УДК 342.7:004.8
DOI https://doi.org/10.24144/2307-3322.2025.91.3.24

ПІДВИЩЕННЯ ПРОЗОРОСТІ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ: ЗАКОНОДАВЧІ ПІДХОДИ ДО СПРОЩЕННЯ ДОСТУПУ КОРИСТУВАЧІВ ДО ІНФОРМАЦІЇ

Остіян Є.З.,
студентка 1 курсу магістратури юридичного факультету
ДВНЗ «Ужгородський національний університет»
ORCID: 0009-0007-4166-7177
e-mail: evgost0112@gmail.com

Остіян Є.З. Підвищення прозорості обробки персональних даних: законодавчі підходи до спрощення доступу користувачів до інформації.

Вказується, розвиток інформаційного суспільства характеризується широким застосуванням мережі Інтернет, веб-ресурсів та баз даних, що уможливлює ефективний пошук інформації, здійснення електронних покупок та отримання різноманітних цифрових послуг.

Стаття розглядає практичні пропозиції до законодавства щодо підвищення рівня прозорості в обробці персональних даних завдяки спрощенню доступу користувачів до інформації про те, хто і як використовує їхні дані. Акцентовано на ефективності впровадження новітніх інформаційних технологій задля досягнення вказаних цілей. На цій основі розширено значення безпеки персональних даних та необхідності їх посиленого правового захисту. Звернено особливу увагу на безпеку даних, що несуть чутливу інформацію, зокрема їхню активну циркуляцію в медицині та медичних мобільних застосунках, які їх зберігають.

Виходячи з цього, робота аналізує сучасні методи захисту персональних даних, визначені українським законодавством та міжнародними нормативно-правовими актами. З огляду на триваючу актуальність євроінтеграції, практичну значущість несе Загальний регламент про захист даних (GDPR). Визначені основні принципи сучасного регулювання персональних даних, а саме законність, прозорість та безпека обробки персональної інформації, обмеження мети, обсягу та строків її зберігання.

Досліджено ключові переваги та ризики імплементації інноваційних технічних рішень: диференційної приватності, гомоморфного шифрування та блокчейну. Описані технології забезпечують належний рівень конфіденційності та відповідають потребам аналітичних процесів сьогодення.

Водночас через вплив цифровізації на правову систему в полі захисту інформації, зокрема в контексті штучного інтелекту, блокчейну та mHealth-рішень, виникає потреба у створенні комплексної моделі, яка б об'єднувала технічні, правові та етичні підходи. Зроблено висновок про необхідність впровадження практик відповідального використання штучного інтелекту й криптографічних технологій. Цей підхід може забезпечити високий рівень безпеки персональних даних, підвищити довіру осіб до інновацій і сприятиме розвитку сталого інформаційно-правового середовища.

Ключові слова: інформація, приватність, технології, дані, GDPR, блокчейн, гомоморфне шифрування.

Ostiian Y.Z. Enhancing transparency in personal data processing: legislative approaches to simplifying user access to information.

It is indicated that the development of the information society is characterized by the widespread use of the Internet, web resources and databases, which enables effective information search, electronic purchases and receipt of various digital services.

The article explores practical legislative proposals aimed at enhancing the transparency of personal data processing by simplifying user access to information regarding who uses their data and in what manner. The focus is placed on the effectiveness of implementing advanced information technologies to achieve these objectives. On this basis, the concept of personal data security and the need for its strengthened legal

protection are further developed. Particular attention is paid to the security of data containing sensitive information, especially when it is actively circulated within the healthcare sector and in medical mobile applications that store such data.

Building upon this, the study analyzes contemporary methods of personal data protection as defined by Ukrainian legislation and international legal instruments. Considering the ongoing relevance of European integration processes, the General Data Protection Regulation is identified as having practical significance. The fundamental principles of modern personal data regulation are outlined – namely, lawfulness, transparency, and security of processing, as well as the limitation of purpose, scope, and storage duration.

The paper examines the key advantages and risks associated with implementing innovative technical solutions, including differential privacy, homomorphic encryption, and blockchain technologies. These technologies ensure an appropriate level of confidentiality while addressing the analytical demands of the modern digital environment.

