УДК 342.7:004.8
DOI https://doi.org/10.24144/2788-6018.2025.04.2.24

НАГЛЯД НАЦІОНАЛЬНИХ ОРГАНІВ ЄС ІЗ ЗАХИСТУ ДАНИХ ЗА ОБРОБКОЮ ПЕРСОНАЛЬНИХ ДАНИХ СИСТЕМАМИ ШТУЧНОГО ІНТЕЛЕКТУ (НА ПРИКЛАДІ CHATGPT)

Гачкевич А.О.,
кандидат юридичних наук, доцент,
доцент кафедри міжнародного та кримінального права
НУЛП «Львівська політехніка»
ORCID: 0000-0002-8494-1937

Гачкевич А.О. Нагляд національних органів ЄС із захисту даних за обробкою персональних даних системами штучного інтелекту (на прикладі ChatGPT).

У статті порушена проблема захисту персональних даних в умовах швидкого розвитку та поширення штучного інтелекту, яка черговий раз актуалізує тематику взаємозв'язку прав людини та новітніх технологій. Фокус уваги зосереджений на правомірності обробки персональних даних системами штучного інтелекту, зважаючи на досвід нагляду національних органів ЄС із захисту даних. Інтерес до проблематики прав людини та штучного інтелекту серед іншого пояснюється залежністю штучного інтелекту від величезних обсягів інформації, включаючи персональні дані, – для того, щоб системи штучного інтелекту були максимально корисним, вони повинні бути забезпечені даними в якнайбільшій кількості. Сьогодні широко застосовуваними стали чат-боти на базі штучного інтелекту, в першу чергу ChatGPT від OpenAI, здатні імітувати вміння спілкуватись. Розробку та використання таких чат-ботів супроводжує виникнення небезпек для захисту персональних даних, вже відзначених національними органами ЄС із захисту даних. У статті пояснені особливості правового статусу національних органів ЄС із захисту даних та наведений перелік їхніх повноважень, спрямованих на забезпечення того, щоб обробка персональних даних системами штучного інтелекту відбувалась у відповідності до стандартів Загального регламенту про захист даних (GDPR). Автор статті розглядає детально кейс «Garante Італії проти OpenAI», пов'язаний з тим, що національний орган Італії з захисту даних виявив порушення порушення правил Загального регламенту про захист даних при навчанні та використанні ChatGPT. У статті наведені відомості про інші кейси за участю OpenAI, ініційовані AEPD Іспанії та UODO Польщі, а також про скарги подані до Datenschutzbehörde Австрії та Datatilsynet Норвегії. Результати дослідження можуть бути цінними для вдосконалення системи захисту персональних даних в Україні – прийняті в Європейському Союзі прогресивні підходи та методи слід враховувати національним органам, які контролюють додержання вимог законодавства щодо персональних даних, а також адаптуватись до високих стандартів ЄС приватним компаніям з огляду на євроінтеграційні прагнення України.

Ключові слова: захист персональних даних, обробка персональних даних, ChatGPT, Загальний регламент про захист даних, Garante Італії проти OpenAI, національні органи ЄС із захисту даних, навчання моделей штучного інтелекту, розробка систем штучного інтелекту, сучасні технології та права людини.

Hachkevych A.O. The Supervision of EU National Data Protection Authorities over personal data processing by AI Systems (The case of ChatGPT).

The article addresses the issue of personal data protection in the context of the rapid development and proliferation of artificial intelligence. This issue once again highlights the complex relationship between human rights and emerging technologies. The focus is on the legitimacy of processing personal data by AI systems, taking into account the experiences of EU national data protection authorities supervisory activities. The growing interest in AI-related human rights issues, among other things, stems from the dependence of artificial intelligence on vast amounts of information, including personal data. To be as helpful as possible, AI systems should be provided with extensive input of data. Among the AI systems widely used today, chatbots based on artificial intelligence, particularly ChatGPT by OpenAI, have gained significant popularity due to their ability to mimic human communication skills. The development and use of such chatbots is accompanied by the emergence of dangers to personal data protection, which the EU national data protection authorities have already noted. The article outlines the specifics of the legal status of EU national data protection authorities and lists their powers designed to ensure that personal data processing by AI systems complies with the stringent standards of the General Data

Protection Regulation. The author thoroughly examines the case of Garante of Italy v. OpenAI that revolves around data protection violations revealed by the Italian national data protection authority due to the lack of GDPR compliance regarding how ChatGPT operates. The article also summarizes cases involving OpenAI and initiated by AEPD of Spain, UODO of Poland, and complaints addressed to Datenschutzbehörde of Austria and Datatilsynet of Norway. The findings of this study may contribute to enhancing Ukraine's personal data protection system. It is essential for national authorities responsible for monitoring and enforcing personal data protection to consider the progressive approaches and methods adopted in the EU and for private companies to adapt to EU standards, especially given the aspirations of Ukraine for European integration.

