

ПІШТА В. І.,

доктор філософії,
доцент кафедри адміністративного,
фінансового та інформаційного права
(Державний вищий навчальний
заклад «Ужгородський національний
університет»)

ВІХЛЯЄВ М. Ю.,

доктор юридичних наук, професор,
професор кафедри адміністративного,
фінансового та інформаційного права
(Державний вищий навчальний
заклад «Ужгородський національний
університет»)

ГЕРЕВИЧ М. О.,

доктор філософії,
доцент кафедри теорії та історії держави
і права
(Державний вищий навчальний
заклад «Ужгородський національний
університет»)

Стаття поширюється на умовах
ліцензії CC BY 4.0

УДК 342.9:004.67:004.8

DOI <https://doi.org/10.32842/2078-3736/2025.4.1.30>

ПІДВИЩЕННЯ ПРОЗОРОСТІ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

У цій статті розглянуто особливості підвищення прозорості обробки персональних даних за допомогою штучного інтелекту, що особливо актуально, зважаючи на стрімкий розвиток цифрових технологій, та того факту, що кількість створених даних постійно збільшується. Зазначено, що кожного року кількість даних, які створюються користувачами цифрових сервісів, соціальних мереж, месенджерів та платформ електронної комерції, зростає. Звертається увага на те, що ринок брокерів даних також зростає. Визначено, що важливими проблемами, які стосуються цифрового середовища є: недосконалість політик конфіденційності, велика кількість суб'єктів, які беруть участь у процесі обробки персональних даних, а також низький рівень обізнаності та практичних навичок у суб'єктів персональних даних щодо захисту своїх прав.

Здійснено аналіз досліджень, які акцентують увагу на тому, що більшість політик конфіденційності важко читати. До того ж політики конфіденційності не відповідають вимогам законодавства та можуть передаватися третім особам непрозоро. Важливо, що ще одним фактором, який відіграє роль у захисті даних, є низький рівень онлайн-грамотності та практичних навичок суб'єктів персональних даних.



Обґрунтовано, що застосування штучного інтелекту дозволить спростити складні тексти політик конфіденційності, а з іншого боку – створювати інструменти, які допоможуть краще контролювати власні дані. Описано можливості платформи конфіденційності, яка за допомогою інтеграції штучного інтелекту, може підвищити прозорість обробки персональних даних. Акцентовується увага на потребі законодавчих змін, що мають посприяти ефективному функціонуванню платформи конфіденційності та гармонізації українського законодавства з європейським задля забезпечення реалізації права суб'єкта персональних даних на поінформованість та належне пояснення того, як саме використовуються його персональні дані.

Ключові слова: *персональні дані, штучний інтелект, прозорість персональних даних, політика конфіденційності, платформа конфіденційності.*

Pishta V. I., Vikhliaiev M. Yu., Herevych M. O. Enhancing transparency in personal data processing using artificial intelligence

This article examines the features of enhancing the transparency of personal data processing using artificial intelligence, which is especially relevant given the rapid development of digital technologies and the fact that the amount of data generated is constantly increasing. It is noted that the amount of data generated by users of digital services, social networks, messengers and e-commerce platforms is growing. It is also emphasized that the data broker market is expanding. It was found that key problems of the digital environment include imperfect privacy policies, a large number of subjects involved in the process of processing personal data, as well as a low level of awareness and practical skills of personal data subjects in protecting their rights.

An analysis of studies was carried out, which emphasize that most privacy policies are difficult for users to understand. In addition, privacy policies do not meet the requirements of the law and can be transferred to third parties in a non-transparent way. It is important that another factor that plays a role in data protection is the low level of online literacy and practical skills among data subjects.

It is substantiated that the use of artificial intelligence will simplify the complex texts of privacy policies, and on the other hand, develop tools that help individuals exercise greater control over their data. The possibilities of a privacy platform are described, which, through the integration of artificial intelligence, can increase the transparency of personal data processing. The need for legislative changes is emphasized, which should contribute to the effective functioning of the privacy platform and the harmonization of Ukrainian legislation with European legislation in order to ensure the exercise of the right of the personal data subject to information and a proper explanation of how his personal data is used.

Key words: *personal data, artificial intelligence, personal data transparency, privacy policy, privacy platform.*

Актуальність обраної нами теми зумовлена тим, що в сучасному світі створюється велика кількість даних, процеси обробки яких часто є малозрозумілими для суб'єктів персональних даних. Це може призводити до порушень з боку володільців, розпорядників чи третіх осіб. Саме тому штучний інтелект (далі – ШІ) може стати інструментом, який буде пояснювати суб'єкту персональних даних ключові положення щодо поводження з його даними та звертати увагу на можливі порушення прав. Загалом застосування ШІ може зробити обробку персональних даних більш прозорою та контрольованою.