At the same time, due to the growing impact of digitalization on the legal system in the field of information protection – particularly in the context of artificial intelligence, blockchain, and mHealth solutions – there emerges a need to develop a comprehensive model integrating technical, legal, and ethical approaches. The study concludes with the assertion that responsible implementation of artificial intelligence and cryptographic technologies is essential. Such an approach can ensure a high level of personal data security, enhance public trust in innovations, and contribute to the development of a sustainable information and legal environment.

Key words: information, privacy, technology, data, GDPR, blockchain, homomorphic encryption.

Актуальність теми дослідження. В умовах сучасного розвитку суспільства, застосування мережі Інтернет, різних сайтів та здійснення певних комп'ютерних баз даних рахується неймовірно зручним. Людина може впевнено знайти належну інформацію, реалізувати онлайн-шопінг, застосувати різні освітні та інші послуги тощо. Проте, варто дотримуватися відповідних правил поводження із персональними даними, аби забезпечити їх ефективність та збереження. Як відомо, персональні дані – це сукупність відомостей або окремі відомості про фізичну особу, яка ідентифікована або може бути однозначно ідентифікована [1]. Будь-яке опрацювання таких даних має здійснюватися на законних підставах та у спосіб, що відповідає встановленим нормам. Суб'єкти персональних даних при цьому повинні бути поінформовані про факт збирання, використання, поширення чи інші форми опрацювання їхніх персональних даних, а також про мету, обсяг і способи такого опрацювання як на поточному етапі, так і в майбутньому.

Аналіз останніх досліджень та публікацій. Сучасний стан та проблемні аспекти підвищення рівня прозорості в обробці персональних даних завдяки спрощенню доступу користувачів до інформації досліджували такі вчені, як Баранов О.А., Брижко В.М., Бєлова М.В., Бєлов Д.М., Головацький Н.Т., Колодій А.М., Машталяр О.М., Політанський В.С. та ряд інших вчених.

Мета даної статті полягає у системному дослідженні сутності обробки персональних даних та визначення рівня підвищення прозорості доступу користувачів до інформації.

Виклад основного матеріалу. Захист персональних даних, як і будь-який інший правовий інститут, ґрунтується на системі принципів, що визначають механізм його функціонування, зміст якого має демократичний характер та зумовлений соціально-правовими факторами. Теоретичне обґрунтування основних аспектів захисту персональних даних дає змогу розкрити правову природу та сутність цього інституту в цілому.

Варто зауважити, що згідно ст. 6 Закону України «Про захист персональних даних» визначено аспект загальних вимог щодо оброблення персональних показників [1, с. 9]. Згідно з думкою Головацького Н.Т., стаття 7 цього Закону несе в собі окремі умови. Законодавець не виділив окремої норми, яка б безпосередньо визначала принципи збирання, оброблення та захисту персональних показників, а натомість інтегрував їх через загальні вимоги до персональних даних. Такий підхід видається логічно обґрунтованим, оскільки виокремлення спеціальної норми вимагало б окремого закріплення принципів збирання, оброблення, захисту та знищення персональних даних як самостійних категорій [2, с. 180].

Відповідно до статті 6 Закону України «Про захист персональних даних», що визначає загальні вимоги до обробки персональних даних, мета їх оброблення повинна бути чітко визначена у законодавчих та нормативно-правових актах, установчих або внутрішніх документах володільця персональних даних і узгоджуватися з положеннями законодавства у сфері захисту персональних даних [2, с. 180].

Відповідно до Загального регламенту про захист даних персональні дані повинні: (а) опрацьовуватися законно, справедливо та прозоро щодо суб'єкта даних; (б) збиратися лише для чітко визначених та законних цілей та не використовуватися далі у спосіб, несумісний із цими цілями; (в) бути достатніми, доречними та обмеженими лише тим обсягом, який необхідний для досягнення визначених цілей; (г) бути точними та, за потреби, оновлюватися. Неточні дані мають бути виправлені або видалені без зволікань; (г) зберігатися не довше, ніж потрібно для досягнення цілей обробки; (д) оброблятися з дотриманням вимог безпеки, що забезпечують захист від несанкціонованого доступу, втрати, знищення або пошкодження даних із застосуванням відповідних технічних та організаційних заходів [13].