Key words: personal data protection, personal data processing, ChatGPT, General Data Protection Regulation, Garante (Italy) v. ChatGPT, national data protection authorities, training AI models, development of AI systems, modern technologies and human rights.

Постановка проблеми. Проблема захисту персональних даних викликає особливий інтерес в умовах швидкого розвитку та поширення штучного інтелекту. Даний інтерес великою мірою обумовлений тим, що штучний інтелект залежить від величезних обсягів інформації, включаючи персональні дані. Для того, щоб зробити системи штучного інтелекту максимально корисним, розробники повинні забезпечувати їх даними в якнайбільшій кількості.

При цьому потреба моделей та систем штучного інтелекту в інформації породжує небезпеки для захисту персональних даних та відповідно дотримання прав людини. Як показує досвід національних органів ЄС із захисту даних (далі – національних органів ЄС), розробка та використання систем штучного інтелекту неодноразово викликали занепокоєння та швидше за все викликатимуть надалі через порушення правил Загального регламенту про захист даних (далі – GDPR). Виходячи з цього, фокус уваги в даній статті зосереджений на дослідженні правомірності обробки персональних даних системами штучного інтелекту.

Порушена у статті проблема належить до тематики взаємозв'язку прав людини та новітніх технологій, значимість якої зростає пропорційно до того, наскільки істотно технологічний прогрес впливає на суспільство. Одним з проявів такого впливу, можливо найбільш помітним за останні роки, стала поява чат-ботів на базі штучного інтелекту (ChatGPT від OpenAI, Google Gemini, Microsoft Copilot, Claude від Anthropic тощо), здатних розуміти по-своєму питання користувачів та давати відповіді на них, тим самим імітуючи людину-співрозмовника.

Метою пропонованої статті є узагальнення досвіду нагляду національних органів ЄС за дотриманням стандартів Загального регламенту про захист даних при обробці персональних даних системами штучного інтелекту, взявши за основу широко застосовуваний чат-бот ChatGPT від OpenAI.

Стан опрацювання проблематики. Правовий статус та діяльність національних органів ЄС із захисту даних були предметом вивчення низки українських вчених. Р. Пристай розглядає особливості законодавчого регулювання та практичної діяльності національних органів з захисту персональних даних в ЄС у соціальних мережах [1]. К. Мельник пояснює, які саме інституції – наддержавні органи ЄС та національні установи – здійснюють контроль над відповідністю законодавчим вимогам Європейського Союзу процесів обробки персональних даних [2]. Різак М. досліджує особливості організації та діяльності уповноваженого органу з питань захисту персональних даних, включаючи практику таких держав ЄС, як Австрія, Бельгія та Німеччина [3]. Слід відзначити, що в українській правовій науці питання, споріднені з діяльністю національних органів ЄС із захисту даних, також вивчали: В. Брижко, Ю. Коваленко, І. Кульчій, О. Легка, Я. Овчаренко, В. Проценко, О. Різенко, О. Рогова, В. Серьогін, О. Шевчук та ін.

Питання захисту персональних даних при розробці та використанні систем штучного інтелекту належить до активно обговорюваних серед українських вчених (Арзянцева Д., Бєлов Д., Бєлова М., Брайчевський С., Деркаченко Ю., Дорош В., Дубняк М., Заярний О., Карапетян О., Колесніков А., Косілова О., Кронівець Т., Некрутенко В., Остіян Є., Пунда О., Санжаровська Л., Солодовнікова Х. тощо). Такий стан речей, на нашу думку, позитивно впливає на підвищення обізнаності громадськості з основами захисту персональних даних та поступово мав би призвести до меншої кількості порушень прав людини. Окремо виділимо кілька статей, в яких розглянуті: виклики та загрози захисту персональних даних у роботі зі штучним інтелектом [4], порушення права на конфіденційність та приватність фізичних осіб внаслідок впровадження штучного інтелекту всюди [5], використання персональних даних для розробки та застосування чат-ботів на основі штучного інтелекту (на прикладі ChatGPT) [6].

