THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE RIGHT TO PRIVACY: THEORETICAL BASIS FOR BALANCING INTERESTS

ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА ПРАВО НА ПРИВАТНІСТЬ: ТЕОРЕТИЧНІ ЗАСАДИ БАЛАНСУ ІНТЕРЕСІВ

Svitlana Kravchuk[1]

DOI: https://doi.org/10.30525/978-9934-26-651-5-18

Abstract. In a world where AI is becoming the invisible architect of social processes, the classic human right to privacy is undergoing a fundamental revision. This study is devoted to a critical analysis of how algorithms capable of predicting behavior and analyzing the smallest digital traces are blurring the traditional boundaries of personal space. The central problem of the work is the search for a "golden mean" – a fragile balance between technological progress, security requirements, and the inviolability of the human right to privacy. The study reveals a paradox: in the pursuit of public benefit and security through AI monitoring, we risk creating an environment where the right to anonymity becomes an inaccessible luxury. Using comparative analysis and legal modeling, the work offers not only a theoretical rethinking of human rights, but also practical guidelines for future legislation that should protect individuals from algorithmic determinism without hindering the innovative development of civilization. The aim of the study is to conduct a theoretical and legal analysis of the transformation of the content of the right to privacy under the influence of AI technologies and to identify optimal legal mechanisms for achieving a balance between the private interests of individuals and the public interests of the state and society in the digital age. The work uses a set of general scientific and special methods of cognition. The dialectical method allowed

[1] Doctor of Philosophy of Law, Associate Professor,
Associate Professor of Department of Law,
Higher Educational Institution
"Academician Yuriy Bugay International and Scientific Technical University", Ukraine

us to consider the right to privacy in its development and contradictions with technological progress. The systemic-structural method was used to analyze the components of information privacy. The comparative legal method was used to compare international standards (GDPR, EU AI Act) with national legislation. It has been proven that the traditional understanding of privacy as "the right to be left alone" is insufficient in the context of total algorithmization. The need to transition to the concept of "information self-determination" has been substantiated, where the object of protection will be not only data, but also predictions and conclusions generated by AI about a person. The main points of conflict have been identified: predictive justice, biometric identification, and algorithmic profiling. The scientific value of the study lies in deepening knowledge about the subjective human right to privacy in the digital environment. The author proposes his own definition of "algorithmic privacy" and formulates theoretical approaches to resolving conflicts between the right to privacy and society's right to security and technological development. The work supplements human rights theory with new aspects of protection against unauthorized cognitive and behavioral influence of algorithms. The conclusions can be used in lawmaking when developing regulatory acts on AI regulation in Ukraine; in law enforcement practice to protect citizens' rights in disputes related to automated data processing; and in the educational process when teaching the disciplines "Theory of State and Law," "Information Law," and the course "Human Rights."

1. Вступ

Нинішнє суспільство дедалі більше залежить від цифрових технологій та штучного інтелекту (далі – ШІ), які активно проникають у всі сфери життя – від медицини й освіти до економіки та державного управління. Разом з очевидними перевагами, такими як автоматизація процесів, підвищення ефективності та персоналізація послуг, виникає низка серйозних викликів, зокрема в сфері дотримання прав людини. Одним із найвразливіших прав у цифрову епоху є право на приватність та безпеку. Масовий збір, зберігання та аналіз персональних даних за допомогою алгоритмів ШІ створює нові ризики для конфіденційності. Особливе занепокоєння викликає те, що великі обсяги даних можуть використовуватися без належного інформування або згоди

особи, а також потенційно застосовуватись для дискримінаційних або маніпулятивних цілей. Наприклад, технології розпізнавання облич, відстеження поведінки користувачів у мережі, аналіз біометричних даних – усе це істотно змінює саму природу приватності як правового та етичного поняття [1, с. 176].

У зв'язку з цим актуалізується питання правового регулювання: чи встигає чинне законодавство за технічним прогресом? Чи достатньо існуючих механізмів для ефективного захисту персональних даних? Умови цифрової епохи вимагають переосмислення підходів до захисту приватності, оновлення правових норм, а також впровадження етичних стандартів у розробці й використанні ШІ.

Таким чином, необхідно не лише усвідомити масштаби проблеми, але й проаналізувати, наскільки правові механізм и в сучасному цифровому світі здатні захистити особисте життя людини в умовах, коли інформація стала новою формою влади.

У сучасному цифровому суспільстві ШІ активно використовується для обробки великих обсягів персональних даних, зокрема, ШІ здатен створювати детальні профілі користувачів, що може призводити до дискримінації та порушення конфіденційності [2].

Європейський Союз впровадив Загальний регламент захисту даних (GDPR) та Закон про штучний інтелект (AI Act), які спрямовані на регулювання використання ШІ та захист персональних даних. Проте дослідники вказують на наявність суперечностей між цими нормативними актами, зокрема щодо принципу мінімізації даних та вимог до якості даних для навчання ШІ [3].

Крім того, існують технічні та етичні виклики, пов'язані з використанням ШІ для оцінки політик конфіденційності. Наприклад, складність та довжина таких політик можуть призводити до «втоми від згоди» у користувачів, що ускладнює їхню здатність приймати обґрунтовані та виважені рішення щодо своїх даних [4].

Таким чином, існує потреба ретельного дослідження ефективності правових механізмів захисту персональних даних у контексті розвитку ШІ та масового збору даних.

Метою дослідження є комплексний аналіз впливу штучного інтелекту на право на приватність у контексті масового збору даних, а також критична оцінка ефективності чинних правових механізмів

захисту персональних даних у цифрову епоху. У межах цієї мети були об'єднані кілька ключових напрямів аналізу: зокрема, визначення основних викликів, які виникають при застосуванні ШІ з точки зору приватності; дослідження взаємодії Загального регламенту про захист даних (GDPR) та Акту про штучний інтелект (AI Act) у сфері правового регулювання; розгляд технічних та етичних аспектів, пов'язаних із використанням ШІ для обробки персональної інформації; а також формування рекомендацій щодо вдосконалення нормативної бази з метою забезпечення ефективного захисту права на приватність в умовах технологічного прогресу.

2. «Природа» загрози приватності та конфіденційності від ШІ. Прозорість та цінність даних

До сьогодні більшість популярних підходів до безпеки та підзвітності ШІ зосереджувались на технологічних характеристиках і ризиках систем штучного інтелекту, уникаючи уваги до працівників, які стоять за лаштунками – тих, хто проєктує, впроваджує, тестує та обслуговує ці системи. Зусилля на кшталт Закону ЄС про ШІ уособлюють цей підхід, оскільки вони визначають регуляторний нагляд за технічними ознаками, як-от обсяг обчислювальних потужностей, використаних для навчання або налаштування моделі ШІ. Так само й система відповідальності за продукцію фокусується на небезпечних характеристиках продукту та применшує поведінку людських рішень. Інші пропозиції, як-от сувора відповідальність або аналогії «сентиєнтного» ШІ до дітей чи диких тварин, так само уникають аналізу людських процесів створення ШІ. Такий технократичний фокус дозволяє інженерам ШІ дистанціюватися від шкоди, яку вони завдають іншим [5].

Штучний інтелект (ШІ) – це галузь інформатики, яка прагне створити програми, здатні виконувати завдання, які зазвичай потребують людського інтелекту. Це може бути розпізнавання голосу чи зображень, навчання, прийняття рішень або аналіз даних. ШІ – це загальний термін Він охоплює технології, як-от машинне навчання, аналіз прогнозів, обробку природної мови та робототехніку.