З огляду на це диференційна приватність як важлива складова принципу обмеження мети згадується у розробці технологій компанії Microsoft. Її суть полягає в тому, що до наявних даних додається статичний шум, який не впливає на загальну точність набору даних, однак при цьому можна відстежити, скільки інформації було розкрито через різні запити. Це слугує гарантією, що сукупні запити ненавмисно не розкриють конфіденційну інформацію. Прикладом є аналітика для менеджерів з персоналу в рамках *Workplace Analytics* з використанням агрегованих даних про співпрацю, не надаючи жодної інформації про окремих осіб [3].

У дослідженні «Making ML models differentially private: Best practices and open challenges» зазначається, що при застосуванні диференційної приватності в машинному навчанні одним із ключових викликів є компроміс між приватністю, точністю і обчислювальними витратами. У великих моделях, де залучені численні шари, функції втрат, оптимізатори, не всі компоненти є «приватно-безпечні», тому важливе коригування архітектури та гіперпараметрів, таких як норма кліпінгу, масштаб шуму і розмір батчів – інакше шум може значно погіршити якість моделі [4].

Ще одним важливим викликом при застосуванні диференційної приватності є точне обчислення рівня приватності, який фактично забезпечує модель. У теорії це описується через параметри ε і δ, що показують, скільки інформації може «витекти» під час навчання. Проте на практиці моделі навчаються з використанням інших технічних підходів, ніж передбачає теорія (наприклад, формування батчів не випадково, а за фіксованим порядком). Через це реальний рівень приватності може бути нижчим, ніж очікувалось [4].

Гомоморфне шифрування – це модель криптографії, яка дозволяє виконувати певні математичні операції над зашифрованими даними таким чином, що що результат обчислення залишається зашифрованим, але після розшифрування відповідає тому, що могло б бути отримано над відкритими даними [5].

Гомоморфні схеми поділяють на кілька категорій, залежно від того, які типи операцій вони підтримують:

- *Частково* гомоморфні схеми (Partial Homomorphic Encryption, PHE): підтримують лише один тип операції – зазвичай або множення, або додавання. До прикладу, RSA й ElGamal демонструють гомоморфізм за множенням, а криптосистема Паїльє (Paillier) – за додаванням. Ці схеми корисні за виконання лише однієї операції над даними;
- *Дещо* гомоморфні схеми (Somewhat Homomorphic Encryption, SWHE): вони підтримують обмежену кількість операцій обох типів (додавання та множення), але з обмеженням глибини обчислень. Якщо виконати надто багато операцій, шифротекст «наповнюється шумом», і результат може бути неточним;
- *Повністю* гомоморфне шифрування (Fully Homomorphic Encryption, FHE): це найуніверсальніший варіант, адже за нього можна виконувати довільне поєднання операцій (додавання, множення і складніші функції) над зашифрованими даними без необхідності їх розшифровувати під час проміжних кроків [5].

У загальному *повністю* гомоморфне шифрування у своїй нинішній формі є все ще новою розробкою для забезпечення безпеки даних. Його створення припадає на 2009 рік. Щодо старіших версій – *частково* і *дещо* – вони існують з кінця 70-х років. Саме тому недоліки повністю гомоморфного шифрування можна охарактеризувати низькою продуктивністю, адже є здебільшого комерційно неможливим для додатків із складними обчисленнями [6, с. 2].

Гомоморфне шифрування може також створювати ризики за некоректної реалізації. Одними з таких виступають небезпечні схеми гомоморфного шифрування, некоректні проєктування шифрування та неправильне управління ключами, тобто невикористання регулярної ротації, небезпечне зберігання та недостатній захист від несанкціонованого доступу до ключів. Задля недопущення несанкціонованого доступу потрібне залучення криптографічних фахівців, перевірені бібліотеки та оновлення алгоритмів шифрування [7].