Метою нашої статті є визначення можливостей ШІ у контексті підвищення прозорості обробки персональних даних.



Стан дослідження проблематики. Дослідження прозорості персональних даних з боку українських вчених-правників є фрагментарними. Н. Головацький досліджував прозорість через доступність та зрозумілість інформації, звертаючи увагу на те, що більший контроль за своїми даними дає можливість відігравати більш активну роль у процесі обробки персональних даних [1, с. 178]. В об'єктиві наукового пошуку В. Базалицького перебувало питання дотримання прозорості під час обробки персональних даних за допомогою ІІІ: він звертав увагу на питання автоматизованих рішень та необхідність інтеграції принципу *privacy by design/privacy by default* [2, с. 1]. У своїх попередніх працях ми вже звертали увагу на захист персональних даних, коли йшлося про дослідження mHealth-додатків. Наше дослідження показало недостатню ефективність чинного законодавства та наголошувало на потребі інтеграції міжнародних стандартів захисту персональних даних [3, с. 949]. Попри згадані вище праці, питання підвищення прозорості обробки персональних даних за допомогою ІІІ станом на сьогодні залишалося поза увагою дослідників.

Основний зміст. Захист персональних даних та прозорість їхнього використання є важливим питанням у контексті стрімкого розвитку цифрових технологій. Сьогодні відбувається зростання кількості цифрових сервісів, соціальних мереж та месенджерів, а також платформ для здійснення електронної комерції, а це має наслідком збільшення кількості даних про користувачів цих сервісів. Так, наприклад, у 2024 році у світі було створено 149 зетабайт даних, натомість у 2025 році ця цифра має зрости до 180 зетабайт [4]. Примітними є й інші показники: у 2024 році розмір світового ринку брокерів даних оцінювався у 278 мільярдів доларів США, а до 2033 року цей показник може скласти 512 мільярдів доларів США, зростаючи у середньорічному темпі 7,3 % з 2025 по 2033 роки [5]. Наведені показники свідчать про те, що чим більше даних продукується і чим більш активно розвивається ринок їхнього комерційного обігу, тим більше уваги слід приділяти питанню підвищення прозорості обробки персональних даних.

При цьому слід розуміти, що законодавство у сфері захисту персональних даних реагує на існуючі виклики із запізненням. Як наслідок приймаються закони, однак розвиток цифрових технологій випереджає їх, призводячи до потреби у нових змінах. Зважаючи на це, ІІІ має стати таким інструментом, який дасть можливість зробити обробку персональних даних більш прозорою.

Саме тому у цій статті ми звернемо увагу на те, як за допомогою використання ІІІ підвищити прозорість під час обробки персональних даних.

Перш за все йдеться про проблему прозорості у сучасному цифровому середовищі. Тут важливі три аспекти, які дозволять краще зрозуміти відповідний акцент: (1) недосконалість політик конфіденційності, (2) кількість суб'єктів, що беруть участь у процесі обробки персональних даних та (3) нерозуміння своїх прав суб'єктами персональних даних та відсутність у них практичних навичок для захисту своїх прав.

Щодо недосконалості політик конфіденційності, то в одному з досліджень автори вивчали політики конфіденційності мобільних додатків, які побудовано навколо *virtual personal assistant*. Дослідники виміряли якість політик конфіденційності за допомогою чотирьох показників: своєчасність, доступність, повнота та зрозумілість. Крім цього за допомогою QuPer було проаналізовано технічні та мовні дані. Виявилося, що тільки 1,7 % досліджених політик конфіденційності мобільних додатків повністю відповідають вимогам, які визначено законодавством [6, 478].

В іншому дослідженні було проведено аналіз політик конфіденційності 276 мобільних додатків. Інструментом для дослідження було обрано шкалу легкості читання Флеша. У підсумку виявлено, що понад 90% з цих політик конфіденційності важко читати, а майже 50 % читаються не менше, ніж за 20 хвилин [7, с. 432].

Як бачимо, розробники або ігнорують вимоги законодавства, або лише формально їх виконують, що призводить до ситуацій, коли суб'єкти персональних даних отримують інформацію, яку їм складно зрозуміти. Особливо це підкреслюється тим, що читання



значної кількості політик конфіденційності потребує більше 20 хвилин. У таких умовах ці документи є, по суті, непридатними для належного ознайомлення.

