли негативні наслідки виявляються поступово або мають розподілений характер, складно визначити момент порушення, суб'єкта відповідальності й обсяг завданої шкоди. Це додатково ускладнює захист прав суб'єктів персональних даних і посилює відчуття правової беззахисності в цифровому середовищі [55; 129].

Обмежена здатність національного законодавства враховувати кумулятивні й непрямі наслідки алгоритмічної обробки персональних даних формує ще один системний дефіцит правового регулювання у сфері штучного інтелекту. Вона засвідчує необхідність переходу від статичної, подієво орієнтованої моделі захисту приватності до динамічного та контекстуального підходу, здатного враховувати тривалий і багатовимірний вплив алгоритмічних систем на права і свободи людини. В Україні немає комплексних нормативних положень, які безпосередньо встановлювали б вимоги щодо людського контролю за рішеннями, прийнятими системами штучного інтелекту під час обробки персональних даних. Чинне законодавство не забезпечує чіткого механізму перевірки алгоритмічних рішень, не визначає меж автоматизованого прийняття рішень, не закріплює процедур перегляду таких рішень людиною, а також не формує правового режиму відповідальності за наслідки функціонування алгоритмів. Це створює ситуацію, коли застосування ШІ в державному управлінні, правоохоронній діяльності та приватному секторі може відбуватися без реальних гарантій захисту прав суб’єктів персональних даних.

Відсутність закріпленого людського елементу в регулюванні підвищує ризики неправомірного профілювання, дискримінаційних наслідків, помилкових висновків і непропорційного втручання в приватне життя. Для забезпечення ефективного захисту персональних даних необхідне нормативне закріплення обов’язковості людського контролю у високоризикових системах ШІ, а також встановлення гарантій доступу до інформації про логіку алгоритмічного рішення, можливості його оскарження та обов’язкового перегляду уповноваженою особою [28].

3.3. Розроблення рекомендацій та пропозицій щодо нормативно-правового забезпечення захисту персональних даних у сфері штучного інтелекту в Україні

З огляду на проаналізовані тенденції та окреслені проблеми, можна сформулювати низку рекомендацій для вдосконалення національного правового механізму захисту персональних даних в умовах використання штучного інтелекту. Такі рекомендації ґрунтуються на найкращих практиках ЄС та інших демократичних держав, що адаптовані до українських реалій. Доцільно враховувати, що в Європейському Союзі регулювання цифрових технологій формується комплексною системою взаємопов'язаних актів, де захист персональних даних функціонує у взаємодії з нормами, що регулюють доступ до даних і безпеку цифрового середовища [118; 124]. Методологічною основою таких пропозицій є ризик-орієнтований підхід [103; 124], згідно з яким різний типаж використання ШІ потребує різного рівня правового регулювання. За цим самим підходом обробка персональних даних із використанням систем, які здатні автоматично оцінювати особу (формувати її цифровий профіль, впливати на доступ до прав і послуг, соціальних благ, правосуддя чи безпеки), має супроводжуватися підвищеними правовими гарантіями [118].

Диференціацію таких гарантій залежно від рівня ризику алгоритмічної обробки персональних даних відображено в порівняльній таблиці запропонованих змін до Закону України «Про захист персональних даних»:

Таблиця 3.1

ПОРІВНЯЛЬНА ТАБЛИЦЯ

до проекту Закону України «Про внесення змін до Закону України «Про захист персональних даних» щодо особливостей обробки персональних даних із використанням систем штучного інтелекту»

Чинна редакція	Запропонована редакція	Аргументація
«Суб'єкт персональних даних має право знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки...» (ст. 8 Закону України «Про захист персональних даних»).	Доповнити: «Суб'єкт персональних даних має право отримувати інформацію про факт використання систем штучного інтелекту під час обробки його персональних даних, логіку автоматизованого прийняття рішень, а також право вимагати перегляду такого рішення людиною та оскаржувати його результати».	Чинна редакція гарантує доступ до інформації про обробку персональних даних, однак не забезпечує прозорості алгоритмічної обробки та автоматизованого прийняття рішень. Запропоноване доповнення спрямоване на посилення контролю особи над використанням її персональних даних у системах штучного інтелекту та забезпечення ефективного захисту її прав.
«Обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних або у випадках, передбачених законами України...» (ст. 6	Доповнити: «У разі використання високоризикових систем штучного інтелекту володілець персональних даних зобов'язаний до початку обробки провести оцінку впливу	Закон не встановлює спеціальних механізмів оцінювання ризиків під час застосування систем штучного інтелекту. Запровадження оцінки впливу дозволить виявляти потенційні порушення прав

Закону України «Про захист персональних даних»).	на захист персональних даних та документально підтвердити вжиття заходів щодо мінімізації ризиків для прав і свобод суб'єктів персональних даних».	суб'єктів персональних даних до початку функціонування таких систем та мінімізувати негативні наслідки їх використання.
«Забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, а також даних, що стосуються здоров'я чи статевого життя...» (ст. 7 Закону України «Про захист персональних даних»).	Доповнити: «Використання біометричних, генетичних та інших чутливих персональних даних для навчання, тестування або функціонування систем штучного інтелекту допускається лише за наявності окремої законної підстави та додаткових організаційних і технічних гарантій захисту».	Чинна редакція не враховує специфіку використання чутливих персональних даних для навчання та функціонування систем штучного інтелекту. Запропоноване доповнення забезпечить підвищений рівень захисту таких даних та мінімізує ризики їх неправомірного використання.

Джерело: розроблено автором за результатами аналізу законодавства України, міжнародних стандартів у сфері захисту персональних даних і штучного інтелекту, а також результатів проведеного анкетування.

Наведена порівняльна таблиця охоплює три напрями вдосконалення Закону України «Про захист персональних даних» у частині регулювання систем штучного інтелекту; усі вони ґрунтуються на ризик-орієнтованому підході.

Перший напрям розширює права суб’єкта персональних даних в умовах алгоритмічної обробки. Чинна редакція закріплює лише загальне право знати про джерела збирання та мету обробки і не враховує особливостей автоматизованого прийняття рішень. Тому запропоновано надати особі право отримувати інформацію про сам факт застосування ШІ та логіку алгоритмічного рішення, вимагати його перегляду людиною й оскаржувати результати. Цей напрям належить до низькоризикових, оскільки стосується інформаційних прав, реалізація яких не потребує суттєвої перебудови процесів обробки.

Другий напрям запроваджує обов’язок проводити оцінку впливу на захист персональних даних до початку використання високоризикових ШІ-систем. За рівнем ризику він є середнім з огляду на додаткове функціональне й організаційне навантаження на суб’єктів обробки. Запропонована норма зобов’язує володільця даних документально підтвердити вжиті заходи мінімізації ризиків ще до запуску системи; нині такого механізму бракує, що унеможливлює превентивне виявлення загроз правам особи.

Третій напрям регулює обробку чутливих категорій персональних даних (біометричних, генетичних та інших) для навчання чи функціонування ШІ-систем і несе високий ризик з огляду на незворотність можливих порушень прав особи. Чинна редакція встановлює загальну заборону обробки таких даних, не враховуючи специфіки ШІ-середовища. Запропоноване доповнення допускає її лише за наявності окремої законної підстави та додаткових організаційних і технічних гарантій захисту.

Слід визначити, що розробник ШІ-системи відповідає за проєктування системи відповідно до принципів privacy by design і privacy by default, мінімізацію дискримінаційних ризиків, якість навчальних даних, наявність

технічної документації, можливість аудиту та належний рівень безпеки. Постачальник ШІ-системи відповідає за надання користувачу достатньої інформації щодо призначення системи, меж її використання, рівня точності, відомих обмежень, можливих ризиків і необхідних заходів людського контролю. Оператор або володілець персональних даних відповідає за законність конкретної мети обробки, належне інформування суб'єктів даних, проведення оцінювання впливу, забезпечення людського втручання, оскарження та недопущення використання результатів ШІ як єдиної підстави для істотного рішення щодо особи. Структурно запропонована модель алгоритмічної відповідальності може бути представлена у вигляді таблиці, у якій відображено основних суб'єктів ШІ-екосистеми, сферу їхнього впливу, ключові обов'язки та можливі підстави відповідальності у сфері обробки персональних даних:

Таблиця 3.2

Авторська модель алгоритмічної відповідальності у сфері обробки персональних даних системами штучного інтелекту

Суб'єкт	**Сфера впливу**	**Основні обов'язки**	**Потенційна відповідальність**
Розробник ШІ-системи	Архітектура моделі, технічні рішення, навчальні дані	Privacy by design/default, мінімізація даних, недискримінаційність, технічна документація, механізми людського контролю	За дефекти архітектури, непрозорість моделі, використання неналежних навчальних даних, відсутність засобів контролю
Постачальник	Введення	Інформування про	За приховування

Суб’єкт	**Сфера впливу**	**Основні обов’язки**	**Потенційна відповідальність**
ШІ-системи	системи в обіг, передача або інтеграція	ризики, межі застосування, технічна документація, інструкції безпечного використання	ризиків, неналежне інформування, передачу системи без гарантій захисту даних
Оператор / користувач ШІ-системи	Конкретне застосування системи	Використання лише за визначеною метою, людський контроль, реагування на скарги, недопущення неправомірного профілювання	За використання поза метою, без людського перегляду, неправомірне автоматизоване рішення
Володілець персональних даних	Визначення мети і засобів обробки	Законна підстава, прозорість, мінімізація, DPIA, забезпечення прав суб’єкта даних	За незаконну або непропорційну обробку, непроведення DPIA, порушення прав суб’єкта
Розпорядник персональних даних	Обробка за дорученням володільця	Безпека даних, виконання доручення, недопущення самостійного використання даних для навчання інших моделей	За перевищення доручення, витік даних, використання даних для власної алгоритмічної мети
Незалежний аудитор /	Перевірка системи та	Оцінка відповідності, перевірка джерел даних,	За формальний або недостовірний

Суб'єкт	Сфера впливу	Основні обов'язки	Потенційна відповідальність
орган оцінки	ризиків	недискримінаційності, прозорості й людського контролю	висновок, ігнорування істотних ризиків

Джерело: розроблено автором за результатами дисертаційного дослідження.

Також необхідно ввести алгоритмічний аудит – документована перевірка ШІ-системи, яка обробляє персональні дані, на відповідність вимогам законності, прозорості, безпеки, недискримінації, точності, пояснюваності та людського контролю. Перевірка може бути незалежною або внутрішньою.

Додатково забезпечити факт того, що обробка біометричних персональних даних із використанням ШІ допускається лише за наявності спеціальної правової підстави, визначеної законом або прямо вираженої згоди особи, якщо така згода є справді добровільною та може бути відкликана без негативних наслідків для особи. Використання біометричних ШІ-систем для дистанційної ідентифікації в публічному просторі має бути дозволене лише у виняткових випадках, за умови легітимної мети, необхідності, пропорційності, обмеження строків, території, кола осіб, попередньої оцінки впливу й незалежного контролю.

Встановити заборону невибіркового, постійного або масового біометричного спостереження за особами в публічно доступних місцях, якщо таке спостереження не має конкретної законної мети, не ґрунтується на чіткій правовій підставі та не супроводжується ефективними гарантіями від зловживань. В умовах воєнного стану або загроз національній безпеці можуть бути винятки, однак їх має бути передбачено законом, вони повинні бути тимчасовими, пропорційними та підконтрольними суду або іншому незалежному органу.