ШІ вже давно вивчається – ще з часів Лейбніца в XVIII столітті, а сучасне розуміння зародилося в 1940-х роках, зокрема завдяки «тесту Тюрінга». Сьогодні розвиток ШІ відбувається особливо

швидко через потужні комп'ютери, великі обсяги даних і вдосконалені алгоритми.

Ми часто використовуємо ШІ, навіть не помічаючи цього. Наприклад, коли нам радять фільми або відповідає автоматизований голос, це приклади звичного, «повсякденного» ШІ. Після того як якась технологія працює добре, її вже не вважають «інтелектом», а просто частиною звичайного цифрового досвіду. Особливу популярність отримав ChatGPT. З кожним роком ШІ стає дедалі потужнішим, доступнішим і поширенішим [6].

Розглянемо життєві переваги для людини користування ШІ. Першою чергою – швидкість. ШІ здатен обробляти величезну кількість інформації за лічені секунди. Він може дати відповідь на майже будь-яке запитання або навчити чомусь новому. Другою – точність. Штучний інтелект не робить помилок у розрахунках – йому допомагають спеціальні формули та алгоритми. Він може розв'язати складні задачі, прокласти маршрут, передбачити погоду або відповісти на логічну загадку. Третьою – ефективність. Четвертою – творчість. Недоліки – неточність (не ідеальність рішень) неправильне розуміння спричинення людської залежності, відсутність людського підходу [7].

Розглянемо типи ШІ. Вузький ШІ (Harrow AI) – найпоширеніший. Він спеціалізується лише на одній задачі. Наприклад, комп'ютер Deep Blue вміє грати в шахи краще за людину, але не може робити нічого іншого. Такий інтелект покликаний допомогти людині, а не замінити її. Загальний ШІ (General AI) – це система, яка здатна розв'язувати задачі в різних галузях, як це робить людина. Вона може вчитися новому досвіду й адаптуватися до змін. Надінтелект (Superintelligence) – це гіпотетична форма ШІ, що перевершує найкращих людей у всьому: науці, етиці, спілкуванні.

Розглянемо зв'язок Big Data з ШІ. Великі дані – це величезні обсяги інформації, які постійно створюються нашими діями: перегляд сайтів, листування, користування смартфоном. Зібрані дані є джерелом навчання для ШІ дозволяє їх обробляти та виявляти в них закономірності, які людина могла б не помітити. Без великих даних ШІ не зміг би стати настільки потужним.

Дослідимо машинне навчання і глибоке навчання. Машинне навчання (Machine Learning) – це процес, під час якого комп'ютер

«вчиться» самостійно, без чіткого програмування. Якщо йому дати достатньо прикладів, він може розпізнавати шаблони та приймати рішення. Є два основні типи: 1. Supervised Learning (контрольоване навчання) – комп'ютеру дають і дані, і правильні відповіді, щоб він навчився встановлювати залежності; Unsupervised Learning (неконтрольоване навчання) – комп'ютер сам шукає закономірності в даних без підказок. Глибоке навчання (Deep Learning) – це підвид машинного навчання, який працює через «нейронні мережі», подібні до людського мозку. Але насправді ці системи не думають як люди. Вони просто передають дані через багато рівнів, на кожному з яких обчислення стають складнішими. Це ускладнює розуміння того, як саме був зроблений висновок – виникає так званий «ефект чорної скриньки».

З науково-технічної точки зору, штучний інтелект є напрямом у сфері комп'ютерних наук, який має на меті створення систем, здатних самостійно обробляти інформацію, розпізнавати образи, працювати з природною мовою та приймати рішення на основі заданих критеріїв. Простіше кажучи, це технології, які дозволяють комп'ютерам і програмам діяти з певною схожістю до людського мислення [8].

Натомість із юридичного погляду сформулювати чітке визначення ШІ значно складніше. Через динамічний розвиток технологій, законодавство має постійно адаптуватися, щоб відповідати новим викликам, які виникають у процесі впровадження і використання систем штучного інтелекту [9].

У цифрову епоху персональні дані стали ключовим ресурсом, що використовується для різноманітних цілей. Однак це також призвело до нових загроз для приватності, включаючи капіталізм спостереження, алгоритмічну упередженість, втрату автономії та ризики безпеки даних.

ШІ працює завдяки обробці великих обсягів даних, які дозволяють йому розуміти потреби користувачів і виконувати певні завдання. Ці дані можуть надходити як з відкритих джерел які були утворені внаслідок усвідомленої передачі інформації людиною. А також – з неусвідомлених джерел, коли ШІ збирає інформацію без відома людини, наприклад, через системи розпізнавання облич.

Через наявність таких механізмів виникає втрата контролю над приватною інформацією. Навіть прості додатки, як-от умовна про-

грама «Знайди моє авто», що допомагає користувачам знаходити свою машину за допомогою фото з геолокацією, можуть створювати ризики для конфіденційності. Зображення можуть ненавмисно включати інших людей, а інформація про місця паркування – бути використана страховими компаніями чи зберігатися довше, ніж очікує користувач. Наступний приклад – відеодзвінки з функцією розпізнавання облич. Хоча їх мета – впізнавання членів родини чи постійних гостей, ці пристрої можуть мимоволі записувати інших людей. Це створює занепокоєння та породжує питання про доступ до даних правоохоронців [10].

ШІ вже використовується урядом у різних сферах. Наприклад, чатботи консультують громадян, автоматизовані системи допомагають з пошуком документів або перекладом. У перспективі ШІ може кардинально змінити роботу державних органів, зробити її ефективнішою та доступнішою для громадян.

Законодавство про конфіденційність, зокрема принципи ОЕСР, було створене ще в 1980-х роках, коли основними обробниками даних були люди. Тепер, коли рішення приймає ШІ, це створює зовсім нові виклики. Хоч ШІ може допомогти збереженню конфіденційності (наприклад, обробляючи дані без участі людини), є і ризики – непрозорі алгоритми, можливість упереджених рішень, надмірне стеження, обман користувачів через «людяність» цифрових помічників. ШІ також здатен створювати унікальні проблеми. Він аналізує. Навчається адаптується та прогнозує поведінку. Алгоритми ШІ часто створюються на основі людських даних, тому легко можуть повторювати або посилювати дискримінаційні упередження. Комбінування старих технологій з ШІ (наприклад, відеокамер з розпізнаванням облич) може перетворити безпечні інструменти на загрозу приватності. Люди довіряють машинам, які говорять людськими голосами, наче це справжні особи – і тому можуть передавати більше приватної інформації, ніж є потреба. Потужні компанії мають перевагу в зборі та використанні даних, а звичайні люди часто не розуміють, як їхня інформація використовується, і не можуть реально її контролювати. Загалом, як навмисне, так і ненавмисне збирання даних штучним інтелектом створює серйозні проблеми щодо приватності. Завдяки алгоритмам машинного навчання компанії можуть аналізувати поведінку клієнтів, поділяти їх на групи за демографічними, поведінковими чи психографічними

ознаками (характер цінності, інтереси) і надсилати точкові пропозиції. Проте така деталізація може передбачати чи розкривати чутливу інформацію – наприклад, політичні погляди чи сексуальну орієнтацію. Бренди прагнуть адаптувати досвід клієнтів під індивідуальні запити, але надмірна персоналізація може викликати негативну реакцію. Так, Urban Outfitters зазнали критики за автоматичне визначення статі користувача без його згоди. Особливо складним стає це питання у зв'язку з появою DeepFakes – технології створення фальшивого мультимедійного контенту. Ці інструменти можуть бути використані для шантажу або онлайн-насилля, що створює серйозні виклики для захисту приватності. ШІ-технології, зокрема чат-боти, активно застосовуються у сфері підтримки клієнтів. Наприклад, McDonald's впровадили голосового помічника в системі drive-thru. Проте згодом компанія була звинувачена в порушенні конфіденційності через запис голосу без згоди. Це ще раз підкреслює необхідність прозорості у використанні таких технологій та дотримання законодавства, як-от GDPR.