Зауважимо, що в іноземній правовій науці захист персональних даних під час розробки та використання систем штучного інтелекту як напрям досліджень розвивається дуже активно відтоді, як

було прийнято GDPR (С. Вахтер, Ф. Ладжіоя, Л. Мітроу, Б. Міттелштадт, Дж. Сартор, Ч. Тейлор та багато інших), а також охоплює все більше й більше нових питань після появи ChatGPT.

Виклад основного матеріалу. Національні органи ЄС належать до інституційної системи забезпечення дотримання прав людини в державах-учасницях ЄС, поряд з наддержавними органами ЄС – Європейським інспектором із захисту даних та Європейською радою із захисту даних (далі – EDPB).

Європейський інспектор із захисту даних (також – Європейський уповноважений з захисту даних) за характером діяльності нагадує омбудсмена, водночас, його функції спеціалізовані навколо захисту персональних даних [2, с. 58], тоді як EDPB має на меті не тільки забезпечувати однакове застосування положень GDPR на території ЄС, а й сприяти тому, щоб національні органи ЄС співпрацювали між собою (до її складу входять і Європейський інспектор із захисту даних, і чільники національних органів ЄС).

Загалом ідея запровадження національних органів ЄС полягала в тому, щоб незалежні від інших органів влади інституції здійснювали нагляд за тим, наскільки в даній держав дотримані стандарти ЄС щодо захисту персональних даних (які, у порівнянні з іншими регіонами світу, є дуже високими). Беручи до уваги твердження М. Різака щодо свого роду підпорядкування національних органів ЄС (також – уповноважених органів з питань захисту персональних даних) парламенту [3, с. 623], вважаємо, що навіть за такої формальної залежності може бути забезпеченою їхня повна самостійність, що підтверджує приклад суддів.

Правовою формою для реалізації цієї ідеї стали відповідні положення глави 6 GDPR, зокрема ст. 51–59 [7].

1. Обов'язок держав запровадити один або декілька незалежних органів для моніторингу застосування положень GDPR у цілях забезпечення основних прав і свобод фізичних осіб щодо обробки персональних даних. Крім того, наголошено на необхідності сприяння вільному руху персональних даних у межах ЄС – хоча самі по собі обробка персональних даних пов'язана з багатьма ризиками, особливо в транскордонному форматі, GDPR заохочує до неї, якщо персональним даним гарантована захищеність (ст. 51).

2. Національні органи ЄС повинні робити усе можливе, щоб положення GDPR застосовувались однаково, в тому числі – співпрацювати між собою (під координуванням EDPB) та з Європейською комісією (ст. 51).

3. У діяльності, яка зумовлена завданнями та відповідає повноваженням, національні органи ЄС володіють незалежністю, а їхнім членам гарантоване невтручання у посадову діяльність (ст. 52).

4. Члени національних органів ЄС призначаються відповідно до прозорої процедури за рішеннями вищих органів державної влади з-поміж осіб належної кваліфікації, з релевантним досвідом у сфері захисту персональних даних (ст. 53).

5. Обов'язок держави прийняти на законодавчому рівні положення щодо формування складу національних органів ЄС, включаючи вимоги до їхніх членів та процедурні правила (ст. 53-54).

6. За загальним правилом повноваження національних органів ЄС поширюються на територію відповідної держави (ст. 55), водночас, у випадку транскордонної обробки даних – слід застосовувати принцип one-stop-shop, який відіграє важливу роль для вивчення досвіду національних органів ЄС щодо дотримання прав людини під час обробки персональних даних системами штучного інтелекту.

Принцип one-stop-shop, або принцип «єдиного вікна», – ми також вважаємо, як і Р. Пристай [1, с. 248], такий варіант перекладу буде найбільш зрозумілим україномовним аналогом, відображаючи відносно нову можливість обслуговування з цілої низки питань в одному місці державними органами або органами місцевого самоврядування, – означає те, що у випадках, коли обробка персональних даних пов'язана з територією більш, ніж однієї держави, повноваження здійснює національний орган ЄС тієї держави, де має місцезнаходження контролер або оператор (ст. 56). Такий принцип пояснює, чому ірландський орган вправі розглядати нові претензії до компанії OpenAI.

