УДК 351.81.085 (477)
DOI https://doi.org/10.32850/LB2414-4207.2023.29.06

ДЕЯКІ ОСОБЛИВОСТІ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ ПРИ ВИКОРИСТАННІ ЧАТ-БОТІВ ЗІ ШТУЧНИМ ІНТЕЛЕКТОМ НА ПРИКЛАДІ CHATGPT

Заярний Олег Анатолійович,
доктор юридичних наук, професор,
професор кафедри інтелектуальної
власності та інформаційного права
Навчально-наукового інституту права
Київського національного університету
імені Тараса Шевченка,
Національний консультант
Офісу Ради Європи в Україні
(м. Київ, Україна)

Деркаченко Юлія Вікторівна,
кандидат юридичних наук,
представник Уповноваженого з
інформаційних прав
Секретаріату Уповноваженого
Верховної Ради України з прав людини
(м. Київ, Україна)

У статті проведено дослідження окремих особливостей обробки персональних даних при використанні чат-ботів зі штучним інтелектом на прикладі ChatGPT. На основі аналізу сучасної практики використання вказаних технологій штучного інтелекту виявлено і охарактеризовано основні ризики для суб'єктів персональних даних, обумовлені використанням ChatGPT.

З урахуванням вимог Закону України «Про захист персональних даних», автором обґрунтовано, що мета обробки персональних даних у відносинах, пов'язаних із використанням ChatGPT має бути заздалегідь визначеною, легітимною стосовно призначення обробки персональних даних, а суб'єкт персональних даних має бути завчасно ознайомлений з метою і процедурами використання персональних даних. Також доведено, що набори персональних даних, які обробляються мають бути пропорційними законній меті і підставам обробки. Окрім цього, суб'єкт персональних даних повинен надати однозначну, вільну і поінформовану згоду на обробку його персональних даних з використанням ChatGPT, а особа, яка одержує таку згоду, повинна гарантувати обов'язкове дотримання вимог Закону України «Про захист персональних даних».

У контексті вимог до забезпечення безпеки обробки персональних даних з використанням ChatGPT, аргументовано наукову позицію, відповідно до якої вирішення відповідної проблеми повинно здійснюватися як на стадії проєктування інформаційних ресурсів чи мобільних застосунків, так і безпосередньо на етапі практичного використання штучного інтелекту.

У висновках викладено основні напрями подальшого удосконалення законодавства України про захист персональних даних у сфері використання штучного інтелекту,

запропоновано прийняти окремий Державний стандарт України (ДСТУ) з уніфікованими правилами технічної обробки інформації про фізичну особу з використанням моделі генеративного штучного інтелекту.

Ключові слова: генеративний штучний інтелект, обробка персональних даних, персональні дані, право на невтручання у приватне і сімейне життя, ChatGPT.

EXPLORING PERSONAL DATA PROCESSING IN AI CHATBOTS: A CASE STUDY OF CHATGPT'S ADVANCED FEATURES

Zaiarnyi Oleh Anatoliyovych,
Dr. Habil. (Law), Professor,
Professor at the Department for Intellectual Property and Information Law, Research and Education Institute of Law, Taras Shevchenko National University of Kyiv,
Expert at Council of Europe Office in Ukraine,
(Kyiv, Ukraine)

Derkachenko Yuliia Viktorivna,
Representative of the Commissioner for Information Rights
Secretariat of the Ukrainian Parliament Commissioner for Human Rights
PhD in Law
(Kyiv, Ukraine)

This article delves into the specific aspects of personal data processing in the context of utilizing chatbots with artificial intelligence, using ChatGPT as a prime example. Through a thorough analysis of the current practices involving these AI technologies, the research identifies and characterizes the primary risks that individuals may face concerning their personal data when interacting with ChatGPT.

Considering the requirements outlined in the Law of Ukraine "On the Protection of Personal Data," the author establishes that processing personal data in ChatGPT-related interactions must adhere to predetermined and legitimate purposes. Furthermore, individuals must be adequately informed in advance about the purpose and procedures of personal data usage. The principle of proportionality is emphasized, highlighting that the sets of personal data processed must be reasonable and directly relevant to the legitimate purpose and grounds of processing.

