УДК 342.1
DOI https://doi.org/10.24144/2307-3322.2023.79.2.2

ВИКЛИКИ ТА ЗАГРОЗИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У РОБОТІ ЗА ШТУЧНИМ ІНТЕЛЕКТОМ

Бєлова М.В.,
доктор юридичних наук, доцент
кафедри конституційного права та порівняльного правознавства
юридичного факультету
ДВНЗ «Ужгородський національний університет»
ORCID ID: https://orcid.org/0000-0003-2077-2342

Бєлов Д.М.,
доктор юридичних наук, професор,
професор кафедри конституційного права та порівняльного правознавства
юридичного факультету
ДВНЗ «Ужгородський національний університет»,
Заслужений юрист України
ORCID ID: https://orcid.org/0000-0002-7168-9488

Бєлова М.В., Бєлов Д.М. Виклики та загрози захисту персональних даних у роботі зі штучним інтелектом.

З розвитком технологій штучного інтелекту з'являються нові можливості використання персональних даних для різних цілей, таких як машинне навчання, автоматизація процесів та управління великими обсягами інформації. Однак, разом з цими можливостями виникають питання щодо захисту приватності особистих даних та дотримання прав людини. Ця стаття спрямована на дослідження викликів та загроз, які становляться актуальними у контексті використання штучного інтелекту з точки зору правознавців.

Ця наукова стаття досліджує виклики та загрози, пов'язані з захистом персональних даних у роботі зі штучним інтелектом (ШІ). Зростаюча роль ШІ в різних сферах життя викликає потребу в обміні та обробці великого обсягу персональних даних. Однак, цей процес народжує серйозні проблеми з приватністю і безпекою.

Стаття аналізує основні виклики, зокрема, нестабільність технологічного прогресу, яка ускладнює розробку ефективних методів захисту персональних даних. Також досліджується проблема обробки великого обсягу даних із забезпеченням їх конфіденційності та цілісності. Важливу увагу приділяється проблемі ідентифікації та управління ризиками, пов'язаними з захистом персональних даних у контексті ШІ.

Стаття також визначає загрози безпеці персональних даних у роботі зі ШІ. Автори розглядають можливість несанкціонованого доступу до персональних даних, крадіжку ідентифікаційних даних, а також можливість використання ШІ для маніпулювання даними з метою шахрайства або дискримінації. Також аналізується проблема алгоритмічної упередженості та ризики недостатньої анонімізації даних.

В заключенні статті наводяться можливі рекомендації та стратегії для захисту персональних даних у роботі зі ШІ. Зокрема, розглядаються необхідність встановлення суворих правил і нормативів для обробки персональних даних, використання шифруван ції та анонімізації даних, розвиток механізмів контролю та перевірки дотримання політик безпеки, а також освіта та підвищення обізнаності користувачів щодо захисту персональних даних.

Ключові слова: персональні дані, штучний інтелект, права людини, приватність, конфіденційність.

Bielova M.V., Byelov D.M. Challenges and threats of personal data protection in working with artificial intelligence.

With the development of artificial intelligence technologies, there are new opportunities to use personal data for various purposes, such as machine learning, process automatization and management

of large volumes of information. However, along with these opportunities, questions arise regarding the protection of personal data privacy and the observance of human rights. This article aims to explore the challenges and threats that are becoming relevant in the context of the use of artificial intelligence from the perspective of legal scholars.

This research paper explores the challenges and threats associated with the protection of personal data when working with artificial intelligence (AI). The growing role of AI in various spheres of life causes the need to exchange and process a large amount of personal data. However, this process raises serious privacy and security issues.

The article analyzes the main challenges, in particular, the instability of technological progress, which complicates the development of effective methods of personal data protection. The problem of processing a large amount of data while ensuring its confidentiality and integrity is also investigated. Important attention is paid to the problem of identification and management of risks related to the protection of personal data in the context of AI.

The article also identifies threats to the security of personal data when working with AI. The author consider the possibility of unauthorized access to personal data, identity theft, and the possibility of using AI to manipulate data for the purpose of fraud or discrimination. The problem of algorithmic bias and the risks of insufficient anonymization of data are also analyzed in the present article. The article concludes with recommendations and strategies for protecting personal data when working with AI. In particular, the need to establish strict rules and regulations for the processing of personal data, the use of encryption and anonymization of data, the development of control mechanisms and verification of compliance with security policies, as well as the education and awareness raising of users regarding the protection of personal data.