Положення GDPR детально визначають компетенцію (ст. 55-56), завдання (ст. 57) і повноваження національних органів ЄС (ст. 58). На нашу думку, квінтесенцією їхньої наглядової діяльності є три ключові ролі:

- слідчого (investigative powers), що дозволяє з'ясовувати усі обставини, які мають відношення до ймовірних порушень захисту персональних даних (п. 1 ст. 58) на підставі отриманих скарг або за власною ініціативою після того, як членам стали відомі факти недотримання GDPR контролерами або операторами даних;
- судді (corrective powers), який вправі по відношенню до контролерів та операторів надсилати попередження, виносити догани, наказувати, встановлювати тимчасові або остаточні обмеження, прикладом яких є заборона доступу до ChatGPT на території Італії навесні 2023 р., тим самим сприяючи виправленню ситуації (п. 2 ст. 58);

- експерта (authorisation and advisory powers), який консультує щодо того, як забезпечити більш ефективний захист персональних даних, роз'яснює будь-яке питання для органів державної влади або громадськості, схвалює кодекси поведінки, згадані у ст. 40 GDPR, та стандартні договірні положення (ст. 28, 46).

Серед усіх національних органів ЄС саме італійський слід виокремити в першу чергу, адже починаючи від березня 2023 р. Garante Італії (офіційна назва – Garante per la protezione dei dati personali) з захисту даних виявляв порушення правил GDPR при навчанні та використанні ChatGPT та висловлював претензії до OpenAI через те, що обробка персональних даних відбувалась неналежним чином. Таблиця 1 містить найважливіші відомості про кейс «Garante Італії проти OpenAI», підготовлені на основі новинних повідомлень [8–11], а також офіційної інформації з веб-сайту Garante [12–15].

Таблиця 1

Дата події	**Опис події**	**Правова оцінка**
20 березня 2023	Стало відомо про витік даних, які стосувались розмов користувачів з ChatGPT та платіжної інформації.	Ст. 33 GDPR зобов'язує повідомляти про подібні інциденти якнайшвидше національні органи ЄС.
30 березня	Garante внаслідок можливих порушень захисту персональних даних прийняв рішення тимчасово обмежити обробку персональних даних компанією OpenAI як контролером персональних даних, що стосувались суб'єктів даних з Італії, та розслідувати питання більш детально за екстреною процедурою.	Позиція Garante: Open AI не виконує зобов'язання з надання інформації про збір і обробку даних при застосуванні ChatGPT; правова підстава для обробки в цілях навчання алгоритмів не названа; дані можуть бути неточними; відсутні засоби перевірки користувачів, які ще не досягли віку 14 років.
5 квітня	Представники OpenAI, серед них С. Альтман, та члени Garante провели конференцію онлайн. OpenAI: висловили готовність співпрацювати з Garante та підтвердили свою переконаність в тому, що вимоги GDPR слід забезпечувати. Garante: заявили про те, що вони не є противниками штучного інтелекту та прогресу технологій, а також закликали дотримуватись правил GDPR.	Ключові позиції сторін відображають дилему орієнтирів для права: технологічний прогрес, коли дотримання прав людини НЕ може бути забезпеченим повністю, зокрема права на приватність, чи цілковите дотримання прав людини, коли поява нових і нових технічних можливостей кращого задоволення людських потреб НЕ може ставати виправданням порушень.
6-7 квітня	Проведені подальші переговори, OpenAI представила Garante свої пояснення щодо пред'явлених претензій, а також надала інформацію щодо подальших дій стосовно виправлення статус-кво.	OpenAI прокоментувала своє відношення до приватності як цінності інтересом у вивченні світу, а не індивідів. Важливі обіцянки мали відношення до істотного скорочення даних для навчання ChatGPT, а також гарантована його відмова надавати таку інформацію, яка має характер конфіденційної.