Central to the article's argument is the importance of obtaining unambiguous, free, and informed consent from the subject of personal data when their information is being processed using ChatGPT. It is incumbent upon the recipient of such consent to ensure strict adherence to the requirements stipulated in the Law of Ukraine "On Personal Data Protection." This emphasis on informed consent serves as a vital safeguard to protect user rights and privacy throughout their interactions with AI chatbots.

By examining the intricacies of personal data processing in AI chatbots, this article seeks to promote responsible and ethical use of ChatGPT and similar technologies, contributing to a safer and more transparent digital landscape for all users.

In the realm of ensuring the security of personal data processing using ChatGPT, a well-founded scientific position highlights the necessity of adopting a comprehensive approach.

According to this perspective, tackling this crucial issue involves implementing measures not only during the design and development of information resources or mobile applications but also throughout the practical deployment and utilization of artificial intelligence.

The conclusions put forth in this study outline the key areas for advancing Ukraine's legislation on personal data protection concerning the domain of artificial intelligence. As part of the proposed measures, the author recommends the establishment of a dedicated State Standard of Ukraine (DSTU) incorporating cohesive regulations for the technical processing of personal information using generative artificial intelligence models.

Key words: generative artificial intelligence, personal data processing, personal data, right to non-interference in private and family life, ChatGPT.

Постановка проблеми. Останніми роками у науковій і практичній літературі розгорнулася активна дискусія щодо ризиків і переваг використання чат-ботів зі штучним інтелектом у різних сферах суспільного життя [1, с. 3]. Значною мірою ця дискусія загострилася після створення 30 листопада 2022 року протоверсії чат-бота з багатофункціональним штучним інтелектом – ChatGTP. Здатністю останніх версій вказаного чат-бота аналізувати значні обсяги тексту, опрацьовувати цифрові зображення і на їх основі генерувати профіль людини, моделювати різні ситуації за участю конкретних осіб, поряд з очевидними перевагами, викликали, також багато ризиків. Їх прояв перед усім пов’язаний з обробкою значних обсягів персональних даних, зокрема тих, дії з якими становлять особливий ризик для прав і свобод людини. Так, зокрема, 25 березня 2023 року компанія OpenAI, розробник ChatGPT, оголосила, що причиною витоку персональних даних багатьох користувачів ChatGPT став збій у їхній системі штучного інтелекту. За даними OpenAI, деякі користувачі мали доступ до повних імен, адрес електронної пошти, платіжних адрес, а також останніх чотирьох цифр номерів кредитних карток і термінів їх дії інших користувачів. Йдеться про приблизно 1,2 мільйони підписників платної версії ChatGPT [2].

Враховуючи ризики, пов'язані із застосуванням ChatGTP, наглядовий орган Італії у сфері захисту персональних даних 31 березня 2023 року виніс рішення про обмеження використання вказаного чат-бота в публічному адмініструванні та бізнесі [3].

З метою забезпечення належного врегулювання суспільних відносин, пов'язаних із застосуванням штучного інтелекту, недопущення застосування цих технологій для безпідставного втручання у приватне і сімейне життя, систематизації ризиків у вказаній сфері правового регулювання, у червні 2023 року Європейським парламентом і Радою Європейського Союзу було прийнято «Акт про штучний інтелект» [4]. Зазначеним актом Європейського Союзу пропонується встановити для власників інформаційних систем, заснованих на технологіях генеративного штучного інтелекту зобов'язання щодо недопущення протиправного копіювання авторського контенту, протиправного збору і подальшого профілювання відомостей про фізичних осіб. Таким чином, на сьогоднішній день активне застосування генеративних систем штучного інтелекту актуалізувало перед юридичною наукою, правотворчими та правозастосовчими органами ряд нових завдань, які вимагають свого комплексного вирішення.

Аналіз останніх досліджень та публікацій. Проблематика захисту персональних даних у відносинах, пов'язаних із застосуванням штучного інтелекту, була предметом значної уваги багатьох вчених правників та практиків. Зокрема, Т. Г. Каткова у своїх працях досліджує проблематику конфіденційності персональних даних у відносинах, пов'язаних із застосуванням штучного інтелекту, особливості одержання поінформованої згоди від суб'єктів персональних даних, безпеку даних, тощо [5, с. 50–51]. У працях В. Р. Некрутенка зроблений значний акцент на систематизації правових ризиків,

обумовлених опрацюванням персональних даних з використанням штучного інтелекту, засобам запобігання таких ризиків [6, с. 54]. Предметом уваги С. М. Брайчевського є проблематика мети, підстав та особливостей процедур обробки персональних даних в системі Інтернету речей, заснованих на широкому використанні технологій штучного інтелекту [7, с. 63–64].