Доповнити процесуальне законодавство положенням про те, що використання результатів ШІ-систем у кримінальному провадженні допускається лише за умови документування джерела даних, способу їх отримання, технічних характеристик системи, рівня точності, відомої похибки, умов застосування, наявності людської перевірки й можливості сторони захисту поставити питання щодо достовірності, методики і допустимості такого результату. Якщо алгоритмічний результат отримано з порушенням законодавства про персональні дані або без належної процесуальної підстави, його не можна використовувати як доказ.

Мають бути розроблені: порядок проведення оцінювання впливу на захист персональних даних для ШІ-систем; методика алгоритмічного аудиту; вимоги до технічної документації; критерії належного людського контролю; порядок інформування суб'єктів персональних даних про автоматизовану обробку; стандарти захисту біометричних даних; рекомендації щодо використання ШІ в правоохоронній діяльності та кримінальному процесі; правила перевірки дискримінаційних ефектів алгоритмічних систем.

Висновки до розділу 3

У третьому розділі дисертації зосереджено увагу на тому, як саме може бути вдосконалено нормативно-правове забезпечення захисту персональних даних у сфері штучного інтелекту в Україні, з огляду на реальні технологічні процеси та сучасні європейські підходи. Аналіз засвідчує, що ефективне регулювання в цій сфері не зводиться до формального оновлення законодавчих приписів, а потребує глибшого переосмислення ролі права в умовах алгоритмічної обробки даних.

Обґрунтовано, що захист персональних даних у контексті використання штучного інтелекту слід розглядати як складову ширшої цифрової правової екосистеми, у межах якої взаємодіють норми про

приватність, регулювання цифрових сервісів, доступ до даних, інформаційну безпеку та гарантії прав людини. Такий підхід надає можливість уникнути фрагментарності правового регулювання та забезпечує послідовне застосування принципів пропорційності, підзвітності й людиноцентричності під час впровадження та використання алгоритмічних систем.

У розділі констатовано, що специфіка обробки персональних даних за допомогою систем штучного інтелекту суттєво ускладнює традиційні уявлення про анонімізацію та мінімізацію даних. Наявність технічних ризиків, пов’язаних із можливістю повторної ідентифікації, витоку навчальних даних і відтворення персональної інформації з моделей, свідчить про обмеженість суто декларативних правових заборон. У зв’язку з цим обґрунтовано необхідність поєднання правових вимог із технічними й організаційними заходами захисту, які здатні реально знизити рівень втручання в приватне життя.

Доведено доцільність застосування ризик-орієнтованого підходу до регулювання систем штучного інтелекту, за якого обсяг правових обов’язків і гарантій визначають залежно від потенційного впливу конкретних технологій на права і свободи людини. Такий підхід дає змогу одночасно забезпечити належний рівень захисту персональних даних у чутливих сферах і не створювати надмірних бар’єрів для розвитку інноваційних рішень. Окремо акцентовано на значенні інституційних орієнтирів і правозастосовної практики, зокрема позицій органів із захисту персональних даних і прикладів побудови розподілених інформаційних інфраструктур. Зазначене дасть змогу адаптувати загальні правові норми до конкретних технологічних ситуацій і забезпечують гнучке й ефективне застосування законодавства без постійного його формального перегляду.

Тож можна дійти висновку, що запропоновані в розділі підходи та рекомендації формують цілісну модель правового регулювання захисту персональних даних у сфері штучного інтелекту, у межах якої нормативні приписи підкріплені інституційними й технічними гарантіями. Така модель

створює передумови для досягнення балансу між розвитком інноваційних технологій і дотриманням фундаментальних прав людини, а також сприяє поступовій інтеграції України до європейського та глобального цифрового правового простору.

ВИСНОВКИ

У висновках дисертації викладено найважливіші наукові та практичні результати, одержані під час дослідження; узагальнено основні теоретичні положення щодо правової охорони й захисту персональних даних у сфері штучного інтелекту; сформульовано практичні рекомендації та конкретні пропозиції з удосконалення нормативно-правового регулювання обробки персональних даних в умовах використання алгоритмічних технологій в Україні.

1. Висвітлено концептуальні засади штучного інтелекту, визначено його вплив на обробку персональних даних. Здійснений аналіз засвідчив, що штучний інтелект у цій сфері не є лише технічним інструментом для швидшого опрацювання інформації, а змінює характер роботи з даними про особу. Сучасні алгоритмічні системи збирають, поєднують, оцінюють і повторно використовують великі обсяги відомостей, що перетворює персональні дані на постійний ресурс для навчання, тестування, упровадження та функціонування ШІ. У таких умовах дані вже не обмежуються одноразовою обробкою для заздалегідь визначеної мети, а стають частиною безперервного процесу, який може породжувати нові відомості про особу, впливати на її правове становище та формувати рішення без безпосередньої участі людини. Зазначене засвідчує, що розвиток алгоритмічних технологій безпосередньо впливає на зміст, межі та внутрішню логіку правового режиму персональних даних, актуалізує необхідність оновлення традиційних підходів до їх охорони й захисту. Саме тому проблема захисту персональних даних у сфері ШІ має не вузько технічний, а системний правовий характер і стосується базових гарантій права людини на приватність.

2. Дослідження стану наукового розроблення проблеми та генези правових підходів до охорони персональних даних у сфері ШІ в Україні дало підстави для висновку, що ця тема ще не дістала достатнього комплексного висвітлення в національній юридичній науці. Українські науковці вже вивчали

питання захисту персональних даних, цифрової приватності, автоматизованої обробки інформації, інформаційної безпеки та правового регулювання штучного інтелекту, однак розглядали переважно ці аспекти окремо. Унаслідок цього сформувалася ситуація, коли науковий інтерес до теми безумовно є, але цілісної моделі правової охорони і захисту персональних даних саме у сфері ШІ в Україні немає. Генеза правових підходів засвідчує, що українське законодавство та правова доктрина протягом тривалого часу орієнтувалися на класичне розуміння персональних даних як об'єкта обробки в межах порівняно стабільних інформаційних систем. Натомість поява Big Data, самонавчальних моделей, алгоритмічного профілювання, інференційного аналізу й біометричних технологій потребує сучаснішого бачення, у межах якого персональні дані оцінюють не лише за фактом їх збирання, а й з огляду на те, які наслідки породжує їх алгоритмічна обробка для прав, свобод і законних інтересів особи.

3. У роботі визначено методологічні підходи до правової охорони та захисту персональних даних в умовах розвитку алгоритмічних технологій. Дослідження засвідчило, що в умовах використання великих масивів даних і самонавчальних моделей традиційні правові принципи, зокрема інформована згода, мінімізація даних та цільове обмеження, не втрачають значення, але потребують нового тлумачення й адаптації до реальних технологічних умов. Згода суб'єкта персональних даних дедалі частіше стає формальною, оскільки особа фактично не може передбачити всі можливі способи подальшого використання її інформації. Принцип мінімізації даних так само постає перед практикою розвитку ШІ, де якість моделі нерідко залежить від обсягу, різноманітності й тривалості використання даних. Саме тому в дисертації обґрунтовано доцільність комплексного підходу, що поєднує юридичні, організаційні, технічні й етичні інструменти. Методологічною основою такого підходу є risk-based approach, за якого інтенсивність правового регулювання визначають не формальною наявністю обробки, а реальним рівнем ризику для особи. У цьому контексті важливе значення мають принципи privacy by design

і privacy by default, проведення DPIA для високоризикових систем, забезпечення людського контролю, прозорості автоматизованих процесів і реальної підзвітності всіх суб'єктів, які беруть участь у життєвому циклі ШІ-системи.

4. Проаналізовано поняття та класифікацію персональних даних у сфері ШІ на основі зарубіжного досвіду. Установлено, що в умовах алгоритмічної обробки правове значення мають не лише звичайні ідентифікаційні дані, а й чутливі, біометричні, поведінкові, технічні, похідні та інференційні дані. Увагу спрямовано на інференційні дані, які не повідомляє особа безпосередньо, вони формуються шляхом аналізу інших відомостей, їх використовують для прогнозування поведінки, оцінки характеристик, визначення рівня ризику чи формування рішення щодо особи. Саме такі дані можуть істотно впливати на доступ до працевлаштування, кредитування, соціальних послуг, державних сервісів або інших можливостей реалізації прав, хоча суб'єкт даних може навіть не знати про їх існування. Порівняльний аналіз засвідчив, що зарубіжні правопорядки відмовляються від вузького підходу, за якого персональні дані розуміють лише як прямо надану інформацію, і визнають важливість захисту даних, які виникають унаслідок аналітичної та прогнозної роботи алгоритмів. На цій підставі в дисертації обґрунтовано, що інференційні дані мають бути окремо враховані в національному законодавстві як самостійний об'єкт правової охорони, оскільки саме вони часто створюють найвищі ризики для прав людини в цифровому середовищі.

5. У дисертації систематизовано міжнародні нормативно-правові акти у сфері захисту персональних даних під час використання ШІ, окреслено їх значення для формування сучасної моделі правового регулювання. Установлено, що центральне місце в цій системі посідає GDPR, який закріплює базові принципи законності, прозорості, мінімізації, обмеження мети, підзвітності та захисту прав суб'єкта персональних даних. Водночас розвиток спеціального регулювання штучного інтелекту зумовлює необхідність урахування не лише загальних правил захисту даних, а й норм,

які стосуються оцінки ризику, автоматизованих рішень, високоризикових систем і людського нагляду. У цьому контексті проаналізовано значення Конвенції 108+, документів Ради Європи, актів OECD, підходів ЮНЕСКО, а також новітніх європейських рішень у сфері ШІ. Систематизація цих актів дала змогу з'ясувати, що міжнародне регулювання послідовно рухається до моделі, у якій захист персональних даних у сфері ШІ розглядають як частину ширшої системи гарантій прав людини. Саме тому міжнародні стандарти вже не обмежуються вимогами до форми згоди чи порядку зберігання даних, акцентуючи на прозорості алгоритмів, оцінюванні ризиків, недопущенні дискримінації, забезпеченні пояснюваності рішень і реальної можливості оскарження.

6. Досліджено правові засади регулювання захисту персональних даних у країнах ЄС, визначено можливості імплементації іноземного досвіду в законодавство України. Порівняльно-правовий аналіз засвідчив, що в європейському правопорядку поступово формується цілісна модель взаємодії між загальним регулюванням захисту персональних даних і спеціальним регулюванням штучного інтелекту. GDPR визначає фундаментальні стандарти обробки персональних даних, а AI Act доповнює їх вимогами до високоризикових ШІ-систем, механізмами оцінювання відповідності, розширеними обов'язками для учасників життєвого циклу системи й акцентом на недопущенні шкоди для прав людини. Для України цей досвід є вкрай важливим у зв'язку з євроінтеграційним курсом, однак у роботі обґрунтовано, що імплементація зарубіжних підходів не має зводитися до механічного перенесення окремих норм. Європейські рішення мають адаптуватися з огляду на українську правову систему, рівень цифровізації, інституційні можливості, особливості державного сектору й умови воєнного стану. Саме тому аргументовано, що для України найперспективнішим є поетапне впровадження європейських підходів зі збереженням їхнього змісту, але з огляду на національний контекст і практичні потреби правозастосування.