Закінчення таблиці 1

11 квітня	Garante оприлюднив перелік вимог до OpenAI, які стосувались (1) інформування про збір та обробку персональних даних, а також їхній зв'язок з навчанням алгоритмів ChatGPT, (2) надання можливостей відмовитись від обробки персональних даних користувачам та (3) виправляти дані, які не є точними або актуальними, (4) вдосконалення політики конфіденційності та підвищення її видимості, (5) опції перевірки віку, (6) проведення інформаційної кампанії.	Для визначення правової підстави для обробки персональних даних в цілях навчання систем штучного інтелекту Garante рекомендував взяти до уваги згоду (у тих випадках, коли суб'єкт даних надає дозвіл), або законний інтерес, який вимагає співставлення цінностей (ст. 6 GDPR).
28 квітня	ChatGPT став знову доступним для користувачів з Італії після того, як компанія OpenAI вирішила окремі проблемні питання.	

Кульмінацією кейсу став грудень 2024 р., – Garante завершив своє розслідування та прийняв рішення стосовно OpenAI. Хоча компанія раніше виконала низку вимог та співпрацювала з італійським національним органом ЄС для того, щоб забезпечувати більш ефективне дотримання стандартів GDPR, за неправомірну обробку персональних даних для навчання ChatGPT (відсутність правової підстави), а також порушення принципу прозорості присуджений штраф у розмірі 15 млн. євро. Крім того, компанію OpenAI зобов'язали провести шестимісячну інформаційну кампанію за власний рахунок про процеси обробки даних ChatGPT та права користувачів відповідно до GDPR [16]. Слід додати, рішення Garante базується на низці положень GDPR, насамперед ст. 5-6, 8, 13.

EAPD Іспанії проти OpenAI. Варто відзначити, паралельно з Італією, ситуація стосовно можливих порушень захисту персональних даних викликала занепокоєння в Іспанії, де національний орган ЄС розпочав своє розслідування у квітні 2023 р. У прес-релізі ми зустрічаємо вже знайому пару цінностей: сприяння розвитку інноваційних технологій, таких як штучний інтелект, а також – дотримання прав та свобод людини [17]. Варто зауважити, що представник EAPD, коментуючи цю ситуацію, відзначив необхідність координування рішень на європейському рівні, – практично в той сам час була створена спеціальна робоча група під егідою EDPB [18]. На момент написання статті жодної інформації про рішення по суті немає.

UODO Польщі проти OpenAI. Схожі претензії до обробки даних ChatGPT стали предметом скарги, направленої до польського національного органу ЄС (Urząd Ochrony Danych Osobowych) у серпні 2023 р. В чому саме скаржник вбачав порушення захисту персональних даних?

По-перше, отримавши неточну інформацію про себе, він не отримав можливості виправлення даних. По-друге, йому не було повідомлено, які саме відомості підлягають обробці. По-третє, скаржник апелював до недотримання принципів ст. 5, насамперед принципу прозорості. По-четверте, за оцінками скаржника, після того, як компанія OpenAI отримала його персональні дані у 2021 р., вона була зобов'язаною поінформувати про факт використання таких даних для навчання моделей штучного інтелекту, як і про джерело отримання. Зауважимо, що скаржник у своїх поясненнях звертав увагу на політику конфіденційності та наводив листування як доказ того, що компанія не виконує стандарти GDPR [19].

Незважаючи на те, що розслідування цієї ситуації розпочалось майже 2 роки тому, до цього часу не повідомлено про прийняття рішення.

Datenschutzbehörde Австрії та Datatilsynet Норвегії. Правозахисна організація NOYB (Європейський центр цифрових прав) подала скаргу до австрійського національного органу ЄС у квітні 2024 р., щоб той розпочав розслідування з приводу правомірності методів обробки даних OpenAI – чи відповідають вони стандартам захисту персональних даних ЄС [20]. Скарга пов'язана з тим, що право суб'єкта даних на доступ не забезпечується (ст. 15 GDPR), як і точність даних (ст. 5). ChatGPT надавав недостовірну інформацію про дату народження публічної людини, виправити яку не вдавалось.

Ще одна скарга, яка була також подана NOYB, адресована норвезькому національному органу ЄС. Користувач ChatGPT отримав недостовірну інформацію про себе за запитом: "Who is Arve Hjalmar Holmen?" [21]. Крім прохання оштрафувати компанію OpenAI, у скарзі зазначено, що такі вихідні дані повинні бути видалені. Натомість саму систему штучного інтелекту слід вдосконалена, щоб результати, які вона видає, були точними.

З великою ймовірністю затримки у правових оцінках даних ситуацій відбуваються внаслідок того, що національні органи ЄС можуть не тільки проводити розслідування, а й шукати спільні підходи до вирішення проблемних питань. Робоча група під егідою EDPB опублікувала у травні 2024 р. свій звіт, присвячений обробці персональних даних ChatGPT [22].