Не зважаючи на існування у науковій літературі ґрунтовних наукових розробок проблематики, яка складає предмет дослідження цієї статті, мало дослідженими лишаються окремі особливості правомірної обробки персональних даних з використанням штучного інтелекту. Йдеться, зокрема, про мету, підстави та спеціальні процедури обробки персональних даних в інформаційних системах, заснованих на генеративних моделях штучного інтелекту, перед усім ChatGTP, протидію ризикам, викликаних застосуванням цих технологій.

Метою статті є дослідження особливостей обробки персональних даних у відносинах, пов'язаних із використанням ChatGPT, формулювання окремих пропозицій щодо удосконалення законодавства України про захист персональних даних з відповідних питань.

Завданнями статті є: 1. Аналіз основних способів обробки персональних даних з використанням ChatGPT та виявлення пов'язаних з такою обробкою ризиків для прав суб'єктів персональних даних. 2. Формулювання на основі системного аналізу норм законодавства та практики Європейського Суду з прав людини основних вимог до правомірної обробки персональних даних з використанням ChatGPT. 3. Виявлення особливостей забезпечення безпеки обробки персональних даних у відносинах, пов'язаних з використанням ChatGPT на стадіях розробки інформаційних ресурсів, мобільних застосунків, де передбачається застосування відповідної моделі штучного інтелекту та на етапі практичного застосування ChatGPT. 4. Вироблення окремих пропозицій щодо удосконалення законодавства України про захист персональних даних та практики його застосування у відносинах, які виникають у зв'язку із розробкою і застосуванням генеративних моделей штучного інтелекту.

Виклад основного матеріалу. Створений на мові програмування Python, ChatGPT використовує у своїй роботі техніки навчання з вчителем та навчання з підтримкою. Поєднання зазначених технік навчання дозволяє не лише будувати діалог з ботом, але і враховувати різні, часто протилежні аспекти поставленого завдання, зберігати історію раніше сформованих запитів користувача. При цьому, основним джерелом інформації, з якого одержуються дані для машинного навчання є довідкові сторінки в мережі Інтернет, а також Інтернет-меми [8].

Аналіз вказаних технічних властивостей ChatGPT в контексті обробки персональних даних означає, що:

по-перше вказана технологія переважно пов'язана з обробкою персональних даних, які перебувають у відкритому доступі, або таких, які потрапили у відкритий доступ без згоди суб'єкта персональних даних або його законного представника;

по-друге, ChatGPT здатний до профілювання суб'єктів персональних даних на основі їхніх запитів, тобто групування конкретних наборів ознак людини за конкретними критеріями; має здатність до накопичення персональних даних та створення образу людини на основі узагальнення значного обсягу фотозображень.

Застосування для вказаних цілей ChatGPT може мати наслідком пряме втручання у приватне і сімейне життя конкретної людини через протиправну обробку персональних даних.

На сьогоднішній день, в юридичній літературі і законодавстві відсутній єдиний підхід до тлумачення поняття «приватне і сімейне життя» [9, с. 112].

У своїй практиці Європейський Суд з прав людини (далі – ЄСПЛ), тлумачить поняття «приватне життя» як широку концепцію, що охоплює навіть аспекти професійного життя та публічної поведінки.

Однак, попри розширене тлумачення приватного життя, не всі види обробки персональних даних, включно з використанням ChatGPT можуть вважатись обмеженням прав, передбачених статтею 8 Конвенції про захист прав людини і основоположних свобод.

Якщо ЄСПЛ визнає, що дія з обробки персональних даних, про яку йдеться, вплинула на право особи на повагу до приватного життя, він буде розглядати, чи було втручання виправданим [10, с. 51–52].

З позицій практики ЄСПЛ, втручання в приватне і сімейне життя може бути визнаним правомірним, якщо у кожному окремо взятому випадку виконано такі умови:

Згідно із законом. Практика ЄСПЛ визнає втручання таким, що здійснено згідно із законом, якщо воно передбачено у положеннях національного законодавства, що має певні характеристики. Закон повинен бути «доступним для зацікавлених осіб і передбачуваним щодо наслідків його дії» [10, с. 53].