Проблема, яка стосується кількості суб'єктів, що беруть участь у процесі обробки персональних даних також варта уваги, оскільки персональні дані можуть передаватися третім особам. При цьому така передача може здійснюватися непрозоро. А це може призвести до ситуації, коли суб'єкт персональних даних не має змоги відслідкувати до кого потрапляють його дані, не говорячи вже про мету такого використання.

Це питання, зокрема, аналізує Г. Рушемайєр, звертаючи увагу на брокерів даних та на те, як вони використовують персональні дані. Авторка зазначає, що дані передаються від однієї компанії до іншої, часто багаторазово. Користувач не знає, хто кінцевий отримувач його даних і з якою метою вони будуть використані [8, с. 27].

Саме тому збільшення кількості суб'єктів, що беруть участь у процесі обробки персональних даних, прямо впливає на прозорість та контроль з боку самого суб'єкта персональних даних. Чим більшою є кількість третіх осіб, що отримують доступ до даних, тим складніше відстежити їхній рух та оцінити, якими можуть бути ризики подальшого використання таких даних.

Зрештою важливо, що багато суб'єктів персональних даних не знають або погано розуміють, якими є їхні права у сфері захисту персональних даних. Цю проблематику досліджено у статті «Online privacy literacy and users' information privacy empowerment: the case of GDPR in Europe», де йдеться про низький рівень онлайн-грамотності у сфері приватності серед громадян держав-членів ЄС. З цього дослідження можна зробити висновок, що низький рівень такої грамотності пов'язаний як із відсутністю знань про свої права, так і з недостатніми навичками щодо захисту даних. Тому автори роблять акцент і на практичних навичках, оскільки на їхню думку саме такі навички дозволяють суб'єкту персональних даних реально керувати своїми даними [9, с. 19-20].

Для того, щоб підвищити рівень розуміння своїх прав у суб'єктів персональних даних та посилити їхню здатність контролювати передачу даних, недостатньо тільки ефективних законодавчих норм. Потрібно також звертати увагу й на практичні аспекти захисту даних: вміння змінювати налаштування конфіденційності, ознайомлюватися з політиками конфіденційності та звертатись за захистом своїх прав у разі їх порушення.

У світлі означених проблем, застосування ШІ відкриває нові можливості для забезпечення прозорості у сфері захисту персональних даних. Використання ШІ має не лише спростити розуміння складних для розуміння політик конфіденційності, а й дати суб'єктам персональних даних можливість застосовувати практичні інструменти для контролю за власними персональними даними. Надалі ми зацентруємо увагу на тому, як саме застосування ШІ може підвищити прозорість обробки персональних даних.

Одна з можливостей – перетворення складної юридичної мови у зрозумілу форму, завдяки створенню коротких резюме або візуальних схем. А. Мента Гарус дослідив питання автоматичного спрощення текстів газет XVIII століття для того, щоб вони були зрозумілими для сучасної аудиторії. Моделі ШІ було використано для того, щоб спрощувати старі та складні речення: довгі речення було скорочено, а застарілі слова замінені на сучасні відповідники. При цьому складні структури перебудовувалися [10].

У випадку, коли ми говоримо про політики конфіденційності, йдеться про важкозрозумілі для більшості людей тексти, тому використання таких інструментів як велика мовна модель дає можливість для спрощення. А це означає, що суб'єкт персональних даних зможе адаптувати для себе політику конфіденційності, яка тим самим буде доступною для розуміння через використання потрібної форми та не вимагатиме значних затрат часу.

Варто згадати й про використання спеціалізованих інструментів для того, щоб суб'єкт персональних даних міг отримувати необхідні йому пояснення у сфері їхнього захисту.

У такому контексті важливою є розробка власних версій ChatGPT, завдяки чому можна створити персоналізованого помічника, який буде працювати в межах інструкцій та



заздалегідь заданого контексту [11]. Подібні рішення можуть дозволити підвищити рівень контролю суб'єкта персональних даних за інформацією про себе.

Нижче ми також наводимо перелік персоналізованих помічників, які засновані на ШІ, та які можна використовувати для отримання пояснень у сфері захисту персональних даних.