7. Розглянуто сучасний стан і тенденції розвитку національного законодавства щодо захисту персональних даних у сфері ШІ. Установлено, що чинне законодавство України містить базові засади охорони й захисту персональних даних, однак загалом залишається фрагментарним і не пропонує вичерпних відповідей на ключові виклики, пов'язані з використанням алгоритмічних систем. Законодавче регулювання зорієнтоване передусім на класичну модель обробки даних і недостатньо враховує автоматизоване прийняття рішень, алгоритмічне профілювання, інференційні дані, високоризикове використання біометрії, а також специфіку обробки даних у державному секторі. Водночас простежується тенденція до поступового наближення національних норм до європейських стандартів. У цьому контексті важливе значення має законопроєкт № 8153, який демонструє спробу оновити підхід до захисту персональних даних і зблизити його з положеннями GDPR. Водночас констатовано, що навіть за наявності такого законодавчого руху українська модель ще знаходиться на етапі становлення, а її розвиток має супроводжуватися чітким розумінням того, що правове регулювання у сфері ШІ має бути не декларативним, а практично придатним для застосування.

8. Виявлено проблеми національного законодавства у сфері захисту персональних даних під час використання ШІ, окреслено основні шляхи їх подолання. До таких проблем віднесено брак у законодавстві чіткого визначення інференційних даних, недостатню регламентацію автоматизованого прийняття рішень й алгоритмічного профілювання, слабкість механізмів людського контролю, відсутність належного інституційного нагляду, невизначеність правил використання біометричних технологій, а також брак чіткої моделі відповідальності осіб, які розробляють, постачають і використовують ШІ-системи. Аналіз також засвідчив, що серйозною проблемою є відсутність належних превентивних механізмів, які мали б діяти до запуску системи, а не лише після виникнення порушення. Саме тому в роботі обґрунтовано необхідність переходу від фрагментарного

реагування до системного регулювання, яке поєднує чітке визначення правового статусу окремих категорій даних, обов'язковість оцінювання ризиків, запровадження algorithmic audit, реальний людський нагляд, судовий або адміністративний контроль за високоризиковими рішеннями та посилення гарантій для особи в разі оскарження автоматизованих результатів. Розв'язання цих проблем можливе лише за умови послідовної гармонізації українського законодавства з європейськими підходами й одночасного врахування українських реалій.

9. Розроблено рекомендації щодо нормативно-правового забезпечення захисту персональних даних у сфері штучного інтелекту в Україні. Обґрунтовано доцільність нормативного закріплення поняття інференційних персональних даних, визначення високоризикової обробки персональних даних із використанням ШІ та встановлення спеціальних гарантій для таких випадків. Запропоновано передбачити обов'язкове проведення DPIA щодо високоризикових ШІ-систем ще на етапі їх проєктування і впровадження, а також закріпити обов'язок дотримання принципів privacy by design і privacy by default як спільної вимоги для розробників, постачальників й операторів таких систем. Важливим напрямом удосконалення законодавства визначено запровадження права особи на зрозуміле пояснення автоматизованого рішення, на людське втручання та ефективне оскарження наслідків алгоритмічної обробки. Аргументовано потребу у введенні algorithmic audit як форми перевірки законності, безпечності, недискримінаційності та належної якості ШІ-систем. Також запропоновано algorithmic responsibility model, у межах якої обов'язки й відповідальність мають бути розмежовані між розробником, постачальником, оператором, користувачем системи та володільцем персональних даних. У сукупності ці рекомендації спрямовані на формування в Україні цілісної, сучасної та практично орієнтованої системи правового регулювання, здатної забезпечити належний рівень захисту персональних даних, водночас створити правові умови для відповідального використання штучного інтелекту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авдєєва Г. К. Проблеми використання систем штучного інтелекту в роботі органів кримінальної юстиції. *Використання технологій штучного інтелекту у протидії злочинності* : матеріали наук.-практ. онлайн-семінару (Харків, 5 листоп. 2020 р.). Харків, 2020. С. 6–10.

2. Авдєєва Г. К. Цифрові докази і системи штучного інтелекту у правозастосовній діяльності. *Питання боротьби зі злочинністю.* 2023. Вип. 46. С. 32–40.

3. Андрощук Г. Штучний інтелект: економіка, інтелектуальні власність, загрози. *Теорія і практика інтелектуальної власності*. 2021. № 2. С. 56–74.

4. Бєлов Д. М., Бєлова М. В., Штучний інтелект в судочинстві та судових рішеннях, потенціал та ризики. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2023. Вип. 78 (4). Ч. 3. С. 289–294.

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

6. Бєлова М. В., Бєлов Д. М. Імплементація штучного інтелекту в досудове розслідування кримінальних справ: міжнародний досвід. *Аналітично-порівняльне правознавство*. 2023. № 2. С. 448–454.

7. Біла книга з регулювання ШІ в Україні: бачення Мінцифри. Версія для консультацій / відп. за розробку Г. Румянцев. Київ, 2024. 30 с. URL: https://backend.hromada.gov.ua/storage/uploads/files/research/bila-kniga-z-regulyuvannya-si-v-ukrayini-bacennya-mincifri/%D0%A0%D0%B5%D0%B3%D1%83%D0%BB%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%A8%D0%86.pdf?tim

8. Біла книга зі штучного інтелекту як джерело формування законодавства Європейського Союзу у сфері штучного інтелекту / [В. В. Мачуський, І. Б. Мачуська, В. М. Тітова та ін.]. *Аналітично-порівняльне правознавство*. 2024. № 2. С. 226–230. URL: https://journal-app.uzhnu.edu.ua/article/view/303207/295288

9. Білан І. А. Глобальні ризики використання чат-ботів, керованих штучним інтелектом. *Інформація і право.* 2024. № 3. С. 147–161.

10. Бисага Ю. М., Бєлова М. В., Бєлов Д. М. Виклики для прав дитини у зв'язку з розвитком штучного інтелекту. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2023. Вип. 77 (3). Ч. 1. С. 88–91.

11. Бліхар М. М. Адміністративно-правове забезпечення інформаційної безпеки в інтернет-просторі. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2021. Вип. 67. С. 345–349. DOI: https://doi.org/10.24144/2307-3322.2021.67.65

12. Брижко В. М. Захист персональних даних: реалії та практика сучасності. *Інформація і право*. 2013. № 3. С. 31–48. URL: https://ippi.org.ua/sites/default/files/13bvmrps.pdf

13. Брижко В. М., Радянська А. І., Швець М. Я. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних. Київ : Тріумф, 2006. 256 с. URL: https://just-dnipro.gov.ua/files/upload/files/24.pdf

14. Дубняк М. В. Економіка даних: правовий та етичний аспект. *Інформація і право*. 2023. № 3 (46). С. 64–74. URL: http://il.ippi.org.ua/article/view/287147

15. Заярний О. А. Адміністративна деліктологія в інформаційній сфері: проблеми теорії та практики : дис. … д-ра юрид. наук : 12.00.07. Київ, 2018. 561 с.

16. Заярний О. А. До питання щодо забезпечення правомірної обробки біометричних даних в діяльності Національної поліції: національні та

міжнародні стандарти. *Юридичний вісник*. 2021. № 6. С. 160–166. DOI: https://doi.org/10.32782/klj-2022-1.03

17. Заярний О. А., Деркаченко Ю. В. Деякі особливості обробки персональних даних при використанні чат-ботів зі штучним інтелектом на прикладі ChatGPT. *Юридичний бюлетень.* 2023. № 29. С. 55–62. DOI: https://doi.org/10.32850/LB2414-4207.2023.29.06

18. Заярний О. До питання удосконалення способів захисту інформаційних прав фізичних осіб у відносинах, пов'язаних із застосуванням технологій штучного інтелекту. *Вісник Київського національного університету імені Тараса Шевченка*. *Серія «Юридичні науки».* 2022. № 1 (120). С. 36–39. DOI: https://doi.org/10.17721/1728-2195/2022/1.120-7

19. Золотар О. О. Інформаційна безпека людини: теорія і практика : монографія. Київ : АртЕк, 2018. 446 с.

20. Каткова Т. Г. Штучний інтелект в Україні: правові аспекти. *Право і суспільство*. 2020. № 6. С. 46–55. URL: http://pravoisuspilstvo.org.ua/archive/2020/6_2020/10.pdf

21. Колесніков А. П., Карапетян О. М. Штучний інтелект: переваги та загрози використання. *Ефективна економіка*. 2023. № 8. С. 1–13. DOI: http://doi.org/10.32702/2307-2105.2023.8.9

22. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

23. Корнейко О. В. Інформаційна безпека в системі публічного управління: правовий аспект. *Державне управління: удосконалення та розвиток*. 2019. № 10. URL: http://www.dy.nayka.com.ua/?op=1&z=1500

24. Машталяр О. М. Масове спостереження та розпізнавання обличчя за допомогою штучного інтелекту: правові виклики та перспективи регулювання в Україні. *Юридичний науковий електронний журнал*. 2024. № 11. С. 317–321. DOI: 10.32782/2524-0374/2024-11/72

25. Машталяр О. М. Проблеми використання штучного інтелекту під час оброблення персональних даних та напрями їх вирішення. *Юридичний*

науковий електронний журнал. 2024. № 8. С. 256–259. DOI: 10.32782/2524-0374/2024-8/59

26. Машталяр О. М. Розпізнавання ходи як інноваційний метод ідентифікації: аналіз можливостей, ризиків та нормативно-правового середовища в Україні. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2025. Вип. 90. Ч. 4. С. 310–317. DOI: 10.24144/2307-3322.2025.90.4.44

27. Машталяр О. М. Штучний інтелект і біометричні дані в кримінальному процесі України: допустимість, ризики, судовий контроль. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2025. Вип. 92. Ч. 3. С. 276–283. DOI: 10.24144/2307-3322.2025.92.3.37

28. Машталяр О. М., Хахановський В. Г. Людський елемент у системах ШІ, що обробляють персональні дані: європейський стандарт і український дефіцит регулювання. *Юридичний науковий електронний журнал.* 2025. № 11. С. 160–163. DOI: 10.32782/2524-0374/2025-11/33

29. Машталяр О. М., Хахановський В. Г. Правові аспекти використання масового відеоспостереження в Україні: між потребами громадської безпеки та гарантіями прав людини. *Modern Science: Trends, Challenges, Solutions* : матеріали І Міжнар. наук.-практ. конф. (Ліверпуль, 21–23 серп. 2025 р.). Ліверпуль, 2025. С. 301–305. URL: https://sci-conf.com.ua/wpcontent/uploads/2025/08/MODERN-SCIENCE-TRENDS-CHALLENGES-SOLUTIONS-21-23.08.25.pdf

30. Некрутенко В. Р. До питання систематизації ризиків, спричинених обробленням персональних даних із використанням технології штучного інтелекту. *Вісник Київського національного університету імені Тараса Шевченка*. *Серія «Юридичні науки».* 2021. № 4 (119). С. 53–58.