Так, наприклад, у справі «Ротару проти Румунії» заявник стверджував про порушення його права на повагу до приватного життя у зв'язку зі збереженням та використанням файлу, який містив інформацію про нього Службою безпеки Румунії. ЄСПЛ встановив порушення статті 8 Конвенції про захист прав людини і основоположних свобод через той факт, що румунське законодавство дозволяє збирати, записувати та зберігати в секретних файлах інформацію, яка може зашкодити інтересам національної безпеки, і не передбачає обмежень щодо здійснення цих повноважень, які залишаються на розсуд влади. Наприклад, у національному законодавстві не визначено вид інформації, яку можна обробляти, категорії людей, до яких застосовуються заходи стеження, обставини, за яких можуть бути вжиті такі заходи, або процедури, яких необхідно дотримуватися. З огляду на ці недоліки Суд дійшов висновку, що національне законодавство не відповідає вимозі передбачуваності в контексті статті 8 Конвенції про захист прав людини і основоположних свобод [11].

Переслідування легітимної мети. Легітимна мета може бути або одним із перерахованих суспільних інтересів, або ж якимсь із захищених прав і свобод інших осіб. Легітимними інтересами, які можуть виправдати втручання відповідно до частини другої статті 8 Конвенції про захист прав людини і основоположних свобод, є інтереси національної та громадської безпеки чи економічного добробуту країни, попередження заворушень чи злочинів, захист здоров'я чи моралі або захист прав і свобод інших осіб.

Як приклад визначення вказаного критерія можна вказати на справу «Пек проти Сполученого Королівства» заявник намагався скоїти самогубство, розрізавши собі вени на вулиці, не підозрюючи, що все це записується на камеру відеоспостереження. Після того як поліцейські, що стежили за записами замкнутої системи ТВ-спостереження, врятували його, вони передали відеоматеріал працівникам ЗМІ, які його оприлюднили, не замаскувавши обличчя заявника. ЄСПЛ встановив, що не було жодних відповідних чи достатніх підстав, які б могли виправдати пряме доведення відеоматеріалу до відома громадськості державними органами без отримання згоди заявника або маскування його особи. Суд дійшов висновку, що статтю 8 Конвенції про захист прав людини і основоположних свобод було порушено [12].

Необхідність у демократичному суспільстві. Стосовно цього критерія ЄСПЛ зазначив, що «поняття необхідності означає, що втручання відповідає нагальній суспільній потребі і, зокрема, є пропорційним переслідуваній легітимній меті». При оцінці того, чи є захід необхідним для реагування на нагальну суспільну потребу, ЄСПЛ

розглядає його відповідність та належність відносно мети, яка переслідується. З цією метою Суд може взяти до уваги, чи намагається втручання вирішити питання, яке, якщо його не вирішувати, може мати негативний вплив на суспільство, чи є свідчення того, що втручання може зменшити такий негативний вплив, та які існують більш широкі соціальні погляди на питання, що розглядається [10, с. 53; 56].

Для дотримання тесту необхідності втручання також має бути пропорційним. У практиці ЄСПЛ пропорційність розглядається в межах концепції необхідності.

Пропорційність вимагає, щоб втручання в гарантовані Конвенцією про захист прав людини і основоположних свобод права не було більшим, ніж це необхідно для досягнення легітимної мети, яка переслідується.

Важливими факторами, які мають враховуватися при здійсненні тесту пропорційності, є обсяг втручання, кількість осіб, на яких здійснюється вплив, та гарантії або застереження, що мають на меті обмеження обсягу та негативного впливу на права осіб.

Так, у справі «С. та Марпер проти Сполученого Королівства» два заявника були заарештовані та обвинувачені у вчиненні кримінального порушення. Поліція відібрала в них відбитки пальців і зразки ДНК на підставі Закону про поліцію та кримінальні докази. Заявники так і не були засуджені за вчинення злочинів: один був виправданий судом, а кримінальне провадження щодо другого заявника було закрито. Однак їхні відбитки пальців, профілі ДНК та клітинні зразки зберігались поліцією в базі даних, при цьому національне законодавство дозволяло їх збереження безстроково. Хоча Сполучене Королівство доводило, що збереження даних допомагає в ідентифікації майбутніх злочинців і таким чином переслідувало легітимну мету виявлення та попередження злочинів, ЄСПЛ вирішив, що втручання у право заявників на повагу до приватного життя було не виправданим [13].