Key words: personal data, artificial intelligence, human rights, privacy, confidentiality.

Постановка проблеми: Проблема захисту персональних даних у роботі з штучним інтелектом (ШІ) виникає з розширенням використання ШІ в різних сферах життя, таких як медицина, фінанси, транспорт, маркетинг та багато інших. З одного боку, використання ШІ може принести значні переваги, забезпечуючи автоматизацію процесів, вдосконалення прийняття рішень та покращення ефективності роботи. З іншого боку, це може ставити під загрозу конфіденційність та безпеку персональних даних.

Одна з головних проблем полягає у зборі та зберіганні великої кількості персональних даних, які потім використовуються для навчання ШІ. Ці дані можуть включати особисту ідентифікаційну інформацію, медичні записи, фінансові дані, геолокаційні дані та іншу конфіденційну інформацію про користувачів. Недостатня захищеність цих даних може призвести до їх несанкціонованого доступу, втрати або використання в злочинних цілях.

Інша проблема пов'язана з недостатньою прозорістю інтелектуальних систем із застосуванням ШІ. Відсутність чіткого розуміння, як саме ШІ приймає рішення та обробляє дані, ускладнює визначення відповідальності за можливі наслідки використання ШІ. Це може породити проблеми в етиці та справедливості, коли автоматизовані системи приймають рішення, які можуть мати серйозний вплив на життя людей.

Також існує проблема з атаками на системи ШІ з метою незаконного доступу до персональних даних. Все це потребує дослідження з метою подальшої розробки нормативної бази та політик для регулювання даної сфери та мінімізації ризиків.

Стан опрацювання проблематики. Проблематика захисту персональних даних у роботі з штучним інтелектом на сьогоднішній день є досить актуальною і отримує все більше уваги з боку науковців, організацій і законодавців. Основні напрямки опрацювання цієї проблематики включають такі питання:

1. Розробка нормативно-правових актів: Багато країн працюють над розробкою і впровадженням законодавчих актів, що регулюють захист персональних даних у контексті ШІ. Наприклад, загальний регламент про захист персональних даних ЄС (GDPR) встановлює правила збору, обробки та передачі персональних даних, включаючи використання ШІ.
2. Розробка технічних заходів безпеки: Дослідники та розробники працюють над розробкою технічних засобів та алгоритмів, що забезпечують безпеку персональних даних у системах зі штучним інтелектом. Це можуть бути методи шифрування даних, контроль доступу, анонімізація даних та інші технічні рішення.

3. Етичні аспекти: Проблематика захисту персональних даних у роботі з ШІ викликає обговорення в етичному контексті. Дослідники і експерти займаються формулюванням етичних принципів та рекомендацій щодо використання ШІ з урахуванням приватності та безпеки персональних даних.

4. Удосконалення правил навчання ШІ: Для забезпечення захисту персональних даних у роботі з ШІ, розробники займаються питаннями агрегації даних, анонімізації, псевдонімізації.

У сфері дослідження викликів та загроз захисту персональних даних у роботі зі штучним інтелектом існує декілька науковців-правників, які внесли значний внесок. Декілька з них включають:

1. Раяна Кало, професор права з Університету Вашингтона, спеціалізується на тематиці технологічного права, включаючи проблематику захисту приватності, безпеки та етики в контексті штучного інтелекту.

2. Шеріл Баумен - юрист та дослідник, зосереджена на проблемах цифрової приватності та захисту даних. Вона є засновницею та головою «The Plug» - медійної компанії, що працює в галузі технологій та розповідає про вплив технологій на афроамериканську громадськість.

3. Евгенія Маркворст - наукова співробітниця Центру права та комп'ютерних технологій Каліфорнійського університету, Берклі. Вона займається дослідженням правових аспектів штучного інтелекту, зокрема, в сфері захисту даних та приватності.