Компанії мають чітко пояснювати, яку вигоду користувач отримає в обмін на свої дані. Багато людей готові ділитися інформацією, якщо це приносить їм користь – покращений досвід, персоналізовані пропозиції чи можливість керувати налаштуваннями приватності. Замість моделі «увімкнено / вимкнено», користувачам варто запропонувати спектр варіантів персоналізації – від повної відмови до глибокої адаптації з інтеграцією сторонніх даних. Це дозволить краще враховувати індивідуальні потреби в балансі між приватністю та персоналізованим досвідом.

Federated Learning (федеративне навчання) – це новітній підхід, за якого дані не передаються на центральний сервер. Замість цього навчання ШІ відбувається локально (наприклад, на смартфоні), а оновлення передаються централізовано. Це дозволяє системі навчатися без безпосереднього збору персональної інформації. Прикладом такої технології є клавіатура Google, яка навчається на основі поведінки користувачів без передачі особистих даних [10].

З розвитком новітніх технологій зростають не лише можливості, а й ризики, пов'язані з їх використанням. Зокрема, інструменти збору та аналізу даних, які дозволяють створювати ефективні системи ШІ, одночасно збільшують імовірність порушення конфіденційності. Особливе

занепокоєння викликає те, як ШІ використовує чутливу інформацію для навчання та вдосконалення моделей. Регулятори намагаються реагувати на ці виклики, створюючи нормативні рамки, але це породжує додаткові труднощі для компаній у сфері відповідності вимогам [11].

Технології штучного інтелекту значною мірою залежать від персональних даних, що робить конфіденційність даних важливою юридичною проблемою в цифрову епоху. Розуміння важливості конфіденційності даних має вирішальне значення для окремих осіб людини, так і організацій.

ШІ створює різні правові проблеми конфіденційності, включаючи несанкціоноване використання даних, проблеми з біометричними даними, прихований збір даних та алгоритмічну упередженість. Вони можуть мати значні наслідки для прав людини та суспільства.

Реальні випадки дотримання вимог ШІ та проблем конфіденційності, такі як витоки даних, системи спостереження та упереджена практика найму, підкреслюють нагальну потребу в регулюванні та відповідальному управлінні даними під час використання ШІ. Штучний інтелект змінює те, як людина живе та працює. Однак ця трансформація несе з собою нові виклики, особливо в сфері конфіденційності даних. Конфіденційність даних є важливою цінністю в нашому все більш цифровому світі. Витік даних та крадіжка особистих даних є поширеними загрозами. Наслідки виходять далеко за рамки фінансових втрат, завдаючи тривалої шкоди репутації та емоційному благополуччю. Організації, які надають пріоритет конфіденційності даних, демонструють свою відданість захисту конфіденційної інформації. Це не лише підвищує підзвітність, але й зміцнює довіру в споживачів. Запровадивши прозору політику використання даних, проводячи регулярні аудити та впроваджуючи надійні заходи безпеки, організації можуть зменшити ризики та створити безпечніше цифрове середовище. Цей проактивний підхід заохочує споживачів впевнено ділитися своїми особистими даними.

Технології штучного інтелекту істотно залежать від особистих даних, використовуючи їх для таких процесів, як збір даних, машинне навчання та прогностичні алгоритми. Ці системи можуть аналізувати закономірності та приймати рішення, які впливають на все: від персоналізованих рекомендацій до фінансових оцінок. Однак таке

широке використання даних також порушує важливі етичні та юридичні питання, скажімо як використовуються наші дані, хто має до них доступ і які можуть бути довгострокові наслідки для нашої конфіденційності та автономії. Оскільки ці інтелектуальні системи накопичують величезні обсяги інформації від користувачів, вони використовують передові методи машинного навчання для виявлення тенденцій та поведінки, які можуть бути не відразу очевидними. Генеративні програми штучного інтелекту розширюють цю можливість, імітуючи реальні сценарії, що дозволяє проводити прогнозну аналітику, яка може спрямовувати майбутні дії. Виникає критична потреба балансу інновацій з етичними міркуваннями та побудова позитивного права. Це не запевнить того що зі стрімким розвитком технологій права особи будуть надійно захищені, проте сприятиме більш довірливим стосункам між користувачами та штучним інтелектом. Впровадження етичних практик штучного інтелекту та зосередження на дотриманні нормативних вимог можуть допомогти пом'якшити правові ризики.

Нині важливо вдосконалити існуючу політику конфіденційності, запровадивши суворіші правила використання даних та забезпечивши повну інформованість користувачів про те, як використовується їхня інформація. Забезпечення чіткіших механізмів згоди та надійних процесів видалення даних може надати людям повноваження та відновити їхній контроль над особистою інформацією. Це особливо важливо в контексті великих технологічних компаній, які обробляють величезні обсяги персональних даних.

3. Технологічні виклики ШІ для приватної сфери та правове регулювання

Оскільки системи спостереження стають все більш поширеними, використання біометричних даних, таких як відбитки пальців, розпізнавання обличчя та сканування райдужної оболонки ока, викликає серйозні проблеми конфіденційності. На відміну від паролів, біометричні дані є постійними, і якщо їх скомпрометувати, їх не можна змінити. Це робить їх головною мішенню для крадіжки особистих даних та інших форм зловживання. З розширенням цих технологій як ніколи важливо враховувати, як збирається, зберігається та захищається біометрична інформація.

Інтеграція біометричних даних у програми штучного інтелекту створює значні етичні дилеми. Наприклад, хоча технологія розпізнавання облич може посилити заходи безпеки, вона часто працює без явної згоди осіб, що призводить до необґрунтованого спостереження. У ситуаціях, коли ці дані зламуються або використовуються неналежним чином, наприклад, під час несанкціонованого доступу до особистих облікових записів або створення дипфейків, негативні наслідки для прав людини можуть бути серйозними. Помітним прикладом є витік біометричної інформації з урядової бази даних, що зробило громадян вразливими до крадіжки особистих даних та шахрайства. Крім того, розгортання таких технологій правоохоронними органами може призвести до значних проблем із правами людини [12].

Приватність у ШІ означає захист особистих або чутливих даних, які збираються, використовуються або зберігаються системами штучного інтелекту. Це поняття тісно пов'язане з приватністю даних – правом особи контролювати, як її дані використовуються, хто має до них доступ, і з якою метою.

Колись приватність асоціювалась переважно з онлайн-покупками. Проте зараз дані масово використовуються для навчання ШІ – часто без явної згоди людини, що створює ризики порушенню її основних прав.

Надання доступу до відкритих даних без дозволу може призводити до серйозних правових наслідків. Наприклад у 2023 році The New York Times подала до суду на OpenAI та Microsoft за незаконне використання авторських матеріалів для навчання ШІ [2]. У тому ж році Google став об'єктом колективного позову за порушення конфіденційності та авторських прав у зв'язку з навчанням моделі Gemini [3]. А ще у 2018 році випадок із Cambridge Analytica продемонстрував ризики неправомірного використання персональних даних користувачів Facebook у політичних цілях.