Таблиця 1

Приклад персоналізованих помічників на основі ШІ, які можна використовувати для отримання пояснень у сфері захисту персональних даних

№	Назва	Опис
1	Data Protection Assistant – AI-Powered Compliance Assistance [12]	Надає експертну допомогу у сфері захисту персональних даних. Допомогає із розумінням GDPR (Загального регламенту про захист даних), CCPA (Закон Каліфорнії про конфіденційність споживачів) та DPDPA (Індійський закон про захист цифрових персональних даних).
2	GDPR – GDPR Compliance Guidance [13]	Допомогає із розумінням положень GDPR (Загального регламенту про захист даних).
3	Personal Data Protection Guide [14]	Надає стратегії та найкращі практики для забезпечення конфіденційності та безпеки даних у цифровому світі.
4	Privacy Pro – GDPR Insights & Analysis [15]	Допомогає орієнтуватися у складних аспектах законодавства про конфіденційність, з акцентом на GDPR (Загальному регламенті про захист даних) у контексті Нідерландів.

Інша можливість підвищення прозорості – це платформи конфіденційності, які можуть використовувати ШІ для відповідних задач.

На сьогодні вченими пропонуються деякі принципи, які можуть стати орієнтирами під час використання такої платформи: (1) доступність; (2) комплексність; (3) зрозумілість; (4) детальність; (5) прозорість [16, с. 29–30].

Платформа конфіденційності може функціонувати, наприклад, як окремий мобільний додаток або бути елементом інфраструктури Дії. У такому випадку згода суб'єкта персональних даних буде надаватися безпосередньо через платформу конфіденційності. При цьому може вирішитися проблема з нерозумінням кількості суб'єктів, що беруть участь у процесі обробки персональних даних, оскільки кожного разу, коли дані будуть надаватися третім особам, володільці мають повідомити про це суб'єкта персональних даних через платформу конфіденційності.

Функціонування описаної платформи має дозволити суб'єктам персональних даних надавати та відкликати згоду, а також бачити повний список суб'єктів, які мають доступ до їхніх персональних даних. Це не лише підвищить рівень довіри до володільців, розпорядників та третіх осіб, а й сприятиме дотриманню законодавства у сфері захисту персональних даних.

Доцільно також звернути увагу на необхідність внесення змін до законодавства про захист персональних даних. Абзац другий частини першої статті 6 Закону України «Про захист персональних даних» передбачає, що:

«Обробка персональних даних здійснюється відкрито і прозоро із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки» [17].

Разом з тим у цьому законі не міститься визначення принципу прозорості, а також не зрозуміло, які саме інструменти мають забезпечувати його дотримання. Відтак звернемося до положень Загального регламенту про захист даних, де у пункті 39 преамбули зазначено, що:



«Принцип прозорості вимагає, щоб будь-яка інформація та повідомлення щодо опрацювання таких персональних даних були доступними і зрозумілими, з використанням чітких і простих формулювань» [18].

Це означає, що принцип прозорості передбачає те, що політики конфіденційності повинні бути зрозумілими та не мають включати складну юридичну термінологію.

Таким чином потрібно, щоб український законодавець деталізував норми, які стосуються принципу прозорості, зокрема акцентуючи увагу на доступності, зрозумілості та використанні простих формулювань. Це дозволить гармонізувати українське законодавство з європейським, а також забезпечить здійснення права суб'єкта персональних даних на поінформованість та належне пояснення того, як саме використовуються відомості про нього.

Належне функціонування платформи конфіденційності також вимагатиме законодавчих змін. Перш за все потрібно буде визначити її функціональні можливості з потребою обов'язкової участі з боку володільців, розпорядників та третіх осіб.

Доповнення також буде потребувати стаття 8 Закону України «Про захист персональних даних», де потрібно внести зміни, які передбачатимуть те, що право на отримання інформації про умови доступу до персональних даних, зокрема інформацію про третіх осіб, буде реалізовуватися через платформу конфіденційності. У цьому випадку також не буде необхідності в існуванні пункту 4 частини другої статті 8 цього закону, яка сьогодні передбачає право на отримання відповіді про те, чи обробляються персональні дані суб'єкта персональних даних за допомогою подання запиту, який може оброблятися протягом тридцяти календарних днів [17].

Однак варто наголосити, що приклади Open Banking у Великій Британії та Digital Markets Act у ЄС можуть показати нам, що попри наявність технічних рішень для перенесення чи контролю даних, бізнес немає мотивації для самостійного впровадження цих рішень. Це пов'язано з тим, що головними проблемами є інвестиції та довіра між учасниками [19]. Тому правове регулювання має стати каталізатором, що призведе до того, що бізнес буде координуватися та брати участь у наповненні централізованого реєстру, що буде підґрунтям для ефективної реалізації своїх прав суб'єктами персональних даних.

