АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС; ФІНАНСОВЕ ПРАВО; ІНФОРМАЦІЙНЕ ПРАВО

УДК 349
DOI https://doi.org/10.32782/TNU-2707-0581/2024.1/11

Гнедюк В.Л.
Український науково-дослідний інститут спеціальної техніки та судових експертиз
Служби безпеки України

ВПЛИВ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ НА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ: ПРАВОВІ АСПЕКТИ

У роботі розглядається впровадження технології штучного інтелекту в сучасному світі та його вплив на різні аспекти життя. Зазначається, що штучний інтелект перетворюється на невід'ємну складову повсякденного існування, проникаючи в різні сфери.

Штучний інтелект (ШІ) – це галузь інформатики, що вивчає створення систем, які здатні виконувати завдання, що вимагають інтелектуальної обробки і аналізу. Метою штучного інтелекту є створення програм, алгоритмів та моделей, які надають комп'ютерам можливість виконувати завдання, які традиційно вважаються властивими людському інтелекту. Це включає в себе вивчення, розпізнавання образів, прийняття рішень, мовленнєву взаємодію та інші аспекти «розумної» поведінки.

Особлива увага приділяється етичним та правовим аспектам використання штучного інтелекту, зокрема у контексті упереджених результатів, непрозорих процесів та втрати контролю над обробкою даних. Також зазначається на ризиках автоматизації та важливості регулювання застосування штучного інтелекту відповідно до міжнародних стандартів.

Також висвітлено стан законодавства в Україні щодо штучного інтелекту.

У роботі зазначено, що законодавство з захисту персональних даних в Україні передбачає символічні штрафи за порушення – до двох тисяч неоподатковуваних мінімумів доходів громадян. Обґрунтовано, що в сфері захисту персональних даних, пов'язаній із штучним інтелектом, існують ризики несанкціонованого доступу, алгоритмічної дискримінації та недостатньої прозорості алгоритмів. Пропонуються шляхи вирішення.

Крім того, вказано, що в ЄС, особливо за допомогою GDPR, та прийняттям «Artificial Intelligence Act», встановлені стандарти для захисту персональних даних у контексті штучного інтелекту. Україна, дотримуючись цих норм, активно впроваджує заходи, включаючи «регуляторну пісочницю». Зазначено, що правильне регулювання визначається як ключовий елемент для забезпечення безпеки та захисту прав користувачів, сприяючи при цьому інноваціям у сфері штучного інтелекту.

Ключові слова: *штучний інтелект, персональні дані, алгоритми, конфіденційна інформація, права, приватність.*

Постановка проблеми. Швидкі темпи технологічного розвитку, зокрема в області штучного інтелекту (ШІ), супроводжуються значними змінами у всіх сферах людського життя, включаючи сферу збереження та обробки персональних даних. Застосування технологій ШІ нерідко виправдано обіцянкою вдосконалення ефективності, зручності та інновацій в різних аспектах нашого повсякденного і професійного життя. Однак разом з цими можливостями виникає необхідність ретельного вивчення та розуміння правових аспектів захисту персональних даних в умовах широкого впровадження технологій штучного інтелекту.

Сучасне суспільство стикається з викликами, пов'язаними зі збільшенням обсягу та різноманітності персональної інформації, яка обробляється та зберігається в електронних системах. В контексті використання ШІ, зокрема алгоритмів машинного навчання, аналізу великих даних та автомати-

зованих систем прийняття рішень, стає важливим визначити граничні рамки для забезпечення конфіденційності та захисту особистих даних.

Аналіз останніх досліджень і публікацій. Робота ґрунтується на аналізі законодавства України та зарубіжних країн, науково-методичної літератури, методичних посібників, наукових статей, періодичних видань та напрацювань сучасних та попередніх вчених і дослідників, серед них: М. В. Бєлова, О. І. Косілова, Т. М. Кронівець, С. Барабашин та багато інших.

Постановка завдання. Мета дослідження – проаналізувати особливості впливу технологій штучного інтелекту на захист персональних даних в правовому контексті.