Загалом, ШІ-системи використовують відкриті дані без належної згоди, що порушує принцип прозорості. Правове врегулювання подібних випадків має зосереджуватись на аспектах власності, безпеки, прозорості та контролю за обробкою даних.

ШІ стає рушієм перегляду правових підходів, адже його здатність збирати різнорідні дані виводить його за межі одного правового поля. Уряд України інтегрує ці технології у публічну сферу, наприклад,

створивши цифрову дипломатичну аватарку на основі реальної особи у 2024 році [10]. Проте це піднімає нові ризики – згода на використання зображення (біометрії), ризик створення фейкових аватарів та дезінформації. Саме тому передбачено маркування таких аватарів QR-кодами.

Іншим прикладом впровадження ШІ є система біометричної ідентифікації за допомогою технології відстеження погляду під час читання. Ай-трекінг несе ризики порушення конфіденційності через глибокий аналіз поведінки.

Водночас, зростає і зворотна загроза – використання ШІ для створення фейкових зображень та інформаційних атак. Наприклад, у 2023 році зображення фейкового вибуху біля Пентагону призвело до фінансових потрясінь [8], а у США виборча кампанія 2024 року супроводжується хвилею дезінформації. Незважаючи на існування Закону про захист виборців від оманливого ШІ, технології розвиваються швидше, ніж механізми їх правового регулювання [13].

Дезінформація шкодить не лише довірі до держави, а й стабільності економіки. Водночас визнано, що судове реагування на фейки є малоефективним у динамічному цифровому середовищі. Альтернативою стає технологічне маркування ШІ-контенту, як це вже впроваджено у Facebook чи Instagram.

Підвищення ефективності правового регулювання передбачає маркування та сертифікацію ШІ-систем, класифікацію за рівнями ризику, як це реалізовано в Акті ЄС про ШІ. Відповідно до нього, технології поділяються на: заборонені (неприйнятний ризик), суворо регульовані (високий ризик), з обмеженнями (обмежений ризик), дозволені без особливих вимог (мінімальний ризик).

Ключові принципи – етика, прозорість, гнучкість та безпека, з особливою увагою до захисту конфіденційності. Персональні дані є одним із ключових елементів ШІ-систем, тому мають бути надійно захищені згідно з міжнародними та національними актами. Так, Рекомендації ЮНЕСКО щодо етики ШІ 2021 року закріплюють низку вимог – прозорість, належний захист, відповідальність, видалення ПД, узгодженість із GDPR та незалежний нагляд.

Україна, впроваджуючи ці стандарти, розробила Дорожню карту з регулювання ШІ, що включає «регуляторну пісочницю», добровільне

маркування, Білу книгу, кодекси поведінки тощо. Проте впровадження ускладнене через війну, нестачу ресурсів і швидкі зміни у цифровому середовищі.

На міжнародному рівні подібні ініціативи, як-от африканська дорожня карта ШІ, демонструють різні акценти: для України – оборонний сектор і євроінтеграція, для Африки – боротьба з бідністю і розвиток.

Це свідчить про трансформаційний потенціал ШІ не лише в особистому, але й у глобальному вимірі. Правовий захист персональних даних дедалі частіше закріплюється в юридично обов'язкових документах. Наприклад, у ЄС законодавство визначає ШІ як «машинну систему, яка діє з різним рівнем автономності, здатна адаптуватися після запуску, і яка на основі вхідних даних формує результати – прогнози, контент, рекомендації чи рішення».

Такий підхід підкреслює складність ШІ та його взаємодію з різними правовими режимами, що створює правову невизначеність. Це пояснює потребу в міжгалузевому та гнучкому підході до регулювання.

У Білий книзі Мінцифри вказується, що ШІ повинен регулюватися через наявне галузеве законодавство. [14]. Отже, вдосконалення чинного права повинно стати головним напрямом правового реагування на виклики цифрової епохи [15].

Ці інциденти підкреслюють нагальну потребу в надійних заходах захисту даних, оскільки безліч людей виявляють, що їхня конфіденційна інформація була скомпрометована. Яскравим прикладом є порушення безпеки у 2021 році, яке сталося у відомій медичній організації, що працює на базі штучного інтелекту, коли стався несанкціонований доступ до особистих медичних записів мільйонів людей. Це порушення не лише поставило під загрозу конфіденційність пацієнтів, але й підірвало довіру до цифрових медичних послуг.

Компанії зіткнулися з негативною реакцією з боку регуляторних органів, що спонукало до впровадження суворіших рекомендацій щодо захисту даних та підвищення прозорості. Оскільки ці порушення тривають, діалог щодо етичного використання штучного інтелекту та його наслідків для конфіденційності стає все більш важливим.

Зростаюча роль штучного інтелекту в спостереженні та правоохоронних органах викликала запеклі дебати щодо конфіденційності та

етики. Оскільки ці технології стають все більш поширеними, вони ставлять серйозні питання щодо балансу між безпекою та особистими свободами.

Ця зростаюча залежність від інструментів спостереження на базі штучного інтелекту викликає важливі питання про те, наскільки суспільство готове ставити безпеку на перше місце у порівнянні з особистими свободами. Оскільки правоохоронні органи інтегрують ці інноваційні технології для моніторингу, побоювання щодо необґрунтованого стеження та потенційного зловживання даними стають дедалі вираженішими. Відсутність прозорості навколо алгоритмів штучного інтелекту ускладнює етичний ландшафт, порушуючи питання щодо відповідальності у випадках порушень або упереджень. Досягнення балансу між потребою безпеки та імперативом захисту прав людини сприяє складному діалогу щодо наслідків використання таких передових інструментів у поліцейській діяльності.

Штучний інтелект у практиці найму та його етичні наслідки

Роль штучного інтелекту в практиці найму має різні етичні наслідки, які заслуговують на наукову увагу, зокрема, побоювання щодо дискримінації та алгоритмічної упередженості, які можуть суттєво вплинути на справедливе ставлення до шукачів роботи.

Оскільки організації все більше покладаються на автоматизовані системи для перевірки кандидатів та оцінки резюме, ризик увічнення існуючих упереджень через ці технології стає критичним питанням. Наприклад, алгоритми, які аналізують історичні дані про найм, можуть ненавмисно надавати перевагу кандидатам, які відповідають певному профілю, потенційно виключаючи кваліфікованих осіб з різним досвідом.

Щоб ефективно долати ці виклики, компанії необхідно юридично зобов'язати впроваджувати прозорі алгоритми найму, проводити регулярні аудити своїх систем на наявність упереджень та сприяти інклюзивним даним навчання, які охоплюють широкий спектр досвіду та точок зору. Проактивний підхід може допомогти створити справедливіший ландшафт найму, водночас не перешкоджаючи використанню ефективності, яку забезпечують сучпільству технології ШІ [11].

Розглянемо чинні нормативні акти, які впливають на штучний інтелект та конфіденційність даних. Такі нормативні акти, як GDPR, вста-

новлюють високі стандарти щодо того, як системи штучного інтелекту обробляють персональні дані, з особливим акцентом на захист прав особистої конфіденційності. Для компаній, які використовують штучний інтелект, це означає не лише дотримання вимог, але й проактивне захищення конфіденційності людей, яким вони служать. Ці правила вимагають від організацій впровадження надійних заходів захисту даних, а також глибокого розуміння того, як штучний інтелект взаємодіє з персональними даними. Нинішнє людство повинне долати такі труднощі, як різні тлумачення законів у різних юрисдикціях, потенційні значні штрафи за недотримання вимог та постійна потреба моніторингу систем ШІ. Крім того, механізми правозастосування, такі як аудити та штрафи, які накладаються регуляторними органами, повинні створювати середовище, де дотримання вимог є важливим не формально, але й таким що вибудовує атмосферу довіри громадськості та гарантує права людини.