31. Остіян Є. З. Штучний інтелект та персональні дані: захист приватності в цифровому середовищі. *Науковий вісник Ужгородського національного університету*. *Серія «Право».* 2024. Вип. 85. Ч. 3. С. 47–53. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/11/9-2.pdf

32. Петрів О. Захист персональних даних у добу штучного інтелекту: міжнародні підходи та виклики. *Центр демократії та верховенства права.* URL: https://cedem.org.ua/consultations/zahyst-personalnyh-danyh-u-dobu-shtuchnogo-intelektu-mizhnarodni-pidhody-ta-vyklyky/

33. Пилипчук В. Г., Брижко В. М. Інформаційна безпека та приватність сфері захисту персональних даних. *Інформація і право*. 2016. № 4. С. 60–70. DOI: https://doi.org/10.37750/2616-6798.2016.4(19).272979

34. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

35. Подгаєцький О. Еволюція розробок у галузі штучного інтелекту в Україні та світі. *Дослідження з історії техніки.* 2012. Вип. 16. С. 48–54. URL: https://ela.kpi.ua/server/api/core/bitstreams/3439f895-7fe4-47b3-ad25-43eaa9a340bd/content

36. Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

37. Про захист персональних даних : проєкт Закону України від 25 жовт. 2022 р. № 8153. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/40707

38. Про інформацію : Закон України від 2 жовт. 1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/rada/show/2657-12#Text

39. Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації : проєкт Закону України від 18 жовт. 2021 р. № 6177. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/27996

40. Прокопович-Ткаченко Д. І., Звєрєв В. П., Козаченко І. М. Інтеграція операційних центрів управління безпекою (SOC) у систему національної безпеки України. *Безпека держави*. 2025. Вип. 1 (5). С. 106–112. URL: https://sts.nangu.edu.ua/article/view/336736

41. Пунда О. О., Арзянцева Д. А. Забезпечення захисту персональних даних фізичних осіб в умовах розвитку штучного інтелекту. *Наука і техніка*

сьогодні. Серія «Право». 2024. № 2 (30). С. 132–142. DOI: https://doi.org/10.52058/2786-6025-2024-2(30)-132-142

42. Радченко А. Інформаційні правовідносини: сучасний стан і перспективи дослідження в українській юриспруденції. *Вісник Львівського університету*. *Серія «Юридична».* 2024. Вип. 78. С. 125–139. DOI: https://doi.org/10.30970/vla.2024.78.125

43. Регулювання штучного інтелекту в Україні: Мінцифри презентує Білу книгу. *Міністерство цифрової трансформації України*. URL: https://www.kmu.gov.ua/news/rehuliuvannia-shtuchnoho-intelektu-v-ukraini-mintsyfry-prezentuie-bilu-knyhu

44. Токарєва К. С., Савліва Н. О. Особливості правового регулювання штучного інтелекту в Україні. *Юридичний вісник. Серія «Повітряне і космічне право»*. 2021. № 3 (60). С. 148–153.

45. Баранов. О.А. Визначення терміну «штучний інтелект». *Інформація і право.* № 1(44)/2023. С. 32–49.

46. Хахановський В. Г., Петрик В. В. Штучний інтелект і електронні докази: проблеми автентичності (юридичний аспект). *Європейський правничий часопис.* 2025. Вип. 8. С. 161–165. DOI: 10.36919/3041-1149(Print).8.2025.161-165

47. Шпакович О. М., Батрименко О. В. Рекомендації щодо гармонізації законодавства Європейського Союзу з національним законодавством України. *Економіка та право*. 2024. № 3. С. 149–156. DOI: 10.32782/ep.2024.3.22

48. Що таке атака методом висновків. *VPN Unlimited.* URL: https://www.vpnunlimited.com/ua/help/cybersecurity/inference-attack?srsltid=AfmBOorPxwj8-f6bz-nBT00fhNOI0YFJ9B7jqyFzMY1DrfikakR49Mqr

49. Янишівський М. М., Красівський О. Я. Обчислювальне право: сумісність із правами людини та законодавче регулювання. *Науковий вісник*

«Демократичне врядування». 2021. Вип. 1 (27). С. 1–18. DOI: 10.33990/2070-4038.27.2021.239197

50. Стасевич С., Олена Голодовська О. Штучний інтелект: історія та становлення. *Інформаційні технології та суспільство*. Вип. 1 (16). 2025. С. 242–248. DOI https://doi.org/10.32689/maup.it.2025.1.31

51. Янишівський М. М. Формування та реалізація публічної політики у сфері штучного інтелекту в Україні. *Економіка, фінанси, менеджмент: актуальні питання науки і практики.* 2024. № 4. С. 96–122. URL: http://efm.vsau.org/storage/articles/April2025/7eX0tkd3OYodRwf55tF6.pdf

52. European Commission. 2018. A definition of Artificial Intelligence: main capabilities and scientific disciplines. Report High-Level Expert Group on Artificial Intelligence.

53. Abadi M. Deep Learning with Differential Privacy / [M. Abadi, A. Chu, I. Goodfellow et al.]. *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (ACM CCS).* 2016. P. 308–318. URL: https://arxiv.org/abs/1607.00133

54. Act on the Protection of Personal Information (APPI) : Law of Japan. *Government of Japan*. URL: https://www.avitar.legal/post/zahist-personalnih-danih-v-aziyi

55. AI and GDPR: supporting responsible innovation. 2024. *Commission européenne pour l'informatique et les libertés (CNIL).* URL: https://www.cnil.fr/en/ai-and-gdpr

56. AI, Data Governance and Privacy. Synergies and areas of international co-operation. 2024. *Organisation for Economic Co-operation and Development (OECD).* URL: https://www.oecd.org/publications/ai-data-governance-and-privacy-2476b1a4-en.htm

57. Algorithms and Artificial Intelligence: Recommendations for Transparency and Governance. 2017. *Commission européenne pour l'informatique et les libertés (CNIL).* URL: https://www.cnil.fr/en/algorithms-and-artificial-intelligence

58. Alzoubi Y. I., Mishra A. Differential privacy and artificial intelligence: potentials, challenges, and future avenues. *EURASIP Journal on Information Security*. 2025. No. 18. P. 1–23. DOI: 10.1186/s13635-025-00203-9

59. Applying Data Protection Principles to Generative AI: Practical Approaches for Organizations and Regulators. December 2024. *Centre for Information Policy Leadership (CIPL).* URL: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_applying_data_protection_principles_genai_dec24.pdf

60. Artificial intelligence – Risk management – Guidance : ISO/IEC 23894:2023. *ISO – International Organization for Standardization*. URL: https://www.iso.org/standard/77304.html

61. Artificial intelligence (subject page). 2024. *European Data Protection Supervisor.* URL: https://www.edps.europa.eu/data-protection/our-work/subjects/artificial-intelligence_en

62. Artificial Intelligence and Data Protection: Declaration. 2018. *Global Privacy Assembly.* URL: https://globalprivacyassembly.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf

63. Artificial Intelligence in Society. OECD Publishing, 2019. *Organisation for Economic Co-operation and Development (OECD).* URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/06/artificial-intelligence-in-society_c0054fa1/eedfee77-en.pdf

64. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. National Institute of Standards and Technology, 2023. 48 p. URL: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

65. Blueprint for an AI Bill of Rights. The White House Office of Science and Technology Policy. 2022. *National Archives*. URL: https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/

66. California Consumer Privacy Act (CCPA) : Civil Code §1798.140. *California Legislative Information.* URL:

https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.140

67. California Privacy Rights Act (CPRA). *California Privacy Protection Agency.* URL: https://thecpra.org/

68. Carlini N. et al. Extracting Training Data from Large Language Models. 2021. *arXiv*. URL: https://arxiv.org/abs/2012.07805

69. Children's Online Privacy Protection Rule (COPPA). *Federal Trade Commission.* URL: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

70. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS 225). 2024. *Council of Europe*. URL: https://rm.coe.int/1680afae3c

71. Data Protection Engineering. 2022. *ENISA.* URL: https://www.enisa.europa.eu/publications/data-protection-engineering

72. Data Protection Impact Assessment Template. *GDPR.eu. General Data Protection Regulation (GDPR) Compliance Guidelines*. URL: https://gdpr.eu/data-protection-impact-assessment-template/ GDPR.eu

73. Data Use and Access Act 2025 : Legislation overview. *Information Commissioner's Office (UK).* URL: https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/

74. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016. (Law Enforcement Directive). *EUR-Lex. Access to European Union law*. URL: https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng

75. Directive 2002/58/EC (ePrivacy Directive). *EUR-Lex. Access to European Union law*. URL: https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng

76. Dubniak M. V. Open data and explanatory artificial intelligence: legal perspectives. *Information and law*. 2024. No. 2 (49). P. 102–117. DOI: 10.37750/2616-6798.2024.2(49).306147.

77. Dwork C., Roth A. The Algorithmic Foundations of Differential Privacy. 2014. *University of Pennsylvania*. URL: https://www.cis.upenn.edu/~aaroth/Papers/privacybook.pdf

78. Efficient protocols from & for differential privacy without a trusted dealer. 2020. *IACR ePrint Archive.* URL: https://eprint.iacr.org/2020/300.pdf

79. European Commission. Ethics Guidelines for Trustworthy AI. 2019. *EU Digital Strategy*. URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

80. European Commission. Proposal for a Council Decision on the signing, on behalf of the European Union, of the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, COM(2024) 264 final, 26.06.2024. *EUR-Lex. Access to European Union law.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52024PC0264

81. *European Data Protection Board (EDPB) :* [website]. URL: https://www.edpb.europa.eu/edpb_enEuropean Data Protection Board

82. Explaining decisions made with AI. 2020. *Information Commissioner's Office (ICO)*. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-ai/

83. Floridi L., Cowls J. A Unified Framework of Five Principles for AI in Society. *Harvard Data Science Review*. 2019. Issue 11. URL: https://hdsr.mitpress.mit.edu/pub/l0jsh9d1

84. Fredrikson M., Somesh J., Ristenpartet T. Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures. *CCS '15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security.* 2015. P. 1322–1333. URL: https://dl.acm.org/doi/10.1145/2810103.2813677

85. Generative AI and the EUDPR: Orientations for ensuring data protection compliance when using generative AI systems (Version 2). 2025. *European Data*

Protection Supervisor. URL: https://www.edps.europa.eu/system/files/2025-10/25-10_28_revised_genai_orientations_en.pdf

86. Generative Artificial Intelligence Profile. NIST AI 600-1. National Institute of Standards and Technology, 2024. 64 p. URL: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

87. Global Digital Compact. *United Nation*s. URL: https://www.un.org/global-digital-compact/en

88. Guidance on AI and data protection. 2023. *Information Commissioner's Office (ICO).* URL: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/

89. Guidelines on Artificial Intelligence and Data Protection. 2019. *Council of Europe.* URL: https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

90. Guidelines on Artificial Intelligence Governance in Ukraine. 2025. *EU4DigitalUA*. URL: https://eu4digitalua.eu/wp-content/uploads/2025/01/ai_guidelines_ua.pdf

91. Hachkevych A. Tools for adaptating Ukraine’s artificial intelligence ecosystem to meet European Union standards. *Law and Innovative Society*. 2024. No. 1 (22). P. 21–31. DOI: https://doi.org/10.37772/2309-9275-2024-1(22)-2

92. Hacker P., Engel A., Mauer M. Regulating ChatGPT and other Large Generative AI Models. *Computers and Society* (Chicago, June 12–15, 2023). Chicago, 2023. DOI: https://doi.org/10.48550/arXiv.2302.02337

93. Helberger N., Diakopoulos N. ChatGPT and the AI Act: Aligning AI Policymaking. *Virginia Journal of Law & Technology*. 2024. Vol. 27 (1). P. 1–30. URL: https://www.researchgate.net/publication/368908006_ChatGPT_and_the_AI_Act/

94. Holtz H. M., Ledendalb J. AI data governance: overlaps between the AI Act and the GDPR. *Law, Innovation and Technology.* 2025. P. 1–30. DOI: 10.1080/17579961.2026.2633677

95. Angeri, H. 2019. “Future of AI is Biological”. Towards Data Science. URL: https://towardsdata science.com/future-of-ai-is-biological-b512d6c40fe6 (дата звернення: 01.03.2023).