Науковці досягають консенсусу в тому, що дослідження та розробка алгоритмів повністю гомоморфного шифрування активно проводиться на даному етапі, тому сьогодні його доречно використовувати у поєднанні з іншими технологіями, що підвищують конфіденційність, такими як безпечні багатосторонні обчислення [6, с. 2].

Блокчейн – це цифровий реєстр, який безпечно записує показники транзакцій у розподіленій системі комп'ютерів. Блокчейн забезпечує сукупність даних завдяки власній незмінній природі за допомогою криптографії та способів консенсусу, що означає, що після запису інформація не може змінюватись заднім числом. Блокчейн становить основу криптовалютних систем, таких як Bitcoin і Ethereum, і відіграє головну роль у підвищенні прозорості, безпеки та довіри не лише у фінансах, але й в інших напрямках. Безсумнівним вважається факт, що сама технологія блокчейн широко застосовується та асоціюється з криптовалютами, хоч по суті, вона становить собою електронний перелік створених записів (блоків інформації) із спроможністю їх перевірки за рахунок публічного доступу та чітко визначеної бази зберігання [14].

Варто також звернути увагу на те, що штучний інтелект на етапі обробки персональних даних викликає такі основні проблеми:

1. Конфіденційність та безпеку. Моделі штучного інтелекту вимагають великих обсягів даних для навчання, що покращує ризик витоку даних та їх зловживання.

2. Упередженість та дискримінація. Алгоритми штучного інтелекту спроможні відображати упередження, що наявні в тренувальних даних, що може призводити до дискримінації відповідних груп користувачів. Це вимагає створення методів для виявлення та усунення упередженостей, а також забезпечення прозорості та справедливості алгоритмічних дій.

3. Нормативно-правові колізії. Наявні правові норми в основному не враховують специфіку штучного інтелекту, що може мати наслідок виникнення правових колізій.

4. Відповідність міжнародним стандартам. Для забезпечення належного рівня захисту даних Україна потребує гармонізації свого законодавства з міжнародними стандартами, такими як Загальний регламент про захист даних.

5. Етичні аспекти. Машталяр О.М. зазначає, що використання штучного інтелекту викликає значні етичні питання, пов'язані з конфіденційністю, безпекою та правами користувачів. Важливо розробити етичні керівництва та стандарти для використання ШІ, щоб забезпечити дотримання етичних норм та захист прав користувачів [10, с. 257].

На думку Бєлової М.В. та Бєлова Д.М., використання штучного інтелекту для обробки персональних даних піднімає питання щодо згоди користувачів і відповідальності за потенційні зловживання. Користувачі повинні мати право контролювати, як їхні дані використовуються, і отримувати чітку інформацію про цілі і методи обробки. Водночас, за врахування збройної агресії росії та необхідності збору та обробки великою кількості додаткової інформації, включаючи геномну інформацію про людину, технології штучного інтелекту та персональні дані, які ними обробляються на території України є вразливими [11, с. 289].

Визначення Блокчейну описується як технологія бази даних, яка опирається на облікову книгу, яка поширюється на всю комп'ютерну мережу та чиї записи можна охарактеризувати як своєрідні блоки. У свою чергу, блоки і їхня послідовність є незмінними, що дає можливість відстежити будь-які дії, що здійснені щодо певного блоку. У сфері охорони здоров'я застосовуються зміни, при яких на заміну паперовим носіям та електронним базам приходять саме Блокчейн-блоки, адже з більш старими методами зберігання інформації спостерігаються проблеми механізму контролю за тим, що відбувається з їхніми чутливими персональними даними. При цьому децентралізована інфраструктура, характерна для Блокчейну, є гарантією безпечності та стійкості до збоїв [8, с. 160].

У такому контексті ефективне використання Блокчейну узгоджується з п. 32 преамбули Загального регламенту про захист даних, а саме з тим, що «згоду необхідно надавати шляхом чіткого ствердження, що становить вільно надане, конкретне, проінформоване та однозначне свідчення погодження суб'єкта даних на опрацювання його або її персональних даних, зокрема, у формі письмової заяви, в тому числі електронними засобами, або у формі усної заяви». Ця згода має лягати на всі види опрацювання даних, що здійснюються для однакових цілей [13]. Це безпосередньо поширюється на контроль безпеки персональних даних і є одною з причин застосування Блокчейну в медицині.