Майбутні тенденції в законодавстві про конфіденційність даних, ймовірно, будуть зосереджені на посиленні дотримання нормативних вимог у міру розвитку технологій штучного інтелекту. Водночас це вимагатиме посилених заходів захисту даних та надійніших рамок для регулювання використання даних. Оскільки штучний інтелект продовжує інтегруватися в різні аспекти повсякденного життя, зростає визнання необхідності комплексних правил конфіденційності. Зацікавлені сторони, включаючи уряди та технологічні компанії, можуть дедалі більше співпрацювати над стандартизованими протоколами для встановлення чітких меж для збору та використання даних. Очікується, що міжнародна співпраця зростатиме, сприяючи створенню середовища, де транскордонна передача даних може відбуватися з більшою впевненістю в правовому захисті.

Поява нових стандартів конфіденційності також може вирішити унікальні проблеми, що виникають через штучний інтелект, гарантуючи, що люди збережуть контроль над своєю особистою інформацією, отримуючи при цьому переваги від технологічного прогресу. Впровадження найкращих практик захисту конфіденційності в застосунках штучного інтелекту полягає у чітких гарантіях того, що завжди буде надаватися пріоритет саме управлінню даними. Дотримуючись такого принципу можна формувати довіру людини до нових техно-

логій. Впровадження найкращих практик може включати навчання співробітників питанням захисту даних та визначенню чітких ролей та обов'язків у рамках управління даними. Вирішальну роль у формуванні культури підзвітності та забезпеченні того, щоб ці політики не лише впроваджувалися, а й активно застосовувалися відіграє керівництво. Впровадження принципів конфіденційності на етапі розробки в додатках штучного інтелекту служить проактивним підходом до захисту даних, забезпечуючи інтеграцію питань конфіденційності в життєвий цикл розробки технологій. Впроваджуючи ці принципово важливі віхи з самого початку, можна виявити потенційні ризики на ранній стадії процесу та ефективно їх пом'якшити. Цей стратегічний крок не лише сприяє довірі споживачів, але й покращує дотримання правил, створюючи систему, яка надає пріоритет безпеці та конфіденційності користувачів. Організації, що застосовують підхід, орієнтований на конфіденційність, можуть оптимізувати робочі процеси, зменшити витрати, пов'язані з витоками даних, та створити конкурентну перевагу на ринку. Зрештою, цей підхід призводить до більш відповідальних інновацій, оскільки зацікавлені сторони стають дедалі уважнішими до етичних наслідків рішень на основі штучного інтелекту.

Підвищення прозорості використання даних є життєво важливим для організацій, що використовують штучний інтелект, оскільки це сприяє підзвітності та формує довіру з користувачами щодо того, як обробляються їхні персональні дані.

Для досягнення цього важливо впровадити чіткі політики конфіденційності, які дозволять користувачам легко розуміти практики та процедури вашої організації. Встановлення надійних механізмів отримання згоди користувачів гарантує, що люди знають і погоджуються з тим, як їхні дані будуть використовуватися.

Регулярна звітність про практику використання даних підкріплює це зобов'язання, надаючи користувачам уявлення про те, як обробляється їхня інформація. Навчання користувачів щодо їхніх прав на дані дає їм можливість контролювати свою особисту інформацію, що зрештою зміцнює стосунки між вашою організацією та її клієнтами.

Саме людина відіграєте вирішальну роль у захисті конфіденційності в цифрову епоху. Розуміння того, як використовуються персональні дані, механізмів згоди на конфіденційність, дає кожному

змогу вживати проактивні заходи для захисту власної цифрової конфіденційності.

Щоб ефективно захистити свої дані, кожен зобов'язаний регулярно переглядати налаштування конфіденційності на своїх платформах соціальних мереж, бути обережним з угодами про згоду та використовувати інструменти конфіденційності для захисту особистої інформації.

Нині кожен має можливість використання віртуальної приватної мережі (VPN) для шифрування інтернет-з'єднання, що ускладнить відстеження онлайн-активності для третіх осіб. Проте необхідно врахувати ризики. Також важливо ознайомитися з останніми політиками конфіденційності та законами про захист даних, щоб повністю зрозуміти кожному свої права та використовувати їх обмірковано та з розумінням.

Захищаючи посилення прав на конфіденційність та підтримуючи законодавство, яке посилює цей захист, кожен може відіграти життєво важливу роль у широкому русі за права споживачів. Інформованість про потенційні ризики та розуміння доступних інструментів дає усвідомлену змогу контролювати свій цифровий слід та мінімізувати ризики витоків даних.

4. Правова детермінація балансу між технологічними інноваціями ШІ та режимом конфіденційності персональних даних

Перспективи на майбутнє щодо балансування інновацій у сфері штучного інтелекту та конфіденційності даних залежать від впровадження етичних практик та заходів підзвітності у сфері штучного інтелекту. Ці підходи повинні ефективно вирішувати проблеми конфіденційності, одночасно сприяючи технологічному прогресу. Існує об'єктивна потреба необхідності постійної обізнаності та адаптації. Адже технології штучного інтелекту розвиваються, все більше інтегруються в повсякденне життя. Кожна сучасна людина повинна розуміти свої права та обов'язки щодо персональних даних.

Сучасна відповідність вимогам виходить за рамки дотримання стандартів – вона стосується управління реальними ризиками. Приймаючи підхід «ризик понад усе», організації можуть відійти від «відповід-

ності контрольним спискам» та створити практики, які забезпечують довгострокову безпеку та зростання. Такий підхід сприяє стійкій системі безпеки, де сертифікати стають доказом ефективного управління ризиками, а не кінцевою метою.

Оскільки штучний інтелект продовжує розвиватися, балансування інновацій із конфіденційністю даних вимагатиме співпраці між підприємствами, політиками та окремими особами. Прозорі практики обробки даних, суворі правила та зосередженість на підзвітності є ключовими для забезпечення того, щоб технологічний прогрес підтримував, а не ставить під загрозу конфіденційність.

Деякі з ризиків включають неправильне використання персональних даних, алгоритмічне упередження та можливість злому або маніпулювання технологією. Крім того, системи ШІ не завжди можуть бути прозорими у тому, як вони приймають рішення, що ускладнює для людей розуміння та контроль використання їхніх даних.

Оскільки ШІ продовжує розвиватися та все більше інтегруватися в наше повсякденне життя, закони та нормативні акти щодо конфіденційності даних необхідно адаптувати, щоб забезпечити захист персональних даних. Це включає вирішення таких питань, як право власності на дані, згода та право бути забутим.

Важливо, щоб правотворці виступали за суворіші закони про конфіденційність даних.

В Україні вже здійснено певні кроки у напрямі правового регулювання ШІ. Зокрема, у 2020 році була затверджена Концепція розвитку штучного інтелекту, яка вперше на законодавчому рівні визначає, що саме вважати штучним інтелектом, а також формулює основні принципи та цілі державної політики у цій сфері. Відповідно до цього документу, ШІ розглядається як система інформаційних технологій, що здатна самостійно вирішувати складні завдання, використовуючи алгоритми, бази знань та методи обробки даних, включаючи ті, які система генерує самостійно під час роботи.