96. Interplay between the AI Act and the EU digital legislative framework, Study, PE 778.575, October 2025. *European Parliament.* URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778575/ECTI_STU%282025%29778575_EN.pdf

97. Italy fines OpenAI €15 million over privacy rules breach. *Reuters*. 2024. 20 December. URL: https://www.reuters.com/technology/italy-fines-openai-15-million-euros-over-privacy-rules-breach-2024-12-20/

98. Italy lifts ban on ChatGPT after data privacy improvements. *Deutsche Welle*. 2024. 29 April. URL: https://www.dw.com/en/ai-italy-lifts-ban-on-chatgpt-after-data-privacy-improvements/a-65469742

99. Khakhanovskyi V., Hrebenkova M. Identification, collection, and investigation of electronic imagery as sources of evidence. *Law Journal of the National Academy of Internal Affairs*. 2022. No. 12 (4). P. 28–39. DOI: 10.56215/04221204.28

100. Mittelstadt B. Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence.* 2019. No. 1. P. 501–507. URL: https://www.nature.com/articles/s42256-019-0114-4

101. Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+). *Council of Europe.* URL: https://rm.coe.int/1680afae3c

102. OECD Principles on Artificial Intelligence. *Organisation for Economic Co-operation and Development (OECD).* URL: https://www.oecd.org/en/topics/sub-issues/ai-principles.html

103. OECD. Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). *OECD Legal Instruments.* URL: https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449

104. Ohm P. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*. 2010. Vol. 57. P. 1701–1777. URL: https://www.uclalawreview.org/pdf/57-6-3.pdf

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

106. Opinion on the Draft Law of Ukraine «On Personal Data Protection» No. 8153 (as of 25 October 2022). 2023. *Council of Europe.* URL: https://rm.coe.int/opinion-on-the-draft-law-of-ukraine-on-personal-data-protection-/1680ad38c2

107. Pratik R. 2021. 'Artificial Intelligence: A Rising Star of Mobile Technology' URL: https://blog.intuz.com/artificial-intelligence-a-rising-star-of-mobile-technology/?utm_campaign=AI&utm_medium=Quora-ans&utm_source=Quora (дата звернення: 01.03.2023).

108. Privacy and Data Protection by Design. 2014. *ENISA*. URL: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

109. Privacy framework : ISO/IEC 29100:2011. *ISO – International Organization for Standardization*. URL: https://www.iso.org/standard/45123.html

110. Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. Version 1.0. 2020. *National Institute of Standards and Technology (NIST)*. URL: https://www.nist.gov/privacy-framework

111. Privacy Information Management : ISO/IEC 27701:2025. *ISO – International Organization for Standardization*. URL: https://www.iso.org/standard/27701

112. Protection of PII in public clouds : ISO/IEC 27018:2019. *ISO – International Organization for Standardization*. URL: https://www.iso.org/standard/76559.html

113. Rada supports draft law «On Personal Data Protection» in first reading. 2024. *EU4DigitalUA*. URL: https://eu4digitalua.eu/en/news/rada-supports-draft-law-on-personal-data-protection-in-first-reading/

114. Recommendation on the Ethics of Artificial Intelligence. SHS/BIO/REC-AIETHICS/2021. *UNESCO*. URL: https://unesdoc.unesco.org/ark:/48223/pf0000380455

115. Reddit sues AI company Anthropic over alleged data scraping. *Associated Press*. 2024. URL: https://apnews.com/article/f5ea042beb253a3f05a091e70531692d

116. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *EUR-Lex. Access to European Union law*. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

117. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32024R1689

118. Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act). *EUR-Lex. Access to European Union law*. URL: https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng

119. Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act). *EUR-Lex. Access to European Union law*. URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng

120. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance (Data Governance Act). *EUR-Lex. Access to European Union law*. URL: https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng

121. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828

(Data Act) (Text with EEA relevance). *EUR-Lex. Access to European Union law*. URL: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng

122. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *EUR-Lex. Access to European Union law.* URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

123. Resolution adopted by the General Assembly A/RES/76/179 «The right to privacy in the digital age». *United Nations*. URL: https://docs.un.org/en/A/RES/76/179.

124. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. 4th ed. Pearson, 2021. 1115 p. URL: https://aima.cs.berkeley.edu/

125. Schermer B. W., Custers B., van der Hof S. The crisis of consent: how stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology*. 2014. Vol. 16 (2). P. 171–182. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418

126. Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5). 2020. *National Institute of Standards and Technology (NIST)*. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

127. Shokri R. Membership Inference Attacks against Machine Learning Models. 2016. *arXiv.* URL: https://arxiv.org/abs/1610.05820.

128. Solove D. Artificial Intelligence and Privacy. *Florida Law Review*. 2024. Vol. 77. No. 1. P. 1–73. (Forthcoming). URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4713111

129. Taylor L. What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*. 2017. Vol. 4. No. 2. DOI: 10.1177/2053951717736335

130. The Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (information page). 2024. *Council of*

Europe. URL: https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

131. The Hamburg Commissioner for Data Protection and Freedom of Information Discussion Paper: Large Language Models and Personal Data. *Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit.* URL: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Discussion_Paper_Hamburg_DPA_KI_Models.pdf

132. The legal basis of legitimate interests: Focus sheet on measures to implement in case of data collection by web scraping. 2024. *Commission européenne pour l'informatique et les libertés (CNIL).* URL: https://www.cnil.fr/en/legal-basis-legitimate-interests-focus-sheet-measures-implement-case-data-collection-web-scraping

133. The Right to Privacy in the Digital Age. A/RES/76/179. 2021. *United Nations.* URL: https://documents.un.org/doc/undoc/gen/n21/363/15/pdf/n2136315.pdf

134. Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021. *DigiChina*. URL: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/

135. Wachter S., Mittelstadt B. A Right to Reasonable Inferences. Columbia Business Law Review, 2019. *SSRN eLibrary*. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829

136. Wachter S., Mittelstadt B., Russell C. Counterfactual explanations without opening the black box: Automated decisions and the GDPR. *Harvard Journal of Law and Technology.* 2018. No. 31 (2). URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063289

137. What Is Differential Privacy? *IEEE Digital Privacy Resource*. URL: https://digitalprivacy.ieee.org/publications/topics/what-is-differential-privacy/

138. White Paper on Artificial Intelligence. 2020. *European Commission*. URL: https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf

139. Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939- VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

140. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 5 жовт. 2017 р. № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text

141. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус : Закон України від 20 лист. 2012 р. № 5492-VI. URL: https://zakon.rada.gov.ua/laws/show/5492-17#Text

142. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 5 липн. 1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

143. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

144. Кодекс України про адміністративні правопорушення : Закон України від 7 груд. 1984 р. № 8073-X. URL: https://zakon.rada.gov.ua/laws/show/8073-10#Text

145. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

146. Цивільний кодекс України : Закон України від 16 січ. 2003 р. № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text

147. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025-2026 року : розпорядження Кабінету Міністрів України від 9 трав. 2025 р. № 457-р. URL: https://zakon.rada.gov.ua/laws/show/457-2025-р#Text

148. Про Єдиний державний реєстр призовників, військовозобов'язаних та резервістів : Закон України від 16 бер. 2017 р. № 1951-VIII. URL: https://zakon.rada.gov.ua/laws/show/1951-19#n50

149. Основи законодавства України про охорону здоров'я : Закон України від 19 лист. 1992 р. № 2801-XII. URL: https://zakon.rada.gov.ua/laws/show/2801-12#Text

150. Податковий кодекс України : Закон України від 2 груд. 2010 р. № 2755-VI. URL: https://zakon.rada.gov.ua/laws/show/2755-17#n1602

151. Про державну реєстрацію актів цивільного стану : Закон України від 1 лип. 2010 р. № 2398-VI. URL: https://zakon.rada.gov.ua/laws/show/2398-17#Text

152. Про Національну програму інформатизації : Закон України від 1 груд. 2022 р. № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text

153. Про публічні електронні реєстри : Закон України від 18 лист. 2021 р. № 1907-IX. URL: https://zakon.rada.gov.ua/laws/show/1907-20#Text

154. Про хмарні послуги : Закон України від 17 лют. 2022 р. № 2075-IX. URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text

155. Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних : постанова Кабінету Міністрів України від 21 жовт. 2015 р. № 835. URL: https://zakon.rada.gov.ua/laws/show/835-2015-п#Text

156. Виборчий кодекс України : Закон України від 19 груд. 2019 р. № 396-IX. URL: https://zakon.rada.gov.ua/laws/show/396-20#Text

157. Господарський процесуальний кодекс України : Закон України від 6 лист. 1991 р. № 1798-XII. URL: https://zakon.rada.gov.ua/laws/show/1798-12#Text

158. Кодекс адміністративного судочинства України : Закон України від 6 лип. 2005 р. № 2747-IV. URL: https://zakon.rada.gov.ua/laws/show/2747-15#Text

159. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

160. Кримінально-виконавчий кодекс України : Закон України від 11 лип. 2003 р. № 1129-IV. URL: https://zakon.rada.gov.ua/laws/show/1129-15#Text

161. Митний кодекс України : Закон України від 13 бер. 2012 р. № 4495-VI. URL: https://zakon.rada.gov.ua/laws/show/4495-17#Text

162. Сімейний кодекс України : Закон України від 10 січ. 2002 р. № 2947-III. URL: https://zakon.rada.gov.ua/laws/show/2947-14#Text

163. Цивільний процесуальний кодекс України : Закон України від 18 бер. 2004 р. № 1618-IV. URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text

164. Про електронні документи та електронний документообіг : Закон України від 22 трав. 2003 р. № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text

165. Про електронні комунікації : Закон України від 16 груд. 2020 р. № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text

166. Про Національну поліцію : Закон України від 2 лип. 2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

167. Про оперативно-розшукову діяльність : Закон України від 18 лют. 1992 р. № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text

168. Про Державний реєстр виборців : Закон України від 22 лют. 2007 р. № 698-V. URL: https://zakon.rada.gov.ua/laws/show/698-16#Text

169. Про медіа : Закон України від 13 груд. 2022 р. № 2849-IX. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text

170. Погорецький М. А. Використання даних EncroChat у кримінальному провадженні: порівняльно-правовий та процесуальний аналіз. *Юридичний науковий електронний журнал.* 2025. № 8. С. 223–229. DOI: https://doi.org/10.32782/2524-0374/2025-8

171. Погорецький М. А. Штучний інтелект у доказуванні в досудовому та судовому провадженнях: доктринальні засади і практика застосування. *Науковий вісник Ужгородського національного університету. Серія Право.* 2025. №91. Ч. 4. С. 398–418. DOI: https://doi.org/10.24144/2307-3322.2025.91.4.56

172. Погорецький М. А. Цифрові технології та докази у розслідуванні злочинів проти основ національної безпеки України: процесуальні проблеми та європейські стандарти. *Аналітично-порівняльне правознавство*. 2025. № 5. Ч. 3. С. 239–256. DOI: https://doi.org/10.24144/2788-6018.2025.05.3.37