Об'єкт дослідження – вплив технологій штучного інтелекту на захист персональних даних.

Предмет дослідження – правові аспекти регулювання обробки та захисту персональних даних у контексті застосування технологій штучного інтелекту.

Виклад основного матеріалу. Штучний інтелект (ШІ) – це галузь інформатики, що вивчає створення систем, які здатні виконувати завдання, що вимагають інтелектуальної обробки і аналізу. Метою штучного інтелекту є створення програм, алгоритмів та моделей, які надають комп'ютерам можливість виконувати завдання, які традиційно вважаються властивими людському інтелекту. Це включає в себе вивчення, розпізнавання образів, прийняття рішень, мовленнєву взаємодію та інші аспекти «розумної» поведінки.

Впровадження технології штучного інтелекту в сучасному світі вже перетворилося на невід'ємну складову нашого повсякденного існування, незважаючи на те, що багато індивідів можуть бути несвідомими щодо цього факту. Характерною особливістю штучного інтелекту є його перехід від абстрактної ідеї до звичайного обчислення та алгоритмічної обробки, коли він активно застосовується. Ці технологічні системи стають не просто штучним інтелектом, але звичайними механізмами обчислень та алгоритмів, інтегруючись у різні сфери нашого життя, такі як розпізнавання мовлення, обробка природної мови та прогнозна аналітика.

Незважаючи на потенційні переваги, такі як підвищення ефективності та зниження витрат, а також удосконалена охорона здоров'я та безпека транспортних засобів, виникають суттєві етичні та правові аспекти, пов'язані із застосуванням технологій штучного інтелекту. Розвиток цих технологій приносить із собою ризики упереджених результатів та непрозорих процесів, створюючи проблеми для суспільства та законодавства, зокрема у контексті прийняття рішень урядовими органами. Автоматизація різних сфер за допомогою штучного інтелекту може також призвести до втрати контролю над обробкою даних та порушення традиційних механізмів управління конфіденційністю [8, с. 295–296].

На відміну від європейських країн стан законодавства в нашій державі знаходиться лише на початковому етапі на шляху до унормування нового типу правовідносин за умови застосування технологій штучного інтелекту у різні сфери та потребує його удосконалення та гармонізації з європейським у цій сфері. Регулювання питань щодо застосування штучного інтелекту має здійснюватися відповідно до норм міжнародних договорів та конвенцій, що ратифіковані більшістю (європейських) держав. Зокрема, відповідно до спеціалізованих міжнародних договорів у сфері розвитку штучного інтелекту: Конвенції Ради Європи про кіберзлочинність, також відома як Будапештська конвенція; Етичної хартії по використанню штучного інтелекту у судовій системі та її середовищі (European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment), Загального Регламенту захисту даних (ЄС) 2016 / 679 від 27.04.16 р. (General Data Protection Regulation) [7, с. 58].

Україна вже використовує досвід провідних європейських держав (зокрема Естонії) у сфері застосування технологій штучного інтелекту у публічне адміністрування та рухається в напрямку створення е-України. Так, Міністерством цифрової трансформації України (далі – Мінцифри України) було розроблено Концепцію розвитку штучного інтелекту в Україні. Як зазначила заступник міністра цифрової трансформації Іонан В.: «Наша головна мета – сприяння розвитку штучного інтелекту й інтеграція його в економічно важливі сектори. Таким чином ми збільшимо частку інтелектуально ємних продуктів і значно зміцнимо позиції України на світовому ринку. Особливу увагу планується приділяти використанню штучного інтелекту в сфері кібербезпеки й оборони. Також дуже важливо мати правильний баланс між штучним інтелектом, розробленим сторонніми постачальниками і національними» [2].

У загальному розумінні, концепція конфіденційності інформації визначається уявленням про те, що люди, як основні обробники інформації, не здатні ефективно взаємодіяти з обчислювальними

здібностями штучного інтелекту, які виходять за межі традиційних концепцій збору та обробки даних. У сучасних умовах розвитку технологій штучного інтелекту, розуміння понять, таких як інформована згода, повідомлення, а також принципи доступу та контролю за особистою інформацією, стає об'єктом фундаментальних викликів, що раніше не враховувалися в такому масштабі та контексті [10].