Таким чином, з позицій практики ЄСПЛ втручання у приватне і сімейне життя, зокрема, у зв'язку з неправомірним застосування технологій на основі генеративного штучного інтелекту може бути правомірним за умови, якщо воно переслідує легітимну мету, ґрунтується на вимогах національного законодавства та є пропорційним у демократичному суспільстві.

З метою недопущення порушення вказаного права людини, Закон України «Про захист персональних даних» визначив [14] загальні вимоги до обробки персональних даних незалежно від стадії її реалізації. Йдеться, зокрема про вимоги, закріплені у ст. 6, 11, 12 та 14 згаданого Закону України.

Поширення вказаних вимог на відносини, пов'язані з використанням ChatGPT з метою обробки персональних даних означає, що:

по-перше, мета такої обробки має бути заздалегідь визначеною, легітимною стосовно призначення обробки персональних даних, а суб'єкт персональних даних має бути завчасно ознайомлений з метою і процедурами використання персональних даних;

по-друге, набори персональних даних, які обробляються мають бути пропорційними законній меті і підставам обробки;

по-третє, суб'єкт персональних даних повинен надати однозначну, вільну і поінформовану згоду на обробку його персональних даних з використанням ChatGPT, а особа, яка одержує таку згоду повинна гарантувати обов'язкове дотримання вимог Закону України «Про захист персональних даних».

Необхідно зауважити, якщо власник інформаційної системи, заснованої на застосуванні ChatGPT має своє місце реєстрації на території Європейського Союзу, або адресу своєї послуги громадянам ЄС, а так само, як і здійснює обробку персональних даних на території ЄС, на нього поширюються вимоги Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб

у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (далі - Загальний регламент ЄС про захист даних), ст. 4 Регламенту [8].

Дотримання більшості нормативних вимог до обробки персональних даних з використанням ChatGPT є можливим ще до початку процесу обробки персональних даних.

Проте, на відміну від Загального регламенту ЄС про захист даних, Закон України «Про захист персональних даних» не здійснює поділ вимог до процедур правомірної обробки даних за проєктуванням інформаційних систем і технологій та за замовчуванням, тобто при вчиненні окремих дій з персональними даними.

Як випливає зі змісту п. 3 преамбули Рекомендації CM / Rec (2020) 1 Комітету Міністрів державам-членам щодо впливу алгоритмічних систем на права людини, схвалених Комітетом Міністрів Ради Європи 08.04.2020 року, Держави-члени Ради Європи повинні забезпечити, через відповідні законодавчі, регуляторні та наглядові рамки, пов'язані з алгоритмічними системами, щоб суб'єкти приватного сектору, які займаються проектуванням, розробкою та постійним впровадженням таких систем, дотримувалися чинних законів та виконували свої обов'язки щодо дотримання прав людини у відповідності з Керівними принципами ООН у сфері бізнесу та прав людини та відповідними регіональними та міжнародними стандартами [16].

Виходячи зі змісту наведеною рекомендації та враховуючи сучасний законодавчий підхід до забезпечення правомірної обробки персональних даних з використанням алгоритмічних систем, зокрема, ChatGPT можна сформулювати наступні **висновки та рекомендації**:

1. Обробка персональних даних повинна здійснюватися з дотриманням підстав її проведення та на основі добровільної, поінформованої згоди суб'єкта персональних даних за умови додержання легітимної та пропорційної мети обробки.

2. Важливою умовою забезпечення правомірної обробки персональних даних з використанням ChatGPT є дотримання розробниками проєктних рішень, де використовується відповідна технологія безпеки персональних даних за проєктуванням і за замовчуванням.

3. Обґрунтованим вбачається прийняття нової редакції Закону України «Про захист персональних даних» та імплементація Модернізованої редакції Конвенції Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (Конвенції 108+).

4. Доцільним також вбачається прийняття окремого ДСТУ «Технічний захист інформації. Забезпечення права на невтручання у приватне і сімейне життя при застосуванні алгоритмічних систем та ботів».

Список використаних джерел:

1. Заярний О. А. До питання удосконалення способів захисту інформаційних прав фізичних осіб, у відносинах, пов'язаних із застосуванням технологій штучного інтелекту. *Вісник Київського національного університету імені Тараса Шевченка (юридичні науки) № 1(120)/2022*. С. 36–39. URL: http://visnyk.law.knu.ua/images/articles/7-120.pdf (дата звернення 27.06.2023 року).