У звіті вказано, що з 15 лютого 2024 р. місцезнаходженням OpenAI на території ЄС є Ірландія – всі спірні ситуації, зумовлені транскордонною обробкою даних, будуть під наглядом ірландського національного органу ЄС. Разом з тим, це не стосується кейсів, що ініційовані раніше, як-от перелічених вище. Частиною звіту є спеціальна анкета для заповнення під час розслідування, завдяки якій буде впроваджуватись більш-менш однаковий підхід до нагляду. Крім того, відзначено те, що OpenAI вже вдосконалила політику конфіденційності та зробила інші важливі кроки в напрямку стандартів GDPR.

Додамо, що звіт акцентує увагу на 3 правилах, дотримання яких впливає на правомірність обробки персональних даних ChatGPT як системою штучного інтелекту:

– на усіх етапах функціонування – від збору даних до розмов з користувачами – повинна бути визначена правова підстава (ст. 6), в тому числі – стосовно чутливих даних;

– застереження щодо того, що контролер даних не несе відповідальності за безпеку даних, не може розглядатись як звільнення його від зобов'язань дотримуватись положень GDPR (ст. 51);

– обов'язок інформування користувачів залежить від того, в який спосіб відбувається збір даних – через вебскрейпінг чи в процесі взаємодії з ChatGPT (тоді слід інформувати користувачів про використання персональних даних для навчання систем штучного інтелекту).

Висновки. Широко застосовувані чат-боти на базі штучного інтелекту породжують ризики та небезпеки для захисту персональних даних, природа яких залишається не до кінця дослідженою. З одного боку, характерний для штучного інтелекту феномен чорної скриньки, яка приховує все, що відбувається всередині, пояснює, чому навіть оператори та контролери даних не знають достеменно, в який спосіб система обробляє дані. Набагато простіші причинно-наслідкові зв'язки між даними у технологіях попередніх поколінь, які були більш придатними для пояснення фахівцями, сформували очікування щодо того, що правомірна обробка персональних даних – не є проблемою для добросовісного контролера чи оператора. Такі очікування навряд чи зможуть виправдати сучасні компанії у сфері штучного інтелекту.

З іншого боку, прагнення до технологічного прогресу не може бути тим аргументом, який зумовлює зміну балансу на користь вдосконалення моделей та систем штучного інтелекту, для яких найважливішим ресурсом залишаються дані, нехтуючи забезпеченням дотримання прав людини, зокрема права на приватність. Безумовно, діяльність таких незалежних інституцій, як національні органи ЄС, має важливе значення для реалізації цінності захисту персональних даних. Своєю можливістю впливати на операторів та контролерів даних, включаючи приватні компанії з величезними доходами, такі органи спроможні не тільки розслідувати ситуації щодо порушень захисту персональних даних, які вже відбулись, а й змінювати суспільство відповідно до ідеалів, на яких розроблявся Загальний регламент про захист даних. Підтвердженням того, наскільки важливе значення мають національні органи ЄС став кейс Garante Італії проти OpenAI, розглянутий детально у цій статті.

Результати цього дослідження можуть бути цінними для вдосконалення системи захисту персональних даних в Україні, яка, на жаль, не має своєї незалежної інституції. Прийняті в Європейському Союзі прогресивні підходи та методи слід враховувати національним органам, які контролюють додержання вимог законодавства щодо персональних даних, а також адаптуватись до високих стандартів ЄС приватним компаніям, зокрема у сфері інформаційних технологій, з огляду на євроінтеграційні прагнення України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Пристай Р. Національні органи захисту даних в Європейському Союзі: роль і практика в сфері захисту персональних даних в соціальних мережах. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Т. 2, № 82. С. 245–252. DOI: https://doi.org/10.24144/2307-3322.2024.82.2.39.
2. Мельник К. Інституційно-правовий захист персональних даних в Європейському Союзі. *Jurnalul juridic national: teorie şi practică*. 2014. Numărul 3 (7). Pag. 275–280.
3. Різак М. Правовий статус уповноваженого органу з питань захисту персональних даних: досвід зарубіжних країн. *Форум права.* 2012. № 3. С. 619–625.
4. Бєлова М., Бєлов Д. Виклики та загрози захисту персональних даних у роботі зі штучним інтелектом. *Науковий вісник Ужгородського університету. Серія: Право.* 2023. Т. 2, № 79. С. 17–22. DOI: https://doi.org/10.24144/2307-3322.2023.79.2.2.