Варто розпочати із визначення конфіденційної інформації. В Законі України «Про доступ до публічної інформації» зазначено, що конфіденційною є інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов [5].

Закон «Про інформацію» має своє визначення, а саме: «конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом» [3].

Конфіденційна інформація про особу, її персональні дані можуть поширюватись лише якщо ця особа надала свою згоду на поширення або самостійно поширила її серед необмеженого кола осіб, наприклад, розповіла про певні факти свого життя в прямому ефірі, опублікувала щось у соціальних мережах у відкритому доступі. Але є виключення, за частиною 2 статті 14 Закону України «Про захист персональних даних», поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини [4].

Отже, концепція персональних даних ґрунтується на ідентифікації – можливості обґрунтовано визначити особу за наданою інформацією. Проте розрізнення між тим, що вважається «особистим», і тим, що вважається таким, що не має особистого характеру, ускладнюється здатністю асоціювати та порівнювати дані з конкретними особами, навіть якщо раніше ці дані розглядалися як «де персоналізовані» чи «не ідентифіковані». У цьому контексті комбінація, на перший погляд, неособистої інформації може стати особистою під час аналізу чи зіставлення. Зі зростанням обсягу доступних даних і вдосконаленням технологій їх обробки та аналізу стає все важче визначити, чи є конкретний набір даних «ідентифікованим»; розгляд окремих фрагментів даних в ізоляції стає непридатним для технологій штучного інтелекту і вже не відображає адекватно можливість визначення їх як «особистої інформації» [8, с. 296].

Аналізуючи нормативно-правові акти українського законодавства, можна дійти висновку, що за порушення законодавства у сфері захисту персональних даних українське законодавство передбачає штрафи, які цілком можна назвати символічними – до двох тисяч неоподатковуваних мінімумів доходів громадян, тобто 34 тисяч гривень (ст. 188–39 Кодексу про адміністративні правопорушення) [1].

Серед викликів та загроз у сфері захисту персональних даних, що пов'язані із використанням штучного інтелекту, можна виділити наступні аспекти:

– Ризик несанкціонованого доступу до персональних даних: використання штучного інтелекту може призвести до збільшення обсягу оброблюваних персональних даних, що створює загрозу можливого несанкціонованого доступу. Це може викликати порушення приватності та потенційні випадки зловживання.

– Ризик алгоритмічної дискримінації: алгоритми, використовувані в штучному інтелекті для прийняття рішень на основі персональних даних, можуть піддаватися дискримінації, якщо базуються на неточних чи необ'єктивних даних. Це може призвести до нерівності, порушень прав та дискримінації осіб на підставі їхніх особистих характеристик.

– Недостатня прозорість та обгрунтованість алгоритмів: використання складних алгоритмів штучного інтелекту створює проблему в розумінні та поясненні того, як саме ці алгоритми приймають рішення на основі персональних даних. Це ускладнює відслідковування та нагляд за їхньою діяльністю [6, с. 20].

Щодо вирішення викликів та проблем у сфері захисту персональних даних при використанні штучного інтелекту, можна запропонувати наступні шляхи:

– Підвищення свідомості та навчання: забезпечення належного розуміння проблем та ризиків використання штучного інтелекту для правозахисників, органів влади, громадських організацій та громадян є важливим етапом. Це можливо через організацію навчальних програм, семінарів та конференцій, спрямованих на підвищення обі-

знаності та розуміння правових аспектів цієї проблеми.

– Створення ефективного правового регулювання: необхідно розробити та впровадити ефективне законодавство, яке забезпечить адекватний захист персональних даних у використанні штучного інтелекту. Це може включати в себе розробку спеціальних правил для обробки даних, визначення відповідальності сторін та встановлення механізмів контролю.