Додатково, Національна асоціація адвокатів України створила спеціальну Робочу групу, яка займається питаннями правового регулювання ШІ. Ця група зосереджена на аналізі правових ризиків, захисті персональних даних, формуванні рамок допустимого використання таких систем у різних галузях та напрацюванні стандартів,

що мають забезпечити дотримання прав людини при впровадженні ШІ в практику.

На рівні Європейського Союзу спостерігається схожа тенденція – розробка нормативної бази, яка поєднує технологічний розвиток із дотриманням етичних та правових принципів. Основна мета ЄС полягає у формуванні довіри до систем ШІ шляхом створення відповідального, безпечного і правового підходу до їх використання. Починаючи з 2021 року, в ЄС триває вдосконалення одного з перших у світі комплексних нормативних актів, присвячених регулюванню штучного інтелекту – Artificial Intelligence Act (Акт про ШІ). Існує системне визначення ШІ на рівні законодавства ЄС. Зокрема зазначено, що система штучного інтелекту – це машинна система, яка може діяти з різним рівнем автономності та створювати результати (наприклад, рішення, рекомендації або прогнози), що мають вплив на реальний чи віртуальний світ.

У контексті практичного застосування означених норм виникає багато запитань для держав, розробників технологій і кінцевих користувачів. Найважливіше питання – невпинний пошук балансу між розвитком інновацій і дотриманням фундаментальних прав, зокрема права на приватність.

Проведемо аналіз міжнародних нормативних актів, які регулюють використання ШІ. GDPR (Загальний регламент захисту даних ЄС) [16] встановлює суворі вимоги до обробки персональних даних, включаючи використання ШІ. Наприклад, стаття 22 надає суб'єктам даних право не підлягати рішенням, що ґрунтуються виключно на автоматизованій обробці (включаючи профілювання), які мають юридичні або подібні значні наслідки. CCPA (Закон Каліфорнії про захист прав споживачів) [17] прямо не згадує ШІ, проте охоплює автоматизовані процеси, які використовуються, наприклад, для профілювання споживачів або прийняття рішень щодо них. Закон гарантує право знати, які персональні дані збираються, і право заборонити їх продаж. Guidelines on Artificial Intelligence and Data Protection [18] – це перші обов'язкові міжнародні інструменти, які враховують ризики, пов'язані з алгоритмами та ШІ. Це прозорість, справедливість та недискримінація при використанні автоматизованої обробки. AI Act [19] пропонує ризик-орієнтований підхід і розділяє системи ШІ на 4 рівні: неприйнятний ризик – забо-

ронено (наприклад, соціальний рейтинг); високий ризик – дозволено лише за умови дотримання вимог щодо безпеки, прозорості, управління ризиками; обмежений ризик – вимагає інформування користувача (наприклад, чат-боти); мінімальний ризик – не регулюється. Роль DPO (Data Protection Officer) – слідкує за дотриманням законодавства щодо обробки персональних даних, зокрема при впровадженні ШІ. Він координує оцінку впливу, прозорість систем, забезпечує зв'язок між технічними командами і наглядовими органами [20].

Розглянемо права суб'єкта даних. GDPR гарантує такі права: доступ до своїх даних; право на видалення (право бути забутим); виправлення даних; обмеження обробки; заперечення проти обробки; право не підпадати під автоматизоване рішення [16].

Суб'єктами юридичної відповідальності за ШІ нині є розробник – за помилки або дискримінацію, вбудовану в алгоритм; оператор / користувач – за спосіб застосування ШІ; компанія – як юридична особа; сама система ШІ (наразі юридично не несе відповідальності але на майбутнє така відповідальність не може виключатись). Крок у цьому напрямку зроблено в законопроєкті штату Каліфорнія щодо безпеки ШІ, який передбачає, що розробники ШІ повинні визначати й впроваджувати протоколи, які втілюють «обов'язок розробника виявляти розумну обережність, аби уникнути створення моделей, що становлять надмірний ризик спричинення або сприяння критичній шкоді». Хоча технологічні лідери виступають проти цього закону, судам не потрібно чекати законодавства, щоб дозволити позови про недбалість проти розробників ШІ [5].

У чинному законодавстві України немає чітко визначеного переліку видів обробки персональних даних, які потребують обов'язкової оцінки впливу на захист даних (DPIA). Проте європейські стандарти, на які орієнтується Україна, такий перелік містять. Наприклад, у статті 35(3) Загального регламенту про захист даних (GDPR) [16] визначено, що DPIA є обов'язковим у випадках: а) масове й систематичне профілювання осіб, яке здійснюється автоматизовано й впливає на людей з юридичної або іншої значущої точки зору; б) масштабна обробка спеціальних категорій персональних даних, таких як дані про здоров'я, біометричні або кримінальні записи; в) систематичне спостереження у публічних місцях, наприклад, відеомоніторинг

у громадських просторах. Також робоча група з захисту даних ЄС надала додаткові орієнтири, за якими обробка вважається високоризиковою. Це зокрема: використання новітніх технологій, як-от штучний інтелект; ситуації, коли витік даних може загрожувати життю чи здоров'ю; обробка даних дітей або здійснення геолокаційного стеження; автоматизоване ухвалення рішень без втручання людини. Європейське законодавство також регламентує ризик-орієнтований підхід для великих онлайн-платформ (VLOP) та пошуковиків (VLSE) з аудиторією понад 45 млн користувачів. Вони мають щорічно оцінювати ризики негативного впливу своїх сервісів, зокрема в частині поширення незаконного контенту або загроз правам людини. Наприклад, Google та Meta вже впровадили певні зміни у свої політики для дотримання цих вимог.

Навіть якщо обробка даних ШІ не потрапляє до категорії високого ризику, регулятори у багатьох країнах ЄС радять все одно проводити оцінювання ризиків, адже через стрімкий розвиток технологій не завжди зрозуміло, які саме наслідки вони можуть мати для людей.

Оцінка ризиків має відбуватись у кілька етапів: спершу аналізується загальний напрямок обробки даних, далі визначається мета аналізу, розробляється методологія, адаптована під конкретну діяльність або технологію, після чого здійснюється безпосередня оцінка. Для підвищення якості цього процесу доцільно залучати зовнішніх фахівців. Такий підхід не лише підвищує безпеку, але й може стати перевагою для бізнесу [21, с. 32-33].

Проєктування систем захисту персональних даних у сфері штучного інтелекту повинно базуватись на чіткому розумінні прав людини та дотриманні вимог законодавства. Кожна людина має право володіти своїми персональними даними та контролювати їх обробку. Зокрема, вона має право: знати звідки зібрані її дані, де вони зберігаються, для чого обробляються, а також де знаходиться власник чи розпорядник цих даних; отримувати інформацію про те, хто має доступ до її персональних даних, у тому числі – хто з третіх осіб їх отримує; мати доступ до власних даних; отримувати відповідь про обробку своїх даних не пізніше ніж за 30 днів після звернення, включаючи зміст таких даних; висловлювати заперечення проти обробки своїх даних; вимагати змінити або видалити свої дані, якщо вони обробляються незаконно або

є неправдивими; захищати свої дані від незаконної обробки, випадкової втрати чи пошкодження, а також від поширення недостовірної або такої, що шкодить репутації, інформації; оскаржувати обробку своїх даних до Уповноваженого з прав людини чи суду; застосовувати правові механізми у випадку порушення законодавства про захист даних; встановлювати обмеження на обробку своїх даних ще під час надання згоди; мати можливість відкликати згоду на обробку персональних даних; знати, як працює автоматична обробка даних; захищатися від автоматизованих рішень, які можуть мати для неї правові наслідки.