ДОДАТКИ

Додаток А

Дані

анкетування 112 осіб – практичних працівників у сфе*рі правозастосування та цифрової безпеки з питань правової охорони і захисту персональних даних у сфері штучного інтелекту

№ з/п	Питання	Результати (у %)
1.	***Ваш стаж професійної діяльності:***	
	а) до 1 року	5,7
	б) від 1 до 3 років	16,5
	в) від 3 до 5 років	40,5
	г) від 5 до 10 років	29,7
	д) понад 10 років	7,6
2.	***Чи пов'язана Ваша професійна діяльність із питаннями захисту персональних даних?***	
	а) так, безпосередньо	35,7
	б) так, частково	14,5
	в) ні, але стикаюся з цими питаннями опосередковано	29,7
	г) ні, не пов'язана	20,1
3.	***Чи мали Ви практичний досвід роботи з технологіями штучного інтелекту або системами автоматизованої обробки даних?***	
	а) так, неодноразово	5,2
	б) так, поодинокі випадки	30,0
	в) безпосереднього досвіду не мав / не мала, але знайомий / знайома з проблематикою	45,6
	г) ні, не мав / не мала такого досвіду	15,7
	д) взагалі не цікаво	3,5
4.	***У якій сфері, на Вашу думку, питання захисту персональних даних при використанні ШІ є найбільш актуальним?***	
	а) правоохоронна діяльність	5,7
	б) кримінальне провадження	16,5
	в) державне управління та цифрові державні послуги	20,5
	г) банківська та фінансова сфера	10,7
	д) медицина	7,6
	е) трудові відносини та HR-аналітика	5,0

№ з/п	Питання	Результати (у %)
	є) відеоспостереження та біометрична ідентифікація	19,0
	ж) соціальні мережі та цифрові платформи	15,0
5.	***Чи вважаєте Ви, що чинне законодавство України достатньо регулює обробку персональних даних із використанням технологій штучного інтелекту?***	
	а) так, чинного регулювання достатньо	20,3
	б) частково, але існують окремі прогалини	24,8
	в) ні, законодавство потребує суттєвого оновлення	48,6
	г) важко відповісти	6,3
6.	***Які основні недоліки чинного законодавства України у сфері захисту персональних даних при використанні ШІ Ви вважаєте найбільш суттєвими?***	
	а) відсутність спеціального правового режиму обробки персональних даних у системах ШІ	30,3
	б) відсутність визначення інференційних персональних даних	25,2
	в) недостатнє регулювання автоматизованого прийняття рішень	6,4
	г) недостатнє регулювання профілювання особи	10,5
	д) відсутність чітких правил використання біометричних даних	2,8
	е) слабкий інституційний нагляд	10,0
	є) відсутність алгоритмічного аудиту	14,8
7.	***Чи потрібно у законодавстві України окремо закріпити правовий режим обробки персональних даних у системах штучного інтелекту?***	
	а) так, обов’язково	40,9
	б) так, але лише для високоризикових систем ШІ	25,1
	в) достатньо загальних норм про захист персональних даних	15,5
	г) ні, у цьому немає потреби	12,7
	д) важко відповісти	5,8
8.	***Чи вважаєте Ви доцільним розмежовувати правову охорону і правовий захист персональних даних у сфері ШІ?***	
	а) так, правова охорона має охоплювати превентивні гарантії до порушення права	21,4
	б) так, правовий захист має охоплювати засоби реагування після порушення або загрози порушення	22,8
	в) ні, ці поняття можна використовувати як тотожні	20,0

№ з/п	Питання	Результати (у %)
	г) так, якщо це істотно змінить ситуацію	19,5
	д) важко відповісти	16,3
9.	***Чи знайоме Вам поняття «інференційні персональні дані»?***	
	а) так, добре знайоме	33,7
	б) частково знайоме	50,4
	в) чув / чула, але не маю чіткого розуміння	12,1
	г) ні, не знайоме	3,8
10.	***Чи вважаєте Ви, що інференційні персональні дані потребують окремого правового регулювання?***	
	а) так, обов'язково	49,7
	б) так, але лише якщо вони істотно впливають на права особи	24,7
	в) ні, їх можна регулювати в межах загального поняття персональних даних	18,7
	г) важко відповісти	6,9
11.	***Які інференційні висновки можуть становити найбільший ризик для прав людини?***	
	а) оцінка кредитоспроможності	40,1
	б) прогноз поведінки особи	16,8
	в) оцінка професійної придатності	9,1
	г) висновки щодо стану здоров'я	16,7
	д) оцінка ризику вчинення правопорушення	5,0
	е) біометрична ідентифікація або класифікація	10,0
	є) соціальний скоринг	2,3
12.	***Чи вважаєте Ви профілювання особи за допомогою ШІ потенційно небезпечним для права на приватність?***	
	а) так, воно створює високі ризики	40,7
	б) так, але ризики залежать від сфери застосування	15,2
	в) ні, якщо є згода особи	24,8
	г) ні, не вбачаю суттєвих ризиків	11,8
	д) важко відповісти	7,5
13.	***Чи потрібно закріпити в законодавстві України право особи на пояснення автоматизованого рішення, прийнятого із використанням ШІ?***	
	а) так, обов'язково	32,7
	б) так, але лише якщо рішення має істотний вплив на права особи	26,4
	в) ні, достатньо права на доступ до персональних даних	21,2

№ з/п	Питання	Результати (у %)
	г) важко відповісти	19,7
14.	***Чи потрібно закріпити право особи на людське втручання або перегляд автоматизованого рішення людиною?***	
	а) так, у всіх випадках автоматизованого рішення	42,2
	б) так, лише щодо рішень із правовими або істотними наслідками	26,5
	в) ні, достатньо технічної перевірки системи	29,2
	г) важко відповісти	2,1
15.	***Яким має бути людське втручання у процес автоматизованого прийняття рішень?***	
	а) формальна перевірка результату алгоритму	21,4
	б) реальний аналіз рішення компетентною особою	42,3
	в) можливість змінити або скасувати автоматизоване рішення	8,2
	г) обов'язкове залучення незалежного експерта	26,1
	д) інше	2,0
16.	***Які види біометричної ідентифікації із використанням ШІ потребують найсуворішого правового контролю?***	
	а) розпізнавання обличчя	20,0
	б) розпізнавання ходи	10,3
	в) розпізнавання голосу	19,8
	г) поведінкова біометрія	13,1
	д) масове відеоспостереження з автоматичною ідентифікацією	12,4
	е) усі перелічені	24,4
17.	***Чи допустиме використання систем розпізнавання обличчя у публічних місцях?***	
	а) так, без обмежень, якщо це потрібно для безпеки	52,0
	б) так, але лише у чітко визначених законом випадках	16,6
	в) так, але тільки за рішенням суду або з дозволу незалежного органу	19,0
	г) ні, таке використання має бути заборонене	10,7
	д) важко відповісти	1,7
18.	***Які ризики використання біометричних ШІ-систем Ви вважаєте найбільш суттєвими?***	
	а) незаконне масове спостереження	15,2
	б) помилкова ідентифікація особи	15,5
	в) дискримінаційні помилки алгоритму	15,1

№ з/п	Питання	Результати (у %)
	г) витік біометричних даних	10,1
	д) використання даних не за первинною метою	18,2
	е) неможливість ефективного оскарження результату	11,9
	є) відсутність незалежного контролю	14,0
19.	***Чи підтримуєте Ви запровадження ризик-орієнтованого підходу до регулювання обробки персональних даних у системах ШІ?***	
	а) так, повністю підтримую	40,2
	б) скоріше підтримую	20,2
	в) скоріше не підтримую	9,5
	г) не підтримую	20,0
	д) важко відповісти	10,1
20.	***Які критерії мають визначати високоризикову обробку персональних даних із використанням ШІ?***	
	а) автономність системи	15,2
	б) масштабність обробки даних	12,7
	в) використання біометричних або чутливих даних	15,2
	г) профілювання особи	19,2
	д) формування інференційних висновків	6,0
	е) істотний вплив рішення на права людини	10,0
	є) непрозорість алгоритму	10,2
	ж) ризик дискримінації	10,2
	з) ризик повторної ідентифікації особи	1,3
21.	***Чи потрібно зробити обов'язковою оцінку впливу на захист персональних даних для високоризикових систем ШІ?***	
	а) так, обов'язково	19,4
	б) так, але лише у державному секторі	30,2
	в) так, але лише для великих приватних компаній	33,2
	г) ні, це має бути рекомендаційним інструментом	10,3
	д) важко відповісти	6,9
22.	***Чи потрібен в Україні обов'язковий алгоритмічний аудит високоризикових ШІ-систем?***	
	а) так, обов'язково	30,8
	б) так, але лише для державних систем	15,2
	в) так, але лише для систем, що обробляють біометричні або чутливі дані	20,2
	г) ні, достатньо внутрішнього контролю	22,9
	д) важко відповісти	10,9

№ з/п	Питання	Результати (у %)
23.	***Хто має нести відповідальність за порушення прав особи внаслідок обробки персональних даних ШІ-системою?***	
	а) розробник ШІ-системи	20,7
	б) постачальник ШІ-системи	22,5
	в) оператор / користувач ШІ-системи	15,1
	г) володілець персональних даних	5,2
	д) орган державної влади, який використовує систему	6,5
	е) усі суб'єкти залежно від їх ролі у життєвому циклі системи	30,0
24.	***Які напрями вдосконалення законодавства України у сфері захисту персональних даних при використанні ШІ Ви вважаєте найбільш актуальними?***	
	а) закріплення поняття інференційних персональних даних	12,0
	б) закріплення поняття високоризикової обробки персональних даних із використанням ШІ	15,0
	в) запровадження обов'язкової оцінки впливу на захист персональних даних	11,0
	г) законодавче закріплення права на пояснення автоматизованого рішення	6,8
	д) законодавче закріплення права на людське втручання	13,6
	е) спеціальне регулювання біометричної ідентифікації	10,1
	є) запровадження алгоритмічного аудиту	10,1
	ж) створення незалежного органу захисту персональних даних	11,2
	з) гармонізація законодавства України з GDPR та AI Act	10,2

Додаток Б

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

у яких опубліковано основні наукові результати дисертації:

1. Машталяр О. М. Проблеми використання штучного інтелекту під час оброблення персональних даних та напрями їх вирішення. *Юридичний науковий електронний журнал*. 2024. № 8. С. 256–259. DOI: 10.32782/2524-0374/2024-8/59

2. Машталяр О. М., Хахановський В. Г. Масове спостереження та розпізнавання обличчя за допомогою штучного інтелекту: правові виклики та перспективи регулювання в Україні. *Юридичний науковий електронний журнал*. 2024. № 11. С. 317–321. DOI: 10.32782/2524-0374/2024-11/72

3. Машталяр О. М. Розпізнавання ходи як інноваційний метод ідентифікації: аналіз можливостей, ризиків та нормативно-правового середовища в Україні. *Науковий вісник Ужгородського національного університету*. *Серія «Право».* 2025. Вип. 90, ч. 4. С. 310–317. DOI: 10.24144/2307-3322.2025.90.4.44

4. Машталяр О. М., Хахановський В. Г. Людський елемент у системах ШІ, що обробляють персональні дані: європейський стандарт і український дефіцит регулювання. *Юридичний науковий електронний журнал*. 2025. № 11. С. 160–163. DOI: 10.32782/2524-0374/2025-11/33

5. Машталяр О. М. Штучний інтелект і біометричні дані в кримінальному процесі України: допустимість, ризики, судовий контроль. *Науковий вісник Ужгородського національного університету*. *Серія «Право».* 2025. Вип. 92, ч. 3. С. 276–283. DOI: 10.24144/2307-3322.2025.92.3.37

6. Машталяр О. М., Петрик В. В. Персональні дані як електронний доказ у кримінальному процесі. *Юридичний науковий електронний журнал.* 2026. № 5. С. 218–221. DOI: 10.32782/2524-0374/2026-5/49

які засвідчують апробацію матеріалів дисертації:

1. Машталяр О. М. Масове відеоспостереження як інструмент забезпечення громадського порядку: переваги та загрози для прав людини в Україні. *Застосування інформаційних технологій у правоохоронній діяльності* : матеріали круглого столу (Харків, 14 груд. 2023 р.). Харків, 2023. С. 68–69.