2. OpenAI виявила причину витоку персональних даних користувачів ChatGPT. 25.03.2023 року. URL: https://enovosty.com/wp-content/themes/newenovosty/fonts/KFOmCnqEu92Fr1Me5A.eot (дата звернення: 27.06.2023 року).

3. В Італі заборонили використання «ChatGTP». 08 квітня 2023 року. URL: https://techno.nv.ua/ukr/it-industry/italy-chatgpt-ban-50314746.html (дата звернення: 27.06.2023 року).

4. В ЄС склали ризики для застосування штучного інтелекту. *Економічна правда від 15.06.2023 року*. URL https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiC7vfC7oGAAxVvhP0HHQPNDrcQFnoECA0QAQ&url=https%3A%2F%2Fwww.epravda.com.ua%2Fnews%2F2023%2F06%2F15%2F701204%2F&usg=AOvVaw1_radPBXuwOWmh_eRo_LO5&opi=89978449 (дата звернення: 27.06.2023 року).

5. Каткова Т. Г. Штучний інтелект в Україні: правові аспекти. *Право і суспільство № 6/2020.* С. 46 – 55. URL: http://pravoisuspilstvo.org.ua/archive/2020/6_2020/10.pdf (дата звернення: 27.06.2023 року).

6. Некрутенко В. Р. До питання систематизації ризиків, спричинених обробленням персональних даних із використанням технології штучного інтелекту. *Вісник Київського національного університету імені Тараса Шевченка (юридичні науки)* № 4(119(021). С. 53–58. URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjHuuqUpoGAAxXDUXcKHdw1DGQQFnoECBAQAQ&url=http%3A%2F%2Fwww.library.univ.kiev.ua%2Fukr%2Fhost%2F10.23.10.100%2Fdb%2Fftp%2Fvisnyk%2Fyurydych_119_2021.pdf&usg=AOvVaw0qcsNTiVvtLFJa9Bg3ykQS&opi=89978449 (дата звернення: 27.06.2023 року).

7. Брайчевський С. М. Проблема персональних даних в системах Інтернету речей з елементами штучного інтелекту. *Інформація і право* № 3(2019). С. 61–67. URL: http://ippi.org.ua/sites/default/files/9_13.pdf (дата звернення: 27.06.2023 року).

8. ChatGPT. URL: https://uk.wikipedia.org/wiki/ChatGPT (дата звернення: 27.06.2023 року).

9. Заярний О.А. Адміністративна деліктологія в інформаційній сфері: проблеми теорії та практики: дис. докт. юрид. наук: спец. 12.00.07. Київ, 2018. 561 с. URL: http://scc.univ.kiev.ua/upload/iblock/d52/dis_Zaiarnyi%20O.A..pdf (дата звернення: 27.06.2023 року).

10. Посібник з Європейського права у сфері захисту персональних даних. К.: К.І.С., 2020. 436 с. URL: https://rm.coe.int/data-protection-handbook-ukr-2020-block-web/1680a1f65e (дата звернення: 27/06/2023 року).

11. Рішення Європейського Суду з прав людини у справі «Ротару проти Румуныъ»/ (Велика палата) 04/042000 року. URL: http://eurocourt.in.ua/Article.asp?AIdx=212 (дата звернення: 27/06/2023 року)/

12. Рішення Європейського Суду з прав людини у справі «Пек проти Об'єднаного Королівства». URL: https://zakon.rada.gov.ua/laws/show/980_165#Text (дата звернення: 27.06.2023 року).

13. Рішення Європейського Суду з прав людини у справі «С. та Марпер проти Сполученого Королівства» (Велика палата)/ 04.12.2008 року URL: https://hudoc.echr.coe.int/fre#%7B%22tabview%22:[%22document%22],%22itemid%22:[%22001-117816%22]%7D (дата звернення: 27.06.2023 року).

14. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17. (дата звернення: 27.06.2023 року).

15. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679. (дата звернення: 27.06.2023 року).

16. Рекомендація CM / Rec (2020) 1 Комітету Міністрів державам-членам щодо впливу алгоритмічних систем на права людини від 08.04.2020 року. URL: Рекомендація CM/Rec (2020)1 від 08.04.2020 | ECHR: Ukrainian Aspect (дата звернення: 27.06.2023 року).