– Використання принципу «за замовчуванням»: у роботі з персональними даними у контексті штучного інтелекту рекомендується встановлювати принцип «за замовчуванням», згідно з яким всі дії мають бути спрямовані на максимальний захист приватності та обмеження передачі даних, якщо не надано іншого вказівника.

– Застосування технічних заходів безпеки: компанії та організації, які використовують штучний інтелект, повинні приділяти особливу увагу використанню технічних засобів безпеки, таких як шифрування даних, системи доступу на основі ролей та аудит діяльності. Це забезпечить конфіденційність та цілісність персональних даних.

Ці заходи обговорюються як можливі шляхи для забезпечення ефективного та справедливого захисту персональних даних у контексті штучного інтелекту [6, с. 21].

Країни світу в останні роки зрозуміли важливість розробки законодавства з захисту персональних даних у контексті штучного інтелекту. ЄС прийняв загальний регламент про захист даних, відомий як Загальний регламент про захист персональних даних (GDPR). Він визначає права громадян ЄС щодо збирання, обробки та зберігання їх персональних даних, включаючи використання штучного інтелекту.

Вже існує декілька прикладів, застосування норм GDPR європейськими регуляторами до розробників систем ШІ. Так, компанія Clearview AI – розробник програмного забезпечення для розпізнавання облич, з використанням штучного інтелекту отримала декілька штрафів через незаконне використання персональних даних осіб в п’яти країнах. Управління з захисту персональних даних у Франції (CNIL), зокрема зазначили, що Clearview AI використовує особисту інформацію без законної згоди користувачів та водночас немає законного інтересу для такого збору, що є серйозним порушенням GDPR.

Італія обмежила доступ до всім відомого Chat GPT, через занепокоєння щодо обробки персональних даних громадян. Так, італійський регулятор зазначає, про відсутність правової основи, яка б виправдовувала масовий збір і зберігання персональних даних з метою «навчання» алгоритмів, що лежать в основі роботи платформи [9].

GDPR став фундаментом для забезпечення високого рівня захисту персональних даних, які використовуються в рамках роботи та навчання ШІ.

У червні 2023 року Європейський Парламент зробив великий крок у напрямку створення правового фундаменту для ефективного та етичного використання штучного інтелекту, схваливши законопроект під назвою «Artificial Intelligence Act».

Однією з основних цілей Акту є захист прав і свобод осіб, які піддаються впливу штучного інтелекту. Закон визначає принципи та правила для обробки персональних даних, використання систем автоматизованого прийняття рішень та інших аспектів штучного інтелекту, сприяючи прозорості, справедливості та законності обробки даних.

Прийняття Акту безпосередньо вплине на регулювання штучного інтелекту в Україні. Кароліна Івасівська, радниця з цифрових прав у ЄС, вказала, що «як тільки Закон про штучний інтелект буде прийнятий, його також повинні будуть прийняти країни-кандидати до ЄС, якою є і Україна».

Уже зараз Україна бере участь у впровадженні Акту. Уряд України прийняв рішення про запуск «регуляторної пісочниці» для розробників штучного інтелекту, контрольованого середовища, де компанії-розробники можуть враховувати вимоги майбутнього законодавства ЄС від самого початку розробки свого продукту [9].

Висновки. Правове регулювання штучного інтелекту в Україні та ЄС виявляється все більш важливим у зв’язку з розвитком технологій. Всі країни зараз активно працюють над створенням адаптованих та ефективних правових норм, що враховують особливості штучного інтелекту. Це дозволяє забезпечити безпеку та захист прав користувачів технологій ШІ, а також створити сприятливі умови для розвитку інновацій та цифрової економіки.

Держава відіграє важливу роль у створенні середовища, в якому зобов’язання щодо розробки безпечного та справедливого штучного інтелекту мають бути збалансовані з технологічним прогресом та правом. Правильний баланс вимагає консультативного, міждисциплінарного підходу, оскільки надмірне, неналежне чи неправильне регулювання може сповільнити впровадження

штучного інтелекту або не в змозі вирішити його справжні виклики. Використання існуючих структур конфіденційності інформації, а також переосмислення традиційних концепцій стане ключовим компонентом у створенні, використанні та регулюванні ШІ.