Метою статті є надання огляду ключових проблем і викликів, пов'язаних з захистом персональних даних у роботі з штучним інтелектом. А саме, вивчення потенційних загроз, вразливостей та ризиків, які пов'язані зі збором, обробкою та зберіганням персональних даних у контексті ШІ; аналіз поточних підходів до захисту даних, існуючі методи і технології, які використовуються для захисту персональних даних у системах з штучним інтелектом; розгляд ролі шифрування, контролю доступу, анонімізації даних та інших технічних заходів у забезпеченні конфіденційності та безпеки даних; нормативно-правовий контекст: законодавство та регулюючі норми, які стосуються захисту персональних даних у роботі з штучним інтелектом, аналіз загальних регламентів, директив та інших нормативно-правових актів, які регулюють збір, обробку та передачу персональних даних у контексті ШІ.

Виклад основного матеріалу. На сьогоднішній день відомі випадки витоку персональних даних, пов'язані з використанням штучного інтелекту, але немає конкретного прецеденту, який був би широко відомий або набув значної уваги громадськості. Проте, можна розглянути деякі випадки, де були порушені принципи захисту персональних даних у контексті використання штучного інтелекту:

Cambridge Analytica: Цей випадок, виявлений у 2018 році, стосувався використання штучного інтелекту для збору та обробки персональних даних мільйонів користувачів Facebook. Компанія Cambridge Analytica, що спеціалізувалася на аналізі даних для політичних кампаній, отримала доступ до персональних даних без належного дозволу користувачів, порушуючи принципи конфіденційності та приватності даних.

Facial Recognition Technology: Використання технології розпізнавання обличчя (Facial Recognition) також може потенційно становити загрозу для приватності осіб. Наприклад, були випадки, коли системи розпізнавання обличчя використовувалися без дозволу користувачів, збираючи їхні персональні дані без належної інформованості та контролю [1].

Кібератаки та витоки даних: Існують випадки, коли зловмисники атакують системи, що використовують штучний інтелект, з метою отримання доступу до персональних даних. Це може призвести до витоку конфіденційної інформації та порушення приватності користувачів.

Ці приклади підкреслюють необхідність встановлення сильного законодавства та заходів безпеки для захисту персональних даних.

В Європі та Україні існують спеціальні законодавчі акти, які регулюють захист персональних даних і визначають правові засади їх обробки. Основним правовим актом в Європейському Союзі є Загальний регламент про захист персональних даних (GDPR), який був прийнятий у 2016 році і набув чинності з 25 травня 2018 року. Україна також має свій закон про захист персональних даних - Закон України «Про захист персональних даних».

Загальний регламент про захист персональних даних (GDPR) - є ключовим юридичним актом, що стосується захисту персональних даних в Європейському Союзі та Європейському економічному просторі. Він встановлює загальні принципи та правила обробки персональних даних, права суб'єктів даних та обов'язки суб'єктів, що здійснюють обробку. Основні принципи GDPR

включають збір та обробку даних на законній підставі, обмеження обробки до визначених цілей, забезпечення точності та цілісності даних, збереження обмеженого строку зберігання даних, а також забезпечення безпеки та конфіденційності даних [2].

Закон України «Про захист персональних даних» встановлює правові засади захисту персональних даних в Україні. Згідно з цим законом, персональні дані є конфіденційною інформацією, яка стосується фізичної особи, і повинні оброблятись у визначених рамках та згідно з принципами, встановленими законом.

Закон України «Про захист персональних даних» встановлює основні принципи та правила обробки персональних даних, включаючи прозорість обробки, обмеження обробки до визначених цілей, забезпечення точності та цілісності даних, обов'язок зберігання обмеженого строку зберігання даних, а також заходи безпеки для захисту даних від несанкціонованого доступу, втрати, знищення або пошкодження.

Особливою рисою закону України є вимога отримання згоди суб'єкта даних на обробку його персональних даних. Згода має бути добровільною, інформованою та конкретною. Суб'єкт даних також має право вимагати доступу до своїх персональних даних, виправлення неправильних даних, видалення або обмеження обробки своїх даних, а також право на переносимість даних.

Крім GDPR та Закону України «Про захист персональних даних», у Європі та Україні існують інші додаткові нормативні акти, які впливають на захист персональних даних, такі як директиви, постанови та інші внутрішні правові акти, що уточнюють та доповнюють основні принципи та вимоги.

Важливо зазначити, що правозастосовні органи, такі як державні органи з контролю за захистом персональних даних, відповідають за нагляд за дотриманням цих законів і захист прав суб'єктів даних. В разі порушення вимог захисту персональних даних, повинна наставати адміністративна або кримінальна відповідальність, а також можуть застосовуватись цивільно-правові засоби захисту.