Право на інформацію та доступ до персональних даних означає, що кожна людина має можливість дізнатися, чи обробляє якась організація її персональні дані, які саме це дані, хто їх отримує, з якою метою, скільки часу вони зберігаються тощо. Запит на доступ має бути виконаний безкоштовно та без зволікань, окрім випадків, передбачених законом. Це може бути, наприклад, надання копій анкет чи інших документів, де фігурує особа. Якщо задовольнити запит складно, про це потрібно повідомити та запропонувати альтернативи. Для цього важливо ще на етапі створення ІТ-системи впроваджувати принципи приватності за замовчуванням і за дизайном.

Право на видалення (або «право бути забутим») передбачає, що особа може вимагати видалення своїх персональних даних, якщо вони обробляються незаконно, застаріли або більше не потрібні. Це право також передбачено в GDPR. У випадку зі штучним інтелектом необхідно передбачити технічні можливості для видалення або анонімізації даних, не порушуючи при цьому роботу системи.

Право на захист від автоматизованого ухвалення рішень дає змогу людині не погоджуватися з рішенням, яке прийняте виключно машиною (наприклад, програмою чи алгоритмом), якщо воно має значний вплив на неї. Такі рішення мають бути прозорими, зрозумілими та контрольованими людиною. Важливо забезпечити можливість втручання людини, пояснення логіки рішень, можливість оскарження та захист від дискримінаційних рішень. Наприклад, якщо система зробила помилку або прийняла рішення через змішані дані, має бути механізм перевірки та виправлення.

Крім того, варто враховувати інші ризики, приміром автоматичне упередження, коли люди надто покладаються на ШІ, або неможливість

пояснення, коли рішення ШІ важко інтерпретувати. Для запобігання цим ризикам слід впроваджувати політики контролю, навчати персонал та створювати умови для людського перегляду рішень.

5. Висновки

Штучний інтелект відіграє дедалі вагомішу роль у сучасному суспільстві, проте його розвиток тісно пов'язаний із масовим збором персональних даних, що ставить під загрозу право на приватність. ШІ має багато переваг – може підвищити ефективність, зменшити витрати, покращити медицину та транспорт. Але водночас виникають виклики – як для прав людини, так і для суспільства людства загалом. Необхідно розробити нові етичні та правові рамки для захисту приватності в умовах цифрової трансформації.

Підсумовуючи можемо дати авторське визначення алгоритмічної приватності, яке охоплює не лише «дані», а й «процеси». Алгоритмічна приватність – це правовий режим захисту особистості від несанкціонованого профайлювання та автоматизованого прийняття рішень, що базуються на прихованих закономірностях цифрового сліду особи. Водночас це стан захищеності цифрового образу людини від інтерпретації системами штучного інтелекту, що забезпечує право особи залишатися непередбачуваною та вільною від алгоритмічного детермінізму. А в технічному сенсі – це це право на контроль не лише над первинними персональними даними, а й над похідними висновками (інференціями), які генеруються ШІ-системами щодо вподобань, стану здоров'я чи політичних поглядів особи.

Наведене стимулює необхідність комплексного перегляду підходів до захисту конфіденційності. Одним із ключових напрямів є впровадження прозорої політики збору й використання даних, що дозволяє користувачам усвідомлено приймати рішення. Також важливо забезпечити варіативність рівнів персоналізації, дозволяючи людині обирати, як саме її дані можуть бути використані. Перспективним рішенням є технологія федеративного навчання, яка зменшує потребу в централізованому зборі даних, залишаючи їх на пристрої користувача.

З огляду на складність викликів, що постають перед суспільством, необхідна тісна співпраця між урядами, технологічними компаніями та громадськістю. Регулятори, подібні до GDPR, відіграють важливу

роль у встановленні правових рамок, однак не менш важливо впроваджувати етичні практики та технічні інновації, які підвищують рівень захисту приватності. Лише шляхом балансу між технологічним прогресом та етичними стандартами можна забезпечити безпечне використання ШІ, що не порушує фундаментальні права людини.

ШІ відкриває великі можливості, але несе значні ризики для приватності. Комплексний підхід – поєднання правових норм, етичних стандартів та технічних заходів – є ключем до безпечного використання цієї технології. Права людини є абсолютними та не можуть бути принесені в жертву технологічній ефективності. Важливим є дотримання ключового принципу pro homine, на користь людині.

Список літератури:

1. Гудзь Л. В. Забезпечення права на приватність у контексті використання штучного інтелекту: потенційні загрози та шляхи їх подолання. 2024. DOI: https://doi.org/10.24144/2307-3322.2024.86.1.25 (дата звернення 19.02.2026).

2. Pareek, K., & Sharma, S. (2025). Impact of Artificial Intelligence on Privacy Rights. *South Eastern European Journal of Public Health*, 2247–2260. DOI: https://doi.org/10.70135/seejph.vi.4128 (дата звернення 19.02.2026).

3. Winau, M. Areas of Tension in the Application of AI and Data Protection Law. *European Data Protection Law Review*. 2023. № 9(2). P. 221–230. DOI: https://doi.org/10.21552/edpl/2023/2/7 (дата звернення 19.02.2026).

4. Aydin I., Diebel-Fischer, H., Freiberger V., Möller-Klapperich J., Buchmann E., Färber M., Lauber-Rönsberg A., & Platow B. Assessing Privacy Policies with AI: Ethical, Legal, and Technical Challenges. 2024. URL: https://arxiv.org/abs/2410.08381 (дата звернення 19.02.2026).

5. Bryan H. Choi, Lawfare. Negligence Liability for AI Developers. URL: https://www.lawfaremedia.org/article/negligence-liability-for-ai-developers (дата звернення 19.02.2026).

6. Що таке штучний інтелект і чого всім раптом стало так цікаво. *ШІ лабораторія.* URL: https://ailaboratory.wixsite.com/shi-ua/post/shcho-take-shtuchnyj-intelect (дата звернення 19.02.2026).

7. Тупальська О. «4 переваги та недоліки ШІ: пожирає тисячі книжок, знає десятки іноземних мов, проте нехтує емоціями людей». URL: https://bigkyiv.com.ua/4-perevagy-ta-nedoliky-shi-pozhyraye-tysyachi-knyzhok-znaye-desyatky-inozemnyh-mov-prote-nehtuye-emocziyamy-lyudej/ (дата звернення 19.02.2026).

8. Office of the Victorian Information Commissioner «Artificial Intelligence and Privacy – Issues and Challenges». URL: https://ovic.vic.gov.au/privacy/resources-for-organisations/artificial-intelligence-and-privacy-issues-and-challenges/ (дата звернення 19.02.2026).

9. Барбашин Сергій Штучний інтелект: правове регулювання в Україні та ЄС. URL: https://barbashyn.law/statti/shtuchnyj-intelekt-pravove-regulyuvannya-v-ukrayini-ta-yes/ (дата звернення 19.02.2026).

10. Lars-Erik Casper Ferm, Park Thaichon, Sara Quach «AI and Its Implications for Data Privacy». URL: https://blog.routledge.com/science-and-technology/ai-and-its-implications-for-data-privacy/ (дата звернення 19.02.2026).

11. Alice Gomstyn, Alexandra Jonker «Exploring privacy issues in the age of AI». URL: https://www.ibm.com/think/insights/ai-privacy (дата звернення 19.02.2026).

12. The growing data privacy concerns with AI: What you need to know (2024). URL: https://www.dataguard.com/blog/growing-data-privacy-concerns-ai/#:~:text=AI%20poses%20various%20privacy%20challenges,consequences%20for%20individuals%20and%20society (дата звернення 19.02.2026).