Список літератури:

1. Кодекс України про адміністративні правопорушення: Закон України від 07.12.84 р., № 8073-X: веб-сайт. URL: https: // zakon. rada. gov. ua / laws / show / 80731–10#Text (дата звернення: 14.01.2024).

2. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження КМУ від 02.12.2020 р., №1556-р: веб-сайт. URL: https: // zakon. rada. gov. ua / laws / show / 1556–2020-%D1%80#Text (дата звернення: 10.01.2024).

3. Про інформацію: Закон України від 02.10.1992 р., № 2657-XII: веб-сайт. URL: https: // zakon. rada. gov. ua / laws / show / 2657–12#Text (дата звернення 11.01.2024.).

4. Про захист персональних даних: Закон України від 01.06.2010 р., № 2297-VI: веб-сайт. URL: https: // zakon. rada. gov. ua / laws / show / 2297–17#Text (дата звернення 12.01.2024).

5. Про доступ до публічної інформації: Закон України від 13.01.2011 р., №2939-VI: веб-сайт. URL: https: // zakon. rada. gov. ua / laws / show / 2939–17#Text (дата звернення: 12.01.2024).

6. Бєлова М. В., Бєлов Д. М. Виклики та загрози захисту персональних даних у роботі зі штучним інтелектом. *Науковий вісник Ужгородського Національного Університету. Сер.: Право.* Вип. 79. Ч. 2. 2023. С. 17–22.

7. Косілова О. І., Солодовнікова Х. К. Права і свободи людини і громадянина V. S. штучний інтелект: проблемні аспекти. *Інформація і право.* № 4 (35). 2020. С. 56–66.

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

9. Барабашин С. Штучний інтелект: правове регулювання в Україні та ЄС: веб-сайт. URL: https: // barbashyn. law / statti / shtuchnyj-intelekt-pravove-regulyuvannya-v-ukrayini-ta-yes/ (дата звернення: 14.01.2023).

10. Artificial Intelligence and Privacy – Issues and Challenges: веб-сайт. URL: https: // ovic. vic. gov. au / privacy / resources-for-organisations / artificialintelligence-and-privacy-issues-and-challenges/#conclusion (дата звернення 13.01.2024).

Hnediuk V.L. IMPACT OF ARTIFICAL INTELLIGENCE TECHNOLOGY ON PERSONAL DATA PROTEKTION: LEGAL ASPECTS

This paper explores the integration of artificial intelligence (AI) technology in the contemporary world and its influence on various aspects of life. It emphasizes that AI has become an integral part of everyday existence, penetrating into diverse spheres.

Artificial Intelligence (AI) is a branch of computer science that focuses on creating systems capable of performing tasks requiring intellectual processing and analysis. The goal of AI is to develop programs, algorithms, and models that enable computers to perform tasks traditionally considered within the realm of human intelligence. This includes learning, pattern recognition, decision-making, speech interaction, and other aspects of «smart» behavior.

Special attention is given to ethical and legal aspects of AI usage, particularly concerning biased outcomes, opaque processes, and loss of control over data processing. The risks of automation and the importance of regulating AI application in accordance with international standards are also highlighted.

The paper delves into the current legislative framework in Ukraine concerning AI. It notes that data protection laws in Ukraine impose symbolic fines for violations, up to two thousand untaxed minimum incomes. The discussion is grounded in the observation that in the realm of personal data protection related to AI, there are risks of unauthorized access, algorithmic discrimination, and insufficient transparency of algorithms. Proposed solutions to address these issues are presented.

Additionally, it is pointed out that the European Union, notably through the General Data Protection Regulation (GDPR) and the adoption of the «Artificial Intelligence Act," has established standards for personal data protection in the context of AI. Ukraine, aligning with these norms, actively implements measures, including a «regulatory sandbox.» It is emphasized that proper regulation is a key element in ensuring the safety and protection of user rights while fostering innovation in the field of artificial intelligence.

Key words: *artificial intelligence, personal data, algorithms, confidential information, rights, privacy.*