Серед викликів та загроз захисту персональних даних у роботі зі штучним інтелектом можна виділити:

Ризик несанкціонованого доступу до персональних даних: Використання штучного інтелекту може призвести до збільшення обсягу персональних даних, що обробляються, та зберігаються. Це створює загрозу можливого несанкціонованого доступу до цих даних, що може призвести до порушення приватності та потенційних зловживань [3].

Ризик алгоритмічної дискримінації: Штучний інтелект використовує алгоритми для прийняття рішень на основі обробки персональних даних. Однак, такі алгоритми можуть бути підвержені дискримінації, якщо вони ґрунтуються на неправильних або необ'єктивних даних. Це може призвести до нерівності, порушення прав та дискримінації осіб на основі їх особистих характеристик [4].

Ризик алгоритмічної дискримінації виникає, коли системи штучного інтелекту, засновані на алгоритмах та машинному навчанні, приймають рішення, які можуть призводити до некоректного, несправедливого або дискримінаційного оброблення індивідів або груп людей на підставі їхніх персональних характеристик, таких як раса, стать, вік, етнічна належність, релігійні переконання тощо [5].

Одним з основних джерел ризику алгоритмічної дискримінації є якість та характеристики вихідних даних, на основі яких системи штучного інтелекту навчаються. Якщо вихідні дані містять приховані відображення дискримінації або нерепрезентативність, то алгоритми можуть усвідомити ці недоліки і відображати їх у своїх рішеннях. Наприклад, якщо навчальний набір даних зайво зосереджений на певних групах або ґендерних нерівностях, система може виносити несправедливі рішення у контексті зайнятості або кредитування.

Крім того, алгоритми можуть надмірно підкреслювати існуючі соціокультурні нерівності, оскільки вони використовуються для прогнозування майбутніх подій на підставі історичних даних. Це може спричиняти зацикленість на стереотипах, виключенні певних груп або надмірне обтяження незахищених груп [6].

Недостатня прозорість і пояснюваність алгоритмів: Штучний інтелект може використовувати складні алгоритми, які важко пояснити та зрозуміти. Це створює проблему в обсязі розуміння, як самі алгоритми приймають рішення на основі персональних даних, що може ускладнити контроль та нагляд за їхньою діяльністю [7].

Серед шляхів вирішення проблем можна запропонувати:

Підвищення свідомості та навчання: Важливо забезпечити, щоб правознавці, органи державної влади, а також громадські організації та громадяни мали достатні знання про проблеми та

ризики використання штучного інтелекту у контексті захисту персональних даних. Це можна забезпечити шляхом проведення навчальних програм, семінарів та конференцій, спрямованих на підвищення обізнаності та розуміння правових аспектів цієї проблеми.

Створення ефективного правового регулювання: Необхідно розробити та впровадити ефективне законодавство, яке забезпечує адекватний захист персональних даних у контексті використання штучного інтелекту. Це може включати створення спеціальних правил щодо обробки даних, визначення відповідальності сторін та установлення механізмів контролю [8].

Необхідність розробки та впровадження ефективного законодавства, що забезпечує адекватний захист персональних даних у контексті використання штучного інтелекту, обумовлена кількома факторами:

Зростання використання штучного інтелекту: Штучний інтелект стає все більш поширеним і використовується у різних сферах, включаючи медицину, фінанси, транспорт, маркетинг і багато інших. Це призводить до збільшення обсягів обробки персональних даних, а отже, до появи нових ризиків та викликів для приватності та захисту даних [9].

Суттєвість персональних даних: Персональні дані містять конфіденційну інформацію про фізичних осіб, включаючи особисту ідентифікацію, фізичний стан, фінансову інформацію тощо. Незаконне збирання, використання або розголошення цих даних може призвести до серйозних наслідків для приватності та безпеки осіб.

Уразливість штучного інтелекту: Штучний інтелект може бути підданий різного роду загрозам, таким як злочинні дії, кібератаки, зловживання даними тощо. Відсутність адекватного законодавства може сприяти зловживанню та порушенню безпеки персональних даних [10].

Використання принципу «за замовчуванням»: У контексті обробки персональних даних у роботі зі штучним інтелектом слід встановлювати принцип «за замовчуванням», згідно з яким всі дії повинні бути спрямовані на максимальний захист приватності та непоширення даних, якщо не зазначено протилежне.