Висновки. Внаслідок проведеного аналізу можемо стверджувати, що процес обробки персональних даних стикається з рядом труднощів: недосконалі політики конфіденційності, які важко зрозуміти, велика кількість суб'єктів, які беруть участь у процесі обробки даних, а також низький рівень обізнаності та практичних навичок у суб'єктів персональних даних. Вказані недоліки призводять до зниження прозорості та зменшення контролю над персональними даними з боку суб'єкта персональних даних. Саме тому застосування III та пропонуваної платформи конфіденційності мають дозволити краще розуміти питання, пов'язані з персональними даними, а також контролювати власні дані, таким чином підвищуючи прозорість їхньої обробки.

Список використаних джерел:

1. Головацький Н. Т. Прозорість та згода як основні принципи захисту персональних даних в Україні. *Науковий вісник Ужгородського національного університету. Серія: Право.* № 83. Ч. 2. С. 178–184.
2. Базалицький В. І. Дотримання прозорості в обробці персональних даних за допомогою штучного інтелекту. *Академічні візії.* 2024. № 32. С. 1–9. URL: <https://academy-vision.org/index.php/av/article/view/1168/1125>
3. Pishta V., Boldizhar S., Popovych T., Holovatskiy N., Potapchuk A., Hechko M. Personal data protection in m-health apps: international experience and prospects for legislative changes in Ukraine. *Wiadomości Lekarskie.* 2025. № 78 (4). P. 949–954. <https://doi.org/10.36740/WLek/203908>
4. Becoming Data. *Medium:* website. URL: <https://medium.com/digital-society/becoming-data-e96bf007c8d1>.
5. Data Broker Market Summary. *Grand View Research:* website. URL: <https://www.grandviewresearch.com/industry-analysis/data-broker-market-report>.



6. Yan Ch., Xie F., Meng M. H., Zhang Ya., Bai G. On the Quality of Privacy Policy Documents of Virtual Personal Assistant Applications. *Proceedings on Privacy Enhancing Technologies Symposium*. 2024. Is. 1. P. 478–493. <https://doi.org/10.56553/popets-2024-0028>
7. Haggag O., Grundy J., Abdelrazak M. An Analysis of Privacy Issues and Policies of eHealthApps. *Proceedings of the 19th International Conference on Evaluation of Novel Approaches to Software Engineering*. 2024. P. 422–433. URL: http://nzjohng.github.io/publications/papers/enase2024_1.pdf.
8. Ruschemeier H. Data Brokers and European Digital Legislation. *The European Data Protection Law Review*. 2023. № 1. P. 27–38.
9. Prince C., Omrani N., Schiavone F. Online privacy literacy and users' information privacy empowerment: the case of GDPR in Europe. *Information Technology & People*. 2024. № 37 (8). P. 1–24.
10. Menta Garuz A. Exploring artificial intelligence techniques in the digital humanities domain from authorship verification to automatic sentence simplification. Doctoral thesis. UNED. Universidad Nacional de Educación a Distancia. 2024. 156 p.
11. Creating a GPT. *Open.ai*: website. URL: <https://help.openai.com/en/articles/8554397-creating-a-gpt>.
12. Data Protection Assistant – AI-Powered Compliance Assistance. *Yeschat.ai*: website. URL: https://www.yeschat.ai/gpts-ZxX6UxVv-Data-Protection-Assistant?utm_source=chatgpt.com.
13. GDPR – GDPR Compliance Guidance. *Yeschat.ai*: website. URL: https://www.yeschat.ai/gpts-20ToA3QiQK-GDPR?utm_source=chatgpt.com.
14. Personal Data Protection Guide. *ChatGPT.com*: website. https://chatgpt.com/g/g-GGLNiNOYt-personal-data-protection-guide?utm_source=chatgpt.com.
15. Privacy Pro – GDPR Insights & Analysis. *Yeschat.ai*: website. URL: https://www.yeschat.ai/gpts-9t557RbaPFX-Privacy-Pro?utm_source=chatgpt.com.
16. Irion K., Yakovleva S., van Hoboken J., Thompson M. A Roadmap to Enhancing User Control via Privacy Dashboards. Amsterdam/Hong Kong: IViR, 2017. 50 p.
17. Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
18. 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://zakon.rada.gov.ua/laws/show/984_008-16#top.
19. Fish T. Building Trust for Data Portability Within the DMA Framework. *TechPolicy*: website. URL: <https://www.techpolicy.press/building-trust-for-data-portability-within-the-dma-framework/>.

Дата першого надходження рукопису до видання: 24.07.2025

Дата прийнятого до друку рукопису після рецензування: 18.08.2025

Дата публікації: 26.09.2025