2. Машталяр О. М., Хахановський В. Г. Правові аспекти захисту персональних даних при використанні технологій штучного інтелекту в експертній діяльності. *Science in the modern world: innovations and challenges* : за матеріалами XIII Міжнар. наук.-практ. конф. (Торонто, 7–9 серп. 2025 р.). Торонто, 2025. С. 254–263.

3. Машталяр О. М. Правові аспекти охорони персональних даних у період воєнного стану та трансформації системи безпеки в Україні. *Креативний простір.* 2025. № 30 : Креативна трансформація та модернізація сучасного суспільства : матеріали Міжнар. наук.-практ. конф. (Харків, 9–11 серп. 2025 р.). С. 9–11.

4. Машталяр О. М., Хахановський В. Г. Правові аспекти використання масового відеоспостереження в Україні: між потребами громадської безпеки та гарантіями прав людини. *Modern Science: Trends, Challenges, Solutions* : матеріали Міжнар. наук.-практ. конф. (Ліверпуль, 21–23 серп. 2025 р.). Ліверпуль, 2025. С. 301–305.

Додаток В

Акти впровадження

ЗАТВЕРДЖУЮ
Проректор Національної
академії внутрішніх справ
доктор юридичних наук, професор
полковник поліції
Сергій ЧЕРНЯВСЬКИЙ
03.11. 2025 року

АКТ

03.11. 2025 м. Київ № 502-ОП

Впровадження результатів дисертації Машталяра Олександра Михайловича на тему: «Правова охорона і захист персональних даних в сфері штучного інтелекту» в освітній процес НАВС

Уклала експертна комісія з виявлення, узагальнення та впровадження позитивного досвіду роботи у складі:

– начальника відділу організації освітнього процесу лейтенанта поліції Бойчук Вікторії Олександрівни;

– т.в.о. начальника відділу організації наукової діяльності, кандидата юридичних наук старшого лейтенанта поліції Горбенко Дар'ї Андріївни;

– завідувача кафедри інформаційних технологій Навчально-наукового інституту права та психології, кандидата фізико-математичних наук, доцента Кудінова Вадима Анатолійовича;

– завідувача кафедри кримінології та інформаційних технологій, доктора філософії права, доцента капітана поліції Школьнікова Владислава Ігоровича;

– начальника відділу аспірантури (ад'юнктури) і докторантури, доктора юридичних наук, професора підполковника поліції Тихонової Олени Вікторівни;

– завідувача загальної бібліотеки Гайдар Людмили Георгіївни.

Комісія розглянула й узагальнила матеріали дисертації, поданої на здобуття ступеня доктора філософії зі спеціальності 081 «Право», та наукові праці аспіранта денної форми навчання кафедри інформаційних технологій Навчально-наукового інституту права та психології Національної академії внутрішніх справ Машталяра Олександра Михайловича на тему: «Правова охорона і захист персональних даних в сфері штучного інтелекту».

Проаналізовано основні результати дослідження Машталяра О.М., зокрема наукові праці, в яких опубліковані теоретичні положення дисертації:

1. Машталяр О. М. Проблеми використання штучного інтелекту під час оброблення персональних даних та напрями їх вирішення. *Юридичний науковий електронний журнал*. 2024. № 8. С. 256-260. URL: http://www.lsej.org.ua/8_2024/61.pdf.
2. Хахановський В. Г., Машталяр О. М, Масове спостереження та розпізнавання обличчя за допомогою штучного інтелекту: правові виклики та перспективи регулювання в Україні. *Юридичний науковий електронний журнал*. 2024. № 11. С. 317-321. URL: http://lsej.org.ua/11_2024/74.pdf.

3. Машталяр О. М. Розпізнавання ходи як інноваційний метод ідентифікації: аналіз можливостей, ризиків і нормативно-правового середовища в Україні. *Науковий вісник Ужгородського національного університету «Право»*. 2025. № 90, ч. 4. С. 310-317. DOI: https://doi.org/10.24144/2307-3322.2025.90.4.44.

4. Машталяр О. М. Масове відеоспостереження як інструмент забезпечення громадського порядку: переваги та загрози для прав людини в Україні: за матеріалами круглого столу: «*Застосування інформаційних технологій у правоохоронній діяльності*» (м. Харків, Україна). 12.12.2024. С. 68-69.

5. Машталяр О. М. Правові аспекти охорони персональних даних у період воєнного стану та трансформації системи безпеки в Україні. *Науковий журнал «Креативний простір». 2025. № 30*: за матеріалами науково-практичної конференції «Креативна трансформація та модернізація сучасного суспільства». С. 9-10. URL: https://www.newroute.org.ua/wp-content/uploads/crp_30.pdf.

6. Машталяр О. М. Правові аспекти захисту персональних даних при використанні технологій штучного інтелекту в експертній діяльності. *Science in the modern world: innovations and challenges*: за матеріалами XIII Міжнародної науково-практичної конференції (м. Торонто, Канада). 09.08.2025. С. 254-263. URL: https://sci-conf.com.ua/wp-content/uploads/2025/08/SCIENCE-IN-THE-MODERN-WORLD-INNOVATIONS-AND-CHALLENGES-7-9.08.25.pdf.

7. Машталяр О. М. Правові аспекти використання масового відеоспостереження в Україні: між потребами громадської безпеки та гарантіями прав людини. *Modern science: trends, challenges, solutions*: за матеріалами I Міжнародної науково-практичної конференції (м. Ліверпуль, Великобританія). 23.08.2025. С. 301-304. URL: https://sci-conf.com.ua/wp-content/uploads/2025/08/MODERN-SCIENCE-TRENDS-CHALLENGES-SOLUTIONS-21-23.08.25.pdf.

На основі проведеного аналізу комісія зробила висновок, що праці Машталяра О.М., містять науково обґрунтовані теоретичні положення і практичні рекомендації, що дає підстави запровадити їх для використання в освітньому процесі Національної академії внутрішніх справ, зокрема при викладанні навчальних дисциплін «Інформаційні технології та системи», «Застосування інформаційних технологій в правоохоронній діяльності», «Аналіз та прогнозування злочинності» під час підготовки навчально-методичних та дидактичних матеріалів, а також рекомендувати їх до вивчення під час самостійної роботи здобувачів вищої освіти.

Члени комісії:

Вікторія БОЙЧУК

Дар'я ГОРБЕНКО

Вадим КУДІНОВ

Владислав ШКОЛЬНІКОВ

Олена ТИХОНОВА

Людмила ГАЙДАР

ЗАТВЕРДЖУЮ
Проректор
Національної академії
внутрішніх справ,
доктор юридичних наук, професор
полковник поліції
Олег ТАРАСЕНКО
03 11 2025 року

АКТ

03.11.2025 м. Київ № 501-нд

Впровадження результатів дисертації Машталяра Олександра Михайловича на тему: «Правова охорона і захист персональних даних в сфері штучного інтелекту» в наукову діяльність НАВС

Уклала експертна комісія з виявлення, узагальнення та впровадження позитивного досвіду роботи у складі:

– т.в.о. начальника відділу організації наукової діяльності, кандидата юридичних наук старшого лейтенанта поліції Горбенко Дар'ї Андріївни;

– завідувача кафедри інформаційних технологій Навчально-наукового інституту права та психології, кандидата фізико-математичних наук, доцента Кудінова Вадима Анатолійовича;

– завідувача кафедри кримінології та інформаційних технологій, доктора філософії права, доцента капітана поліції Школьнікова Владислава Ігоровича;

– начальника відділу аспірантури (ад'юнктури) і докторантури, доктора юридичних наук, професора підполковника поліції Тихонової Олени Вікторівни;

– завідувача загальної бібліотеки Гайдар Людмили Георгіївни.

Комісія розглянула й узагальнила матеріали дисертації, поданої на здобуття ступеня доктора філософії зі спеціальності 081 «Право», наукові праці аспіранта денної форми навчання кафедри інформаційних технологій Навчально-наукового інституту права та психології Національної академії внутрішніх справ Машталяра Олександра Михайловича на тему: «Правова охорона і захист персональних даних в сфері штучного інтелекту» та на основі проведеного аналізу зробила висновок, що надана робота містить низку обгрунтованих теоретичних положень і пропозицій спрямованих на удосконалення нормативно-правового регулювання захисту персональних даних у сфері штучного інтелекту, підвищення ефективності правового механізму їх охорони та запровадження дієвих методів протидії порушенням у цій галузі.

Проаналізовано основні результати дослідження Машталяра О.М., зокрема наукові праці, в яких опубліковані теоретичні положення дисертації:

1. Машталяр О. М. Проблеми використання штучного інтелекту під час оброблення персональних даних та напрями їх вирішення. *Юридичний науковий електронний журнал*. 2024. № 8. С. 256-260. URL: http://www.lsej.org.ua/8_2024/61.pdf.
2. Хахановський В. Г., Машталяр О. М. Масове спостереження та розпізнавання

обличчя за допомогою штучного інтелекту: правові виклики та перспективи регулювання в Україні. *Юридичний науковий електронний журнал.* 2024. № 11. С. 317-321. URL: http://lsej.org.ua/11_2024/74.pdf.

3. Машталяр О. М. Розпізнавання ходи як інноваційний метод ідентифікації: аналіз можливостей, ризиків і нормативно-правового середовища в Україні. *Науковий вісник Ужгородського національного університету «Право»*. 2025. № 90, ч. 4. С. 310-317. DOI: https://doi.org/10.24144/2307-3322.2025.90.4.44.

4. Машталяр О. М. Масове відеоспостереження як інструмент забезпечення громадського порядку: переваги та загрози для прав людини в Україні: за матеріалами круглого столу: «*Застосування інформаційних технологій у правоохоронній діяльності*» (м. Харків, Україна). 12.12.2024. С. 68-69.

5. Машталяр О. М. Правові аспекти охорони персональних даних у період воєнного стану та трансформації системи безпеки в Україні. *Науковий журнал «Креативний простір». 2025. № 30*: за матеріалами науково-практичної конференції «Креативна трансформація та модернізація сучасного суспільства». С. 9-10. URL: https://www.newroute.org.ua/wp-content/uploads/crp_30.pdf.

6. Машталяр О. М. Правові аспекти захисту персональних даних при використанні технологій штучного інтелекту в експертній діяльності. *Science in the modern world: innovations and challenges*: за матеріалами XIII Міжнародної науково-практичної конференції (м. Торонто, Канада). 09.08.2025. С. 254-263. URL: https://sci-conf.com.ua/wp-content/uploads/2025/08/SCIENCE-IN-THE-MODERN-WORLD-INNOVATIONS-AND-CHALLENGES-7-9.08.25.pdf.