Застосування технічних заходів безпеки: Компанії та організації, які використовують штучний інтелект, повинні приділяти особливу увагу технічним заходам безпеки, таким як шифрування даних, системи доступу на основі ролей та аудиту діяльності, щоб забезпечити конфіденційність та цілісність персональних даних.

Країни світу в останні роки зрозуміли важливість розробки законодавства з захисту персональних даних у контексті штучного інтелекту. Ось кілька прикладів досвіду країн у цій сфері:

1. Європейський союз (ЄС): 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.
2. Канада: Канада прийняла Закон про захист персональних інформацій, який має загальний характер і визначає правила для обробки персональних даних, включаючи їх використання у сфері штучного інтелекту.
3. Сполучені Штати Америки: В США поки що немає загального федерального закону про захист персональних даних, але деякі штати, такі як Каліфорнія, прийняли власне законодавство. Наприклад, Закон про конфіденційність споживача Каліфорнії (CCPA) містить положення, які стосуються захисту персональних даних у контексті штучного інтелекту.
4. Японія: Японія ухвалила Закон про захист персональних даних, який містить положення про використання штучного інтелекту та інших технологій. Він надає права громадянам на контроль за використанням їх персональних даних.

Висновки. Отже, захист персональних даних у роботі зі штучним інтелектом стає дедалі важливішою проблемою у сучасному світі. Використання штучного інтелекту вимагає уваги до правових аспектів та заходів забезпечення приватності.

Список використаних джерел:

1. World Intellectual Property Organization (WIPO) - Artificial Intelligence and Intellectual Property Policy Considerations. URL: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf.
2. European Commission – Intellectual Property and the Rise of AI.URL: https://ec.europa.eu/jrc/sites/jrcsh/files/jrc114868.pdf.

3. United States Copyright Office - Copyright Office Issues Report on Copyright and the Music Marketplace: https://www.copyright.gov/policy/musiclicensingstudy/.
4. Stanford Law School - Intellectual Property and Artificial Intelligence: A Primer. URL: https://law.stanford.edu/wp-content/uploads/2018/06/Intellectual-Property-and-Artificial-Intelligence-A-Primer.pdf.
5. Рішення Європейського суду у справі «Nash v. Mashreqbank PSC» від 4 березня 2021 року. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62019CJ0310&from=EN.
6. Закон України «Про авторське право та суміжні права» від 23 грудня 1993 року. URL: https://zakon.rada.gov.ua/laws/show/3792-12.
7. Закон США «Про авторське право» (Copyright Act). URL: https://www.copyright.gov/title17/.
8. Звіт Європейської комісії «Підсумки консультацій з громадськістю щодо створення єдиного ринку цифрових товарів та послуг» (англ.). URL: https://ec.europa.eu/info/publications/single-market-strategy-public-consultation-results_en.
9. Стаття «Who Owns AI-Created Works?» на порталі Intellectual Property Watch (англ.). URL: https://www.ip-watch.org/2020/06/05/owns-ai-created-works/.
10. Стаття «AI Created a $16,000,000 Painting, But Who Owns the Rights?» на порталі Art Law Journal (англ.). URL https://artlawjournal.com/ai-created-a-16000000-painting-but-who-owns-the-rights/.
11. Бисага Ю.М., Бєлов Д.М., Заборовський В.В. Штучний інтелект та авторські і суміжні права. *Науковий вісник УжНУ. Серія «Право».* Випуск 76(2). Ч. 2. 2023. С. 299–304.
12. Бєлова М.В., Бєлов Д.М. Імплементація штучного інтелекту в досудове розслідування кримінальних справ: міжнародний досвід. *Аналітично-порівняльне правознавство*. № 2. 2023. С. 448–454.
13. Бисага Ю.М., Бєлова М.В., Бєлов Д.М. Виклики для прав дитини у зв'язку з розвитком штучного інтелекту. *Науковий вісник УжНУ. Серія «Право».* Випуск 77(3). Ч. 1. 2023. С. 88–91.
14. Бєлов Д.М., Бєлова М.В., Штучний інтелект в судочинстві та судових рішеннях, потенціал та ризики. *Науковий вісник УжНУ. Серія «Право».* Випуск 78(4). Ч. 3. 2023. С. 289–294.