13. Максимова В. Чи знищив штучний інтелект демократію? Уроки виборів 2024 у світі. *Чесно.* 2026. URL: https://www.chesno.org/post/6348/ (дата звернення 19.02.2026).

14. Біла книга з регулювання ШІ в Україні. (2024). 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?time=1744806741842 (дата звернення 19.02.2026).

15. Остіян Є. З. (2024) Штучний інтелект та персональні дані: захист приватності в цифровому середовищі URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/315480 (дата звернення 19.02.2026).

16. Загальний регламент про захист даних (GDPR). URL: https://gdpr-text.com/uk/ (дата звернення 19.02.2026).

17. California Consumer Privacy Act (CCPA). 2024. URL: https://oag.ca.gov/privacy/ccpa (дата звернення 19.02.2026).

18. Guidelines on Artificial Intelligence and Data Protection. 2019. URL: https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8 (дата звернення 19.02.2026).

19. AI Act. URL: https://artificialintelligenceact.eu/ (дата звернення 19.02.2026).

20. Data protection officer – кому потрібен і які функції у фахівця. 2022. URL: https://stalirov.lawyer/uk/posts/data-protection-officer (дата звернення 19.02.2026).

21. Проєкт EU4DigitalUA « Права людини в епоху штучного інтелекту: виклики та правове регулювання». 2024. URL: https://eu4digitalua.eu/wp-content/uploads/2024/02/guia_ukr_5.pdf (дата звернення 19.02.2026).

References:

1. Hudz L. V. (2024) *Zabezpechennia prava na pryvatnist u konteksti vykorystannia shtuchnoho intelektu: potentsiini zahrozy ta shliakhy yikh podolannia.* [Ensuring the right to privacy in the context of artificial intelli-

gence use: potential threats and ways to overcome them]. DOI: https://doi.org/10.24144/2307-3322.2024.86.1.25 (accessed: 19.02.2026). (in Ukrainian)

2. Pareek, K., & Sharma, S. (2025). *Impact of Artificial Intelligence on Privacy Rights. South Eastern European Journal of Public Health*, 2247–2260. DOI: https://doi.org/10.70135/seejph.vi.4128 (accessed: 19.02.2026).

3. Winau, M. (2023). *Areas of Tension in the Application of AI and Data Protection Law.* European Data Protection Law Review, 9(2), 221–230. DOI: https://doi.org/10.21552/edpl/2023/2/7 (accessed: 19.02.2026).

4. Aydin, I., Diebel-Fischer, H., Freiberger, V., Möller-Klapperich, J., Buchmann, E., Färber, M., Lauber-Rönsberg, A., & Platow, B. (2024). Assessing Privacy Policies with AI: Ethical, Legal, and Technical Challenges. URL: https://arxiv.org/abs/2410.08381 (accessed: 19.02.2026).

5. Bryan, H. Choi, Lawfare. Negligence Liability for AI Developers. URL: https://www.lawfaremedia.org/article/negligence-liability-for-ai-developers (accessed: 19.02.2026).

6. Shcho take shtuchnyi intelekt i choho vsim raptom stalo tak tsikavo. [What is artificial intelligence and why has everyone suddenly become so interested in it] *ShI laboratoriia.* URL: https://ailaboratory.wixsite.com/shi-ua/post/shcho-take-shtuchnyj-intelect (accessed: 19.02.2026).

7. Tupalska O. *4 perevahy ta nedoliky ShI: pozhyraie tysiachi knyzhok, znaie desiatky inozemnykh mov, prote nekhtuie emotsiiamy liudei.* [4 advantages and disadvantages of AI: it devours thousands of books, knows dozens of foreign languages, but disregards human emotions]. URL: https://bigkyiv.com.ua/4-perevagy-ta-nedoliky-shi-pozhyraye-tysyachi-knyzhok-znaye-desyatky-inozemnyh-mov-prote-nehtuye-emocziyamy-lyudej/ (accessed: 19.02.2026). (in Ukrainian)

8. Office of the Victorian Information Commissioner «Artificial Intelligence and Privacy – Issues and Challenges». URL: https://ovic.vic.gov.au/privacy/resources-for-organisations/artificial-intelligence-and-privacy-issues-and-challenges/ (accessed: 19.02.2026).

9. Barbashyn S. *Shtuchnyi intelekt: pravove rehuliuvannia v Ukraini ta YeS*. [Artificial intelligence: legal regulation in Ukraine and the EU]. URL: https://barbashyn.law/statti/shtuchnyj-intelekt-pravove-regulyuvannya-v-ukrayini-ta-yes/ (accessed: 19.02.2026). (in Ukrainian)

10. Lars-Erik Casper Ferm, Park Thaichon, Sara Quach «AI and Its Implications for Data Privacy». URL: https://blog.routledge.com/science-and-technology/ai-and-its-implications-for-data-privacy/ (data zvernennia: 19.02.2026).

11. Alice Gomstyn, Alexandra Jonker, Exploring privacy issues in the age of AI. URL: https://www.ibm.com/think/insights/ai-privacy (accessed: 19.02.2026).

12. The growing data privacy concerns with AI: What you need to know (2024). URL: https://www.dataguard.com/blog/growing-data-privacy-concerns-ai/#:~:text=AI%20poses%20various%20privacy%20challenges,consequences%20for%20individuals%20and%20society (accessed: 19.02.2026).

13. Maksymova V. (2026). *Chy znyshchyv shtuchnyi intelekt demokratiiu? Uroky vyboriv 2024 u sviti.* [Has artificial intelligence destroyed democ-

racy? Lessons from the 2024 elections around the world]. *Chesno.* URL: https://www.chesno.org/post/6348/ (accessed: 19.02.2026). (in Ukrainian)

14. *Bila knyha z rehuliuvannia ShI v Ukraini.* [White paper on AI regulation in Ukraine]. (2024). 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?-time=1744806741842 (accessed: 19.02.2026).

15. Ostiian Ye. Z. (2024) *Shtuchnyi intelekt ta personalni dani: zakhyst pryvatnosti v tsyfrovomu seredovyshchi* [Artificial intelligence and personal data: protecting privacy in the digital environment]. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/315480 (accessed: 19.02.2026). (in Ukrainian)

16. Zahalnyi rehlament pro zakhyst danykh (GDPR). [General Data Protection Regulation]. URL: https://gdpr-text.com/uk/ (accessed: 19.02.2026).

17. California Consumer Privacy Act (CCPA). (2024). URL: https://oag.ca.gov/privacy/ccpa (accessed: 19.02.2026).

18. Guidelines on Artificial Intelligence and Data Protection. (2019). URL: https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8 (accessed: 19.02.2026).

19. AI Act. URL: https://artificialintelligenceact.eu/ (accessed: 19.02.2026).

20. Data protection officer – komu potriben i yaki funktsii u fakhivtsia. [Data protection officer – who needs one and what are their responsibilities?]. (2022). URL: https://stalirov.lawyer/uk/posts/data-protection-officer (accessed: 19.02.2026).

21. Proiekt EU4DigitalUA «Prava liudyny v epokhu shtuchnoho intelektu: vyklyky ta pravove rehuliuvannia». [EU4DigitalUA project "Human rights in the age of artificial intelligence: challenges and legal regulation."]. (2024). URL: https://eu4digitalua.eu/wp-content/uploads/2024/02/guia_ukr_5.pdf (accessed: 19.02.2026).