5. Остіян Є. Штучний інтелект та персональні дані: захист приватності в цифровому середовищі. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Т. 3, № 85. С. 47–53. DOI: https://doi.org/10.24144/2307-3322.2024.85.3.7.
6. Заярний О., Деркаченко Ю. Деякі особливості обробки персональних даних при використанні чат-ботів зі штучним інтелектом на прикладі ChatGPT. *Юридичний бюлетень.* 2023. Вип. 29. С. 55–62.
7. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *An official EU website.* URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (дата звернення: 15.06.2025).
8. McCallum S. ChatGPT banned in Italy over privacy concerns. *BBC.* URL: https://www.bbc.com/news/technology-65139406 (дата звернення: 15.06.2025).
9. Pollina E., Armellini A. Italy fines OpenAI over ChatGPT privacy rules breach. *Reuters.* URL: https://www.reuters.com/technology/italy-fines-openai-15-million-euros-over-privacy-rules-breach-2024-12-20/ (дата звернення: 15.06.2025).
10. Hood L. ChatGPT: lessons learned from Italy's temporary ban of the AI chatbot. *The Conversation.* URL: https://theconversation.com/chatgpt-lessons-learned-from-italys-temporary-ban-of-the-ai-chatbot-203206 (дата звернення: 15.06.2025).
11. Italy's privacy watchdog fines OpenAI €15 million after probe into ChatGPT data collection. *Euronews.* URL: https://www.euronews.com/next/2024/12/20/italys-privacy-watchdog-fines-openai-15-million-after-probe-into-chatgpt-data-collection (дата звернення: 15.06.2025).
12. Provvedimento del 30 marzo 2023 [9870832*]. Garante per la protezione dei dati personali.* URL: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832 (дата звернення: 15.06.2025).
13. ChatGPT: OpenAI collabora con il Garante privacy con impegni per tutelare gli utenti italiani. *Garante per la protezione dei dati personali.* URL: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9872832 (дата звернення: 15.06.2025).
14. Provvedimento dell'11 aprile 2023 [9874702]. *Garante per la protezione dei dati personali.* URL: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874702 (дата звернення: 15.06.2025).
15. ChatGPT: OpenAI riapre la piattaforma in Italia garantendo più trasparenza e più diritti a utenti e non utenti europei. *Garante per la protezione dei dati personali.* URL: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9881490 (дата звернення: 15.06.2025).
16. Comunicato stampa - ChatGPT, il Garante privacy chiude l'istruttoria. OpenAI dovrà realizzare una campagna informativa di sei mesi e pagare una sanzione di 15 milioni di euro. *Garante per la protezione dei dati personali.* URL: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10085432 (дата звернення: 15.06.2025).
17. Spain opens an investigation into OpenAI's ChatGPT over a potential data breach. *Euronews.* URL: https://www.euronews.com/next/2023/04/14/spain-opens-an-investigation-into-openais-chatgpt-over-a-potential-data-breach (дата звернення: 15.06.2025).
18. Spain asks EU data protection board to discuss OpenAI's ChatGPT. *Reuters.* URL: https://www.reuters.com/technology/spains-data-regulator-asks-eu-data-protection-committee-evaluate-chatgpt-issues-2023-04-11/ (дата звернення: 15.06.2025).
19. The technology has to be compliant with the GDPR. *Urząd Ochrony Danych Osobowych.* URL: https://uodo.gov.pl/en/553/1567 (дата звернення: 15.06.2025).
20. Complaint. *European Center for Digital Rights.* URL: https://noyb.eu/sites/default/files/2024-04/OpenAI%20Complaint_EN_redacted.pdf (дата звернення: 15.06.2025).
21. Norway: OpenAI faces GDPR complaint over ChatGPT's defamatory AI hallucinations. *Business and Human Rights Resource Centre.* URL: https://www.business-humanrights.org/en/latest-news/norway-openai-faces-gdpr-complaint-over-chatgpts-defamatory-ai-hallucinations (дата звернення: 15.06.2025).
22. Report of the work undertaken by the ChatGPT Taskforce. *European Data Protection Board.* URL: https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf (дата звернення: 15.06.2025).