7. Машталяр О. М. Правові аспекти використання масового відеоспостереження в Україні: між потребами громадської безпеки та гарантіями прав людини. *Modern science: trends, challenges, solutions*: за матеріалами I Міжнародної науково-практичної конференції (м. Ліверпуль, Великобританія). 23.08.2025. С. 301-304. URL: https://sci-conf.com.ua/wp-content/uploads/2025/08/MODERN-SCIENCE-TRENDS-CHALLENGES-SOLUTIONS-21-23.08.25.pdf.

На основі проведеного аналізу комісія зробила висновок про те, що вищезазначені матеріали дисертаційного дослідження Машталяра О.М. на тему: «Правова охорона і захист персональних даних в сфері штучного інтелекту» застосовуються під час підготовки монографій, підручників, навчальних посібників, методичних рекомендацій, узагальнення аналітичних матеріалів, обгрунтування пропозицій до чинних проєктів нормативно-правових актів, підготовка яких потребує проведення відповідних наукових досліджень або містить наукову складову.

Члени комісії:

Дар'я ГОРБЕНКО

Вадим КУДІНОВ

Владислав ШКОЛЬНІКОВ

Олена ТИХОНОВА

Людмила ГАЙДАР

НАЦІОНАЛЬНА АСОЦІАЦІЯ
АДВОКАТІВ УКРАЇНИ
РАДА АДВОКАТІВ
КИЇВСЬКОЇ ОБЛАСТІ

UKRAINIAN NATIONAL
BAR ASSOCIATION
KYIV REGIONAL
BAR COUNCIL

код за ЄДРПОУ 38536488
04080, м. Київ, вул. Кирилівська, 15
тел: +38 (050) 732-27-73
email: info@radako.com.ua, веб-сайт: www.radako.com.ua

USREOU 38536488
15 Kyrylivs'ka Street, Kyiv, 04080 Ukraine
phone: +38 (050) 732-27-73
email: info@radako.com.ua, web-site: www.radako.com.ua

Вих. № 1885,0,2,25
від 30 12 2025 р.

ЗАТВЕРДЖУЮ

Голова
Ради адвокатів Київської області
Петро БОЙКО

«30» грудня 2025 р.

АКТ
про впровадження результатів дисертаційного дослідження Машталяра О.М. у діяльність Ради адвокатів Київської області

Комісія у складі: Голови Ради адвокатів Київської області **Бойка П.А.;** секретаря Ради адвокатів Київської області **Демидюк О.Б.;** склала цей Акт про те, що комісією розглянуто результати дисертаційного дослідження Машталяра О.М.. на тему «Правова охорона і захист персональних даних в сфері штучного інтелекту» на здобуття наукового ступеня доктора філософії в галузі знань 08 «Право» за спеціальністю 081 «Право».

За результатами проведеного аналізу Комісія дійшла висновку, що дисертаційне дослідження має комплексний і системний характер, вирізняється науковою ґрунтовністю та високим рівнем актуальності й присвячене всебічному дослідженню проблем правової охорони та захисту персональних даних у процесах використання технологій штучного інтелекту. Запропоновані автором наукові положення та висновки, спрямовані на вдосконалення національного законодавства і правозастосовної практики у сфері обробки персональних даних, забезпечення балансу між інноваційним розвитком ШІ та гарантіями прав і свобод людини, посилення механізмів правового контролю й відповідальності за

порушення у цій сфері, є науково виваженими та мають суттєву практичну цінність.

Висновки та рекомендації наукових публікацій щодо правових режимів обробки персональних даних із використанням штучного інтелекту, гарантій захисту приватності, вимог до прозорості та безпеки алгоритмічних систем, а також удосконалення механізмів нагляду і правового захисту суб'єктів персональних даних можуть бути використані у науково-методичних розробках, що здійснюються Радою адвокатів Київської області. Зазначені напрацювання можуть слугувати теоретичною й практичною основою для підготовки аналітичних матеріалів, рекомендацій у сфері правової політики, а також навчально-методичних матеріалів для адвокатів.

Положення та висновки дисертаційного дослідження є науково обґрунтованими та застосовуються у науково-дослідній діяльності як підґрунтя для подальших досліджень у сфері захисту персональних даних і правового регулювання використання штучного інтелекту. У практичній діяльності Ради адвокатів Київської області результати дослідження враховані та використовуються в роботі.

Загальний висновок: результати дисертаційного дослідження Машталяра О.М. є актуальними, мають виражену практичну спрямованість і можуть бути рекомендовані адвокатам для практичного застосування під час надання правової допомоги, зокрема у справах, пов'язаних із захистом персональних даних та використанням технологій штучного інтелекту.

Голова
Ради адвокатів
Київської області _____ **Петро БОЙКО**

Секретар
Ради адвокатів
Київської області _____ **Ольга ДЕМИДЮК**

АДВОКАТСЬКЕ БЮРО «ОЛЕКСАНДР БАЙДИК ТА ПАРТНЕРИ»

Код ЄДРПОУ: 41368123
адреса: 02072, м. Київ,
просп. М.Бажана 16, оф.233
тел. +38 (066)-177-51-96,
+38 (067)-552-62-84
email: 3531575@gmail.com

LAW FIRM «OLEKSANDR BAIDYK&PARTNERS»

USREOU code: 41368123
adress: 02072, Ukraine, Kyiv,
M.Bazshana ave. 16, of.233
phone +38 (066)-177-51-96,
+38 (067)-552-62-84
email: 3531575@gmail.com

АКТ
про впровадження результатів дисертаційного дослідження МАШТАЛЯРА Олександра Михайловича у практичну діяльність адвокатського бюро

АДВОКАТСЬКЕ БЮРО «ОЛЕКСАНДР БАЙДИК ТА ПАРТНЕРИ», код ЄДРПОУ: 41368123, в особі Керуючого БАЙДИКА Олександра Анатолійовича, склало цей Акт про те, що результати дисертаційного дослідження Машталяра Олександра Михайловича на тему «Правова охорона і захист персональних даних у сфері штучного інтелекту», поданого на здобуття наукового ступеня доктора філософії в галузі знань 08 «Право» за спеціальністю 081 «Право», були розглянуті та враховані у практичній діяльності адвокатського бюро.

За результатами опрацювання дисертаційного дослідження встановлено, що робота має цілісний і прикладний характер, вирізняється актуальністю та спрямована на розв'язання практичних проблем правового регулювання оброблення персональних даних із застосуванням технологій штучного інтелекту. У дисертації всебічно проаналізовано правові ризики автоматизованого прийняття рішень, використання біометричних даних та алгоритмічного профілювання, а також обґрунтовано процесуальні й матеріально-правові гарантії забезпечення прав суб'єктів персональних даних.

Обґрунтовані автором висновки та пропозиції щодо дотримання принципів законності, пропорційності та прозорості під час оброблення персональних даних у системах штучного інтелекту, посилення судового й адвокатського контролю за застосуванням відповідних технологій, а також удосконалення механізмів правового захисту фізичних осіб, мають істотне значення для практики адвокатської діяльності.

Матеріали та результати дисертаційного дослідження використовуються у діяльності адвокатського бюро, зокрема:

- під час надання правничої допомоги у справах, що стосуються оброблення персональних і біометричних даних;
- при формуванні правових позицій, підготовці процесуальних документів та правових висновків щодо правомірності використання технологій штучного інтелекту;
- у консультативній роботі з питань дотримання вимог національного законодавства та міжнародних стандартів у сфері захисту персональних даних;
- при розробленні внутрішніх методичних і аналітичних матеріалів для адвокатів бюро.

Положення та висновки дисертації застосовуються у поточній практичній діяльності адвокатів адвокатського бюро як науково обґрунтована основа для формування правових позицій і підвищення якості надання правничої допомоги у справах, пов'язаних із використанням цифрових технологій та штучного інтелекту.

Результати дисертаційного дослідження МАШТАЛЯРА Олександра Михайловича на тему «Правова охорона і захист персональних даних у сфері штучного інтелекту» є актуальними, науково обґрунтованими, мають практичну спрямованість і впроваджені у діяльність адвокатського бюро.

КЕРУЮЧИЙ
АБ «ОЛЕКСАНДР БАЙДИК ТА ПАРТНЕРИ» _____
Олександр БАЙДИК

01.12.2025

АДВОКАТСЬКЕ БЮРО «ВЛАДИСЛАВА ШИПОШІ»
Україна, 02072, місто Київ, проспект Бажана Миколи, будинок 16, офіс 233, кабінет 7
Код ЄДРПОУ: 45350811

АКТ
про впровадження результатів дисертаційного дослідження
МАШТАЛЯРА Олександра Михайловича у практичну діяльність адвокатського бюро

АДВОКАТСЬКЕ БЮРО «ВЛАДИСЛАВА ШИПОШІ», код ЄДРПОУ: 45350811, в особі Керуючого бюро ШИПОШІ Владислава Миколайовича, склало цей Акт про те, що було розглянуто результати дисертаційного дослідження МАШТАЛЯРА Олександра Михайловича на тему «Правова охорона і захист персональних даних в сфері штучного інтелекту» на здобуття наукового ступеня доктора філософії в галузі знань 08 «Право» за спеціальністю 081 «Право» та впроваджено у практичну діяльність адвокатського бюро.

У ході аналізу дисертаційного дослідження встановлено, що робота має комплексний, системний та прикладний характер, відзначається актуальністю та спрямованістю на вирішення практичних проблем правового регулювання оброблення персональних даних із використанням технологій штучного інтелекту. У дисертації ґрунтовно досліджено правові ризики автоматизованого прийняття рішень, використання біометричних даних, алгоритмічного профілювання, а також визначено процесуальні та матеріально-правові гарантії захисту прав суб'єктів персональних даних.

Сформульовані автором висновки та пропозиції щодо необхідності забезпечення законності, пропорційності та прозорості оброблення персональних даних у системах штучного інтелекту, посилення судового та адвокатського контролю за використанням таких технологій, а також удосконалення механізмів правового захисту фізичних осіб, мають істотну практичну цінність для адвокатської діяльності.

Результати дисертаційного дослідження впроваджені у практичну діяльність адвокатського бюро, зокрема:

- під час надання правничої допомоги клієнтам у справах, пов'язаних із обробленням персональних та біометричних даних;
- при підготовці правових позицій, процесуальних документів та правових висновків щодо законності використання технологій штучного інтелекту;
- у консультативній діяльності з питань дотримання вимог законодавства України та міжнародних стандартів у сфері захисту персональних даних.

Положення та висновки дисертації використовуються у практичній роботі адвокатського бюро як науково обґрунтована база для формування правових позицій та підвищення якості правничої допомоги у справах, пов'язаних із цифровими технологіями та штучним інтелектом.

Результати дисертаційного дослідження МАШТАЛЯРА Олександра Михайловича на тему «Правова охорона і захист персональних даних в сфері штучного інтелекту» є актуальними, науково обґрунтованими, мають прикладну спрямованість та впроваджені у практичну діяльність адвокатського бюро.

КЕРУЮЧИЙ
АБ «ВЛАДИСЛАВА ШИПОШІ» _____ **Владислав ШИПОША**
21.11.2025