Деякі дослідження вказують, що наразі зростає попит на mHealth-додатків (медичні мобільні додатки). У таких реаліях, де чутлива інформація про особу вкрай піддана ризикам порушення конфіденційності, потрібне вдосконалення українського законодавства на основі правових стандартів США, Канаді та ЄС. [9, с. 952].

Висновки. Сучасні підходи до захисту персональних даних, закріплені в українському законодавстві та міжнародних актах, зокрема у Загальному регламенті про захист даних, спрямовані на забезпечення законності, прозорості та безпеки обробки інформації. Вони визначають вимоги до мети, обсягу та строків зберігання даних. Особливу увагу сьогодні приділяють сучасним технологічним рішенням, таким як диференційна приватність та гомоморфне шифрування, які у свою чергу дозволяють підвищити рівень конфіденційності, не втрачаючи ефективності аналітичних процесів. Використання таких інструментів дає можливість поєднати потребу в обробці великих масивів даних із захистом прав людини на приватність.

Разом з цим, розвиток технологій штучного інтелекту, блокчейну, mHealth-рішень та інших цифрових інновацій призводить до викликів для правового регулювання. А це вже вимагає не тільки технічних, а й етичних підходів до обробки даних. Саме тому подальший розвиток системи правового регулювання у сфері захисту персональних даних має спиратися на правові, технологічні та організаційні механізми. Власне ці питання і становлять перспективу для подальших наукових досліджень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про захист персональних даних: Закон України від 01.06.2010 № 2297. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 20.09.2025).
2. Головацький Н.Т. Прозорість та згода як основні принципи захисту персональних даних в Україні. *Науковий вісник Ужгородського Національного Університету*. Серія: Право. 2024. С. 178–184. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/07/27-1.pdf (дата звернення: 20.09.2025).
3. Sarah Bird. Putting differential privacy into practice to use data responsibly. AI Blog for Business & Tech. *Microsoft*. 2020. URL: https://blogs.microsoft.com/ai-for-business/differential-privacy/ (дата звернення: 20.09.2025).
4. Ponomareva N, Kurakin A. Making ML models differentially private: Best practices and open challenges. *Google Research*. 2023. URL: https://research.google/blog/making-ml-models-differentially-private-best-practices-and-open-challenges/ (дата звернення: 20.09.2025).
5. Що таке повністю гомоморфне шифрування (FHE)? *ForkLog UA*. 2025. URL: https://forklog.com.ua/exclusive/shho-take-povnistyu-gomomorfne-shyfruvannya-fhe (дата звернення: 20.09.2025).
6. Мовчанюк М.Т., О.В. Салієва. Аналіз сучасних гомоморфних систем шифрування. Вінницький національний технічний університет. URL: https://conferences.vntu.edu.ua/index.php/mn/mn2022/paper/viewFile/14977/12665 (дата звернення: 20.09.2025).
7. Гомоморфне шифрування. KeepSolid Inc. URL: https://www.vpnunlimited.com/ua/help/cybersecurity/homomorphic-encryption (дата звернення: 20.09.2025).
8. Пішта В.І. Проблема правового регулювання блокчейн у сфері охорони здоров'я. *Digital Trends and Anti-Corruption Reforms in Public Administration*: Scientific monograph. Riga, Latvia: Baltija Publishing, 2023. P. 159–167. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/view/399/10844/22597-1 (дата звернення: 20.09.2025).
9. 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. URL: https://doi: 10.36740/WLek/203908 (дата звернення: 20.09.2025).
10. Машталяр О.М. Проблеми використання штучного інтелекту під час оброблення персональних даних та напрями їх вирішення. *Юридичний науковий електронний журнал*. 2024. № 8. С. 256–259. URL: http://lsej.org.ua/8_2024/61.pdf (дата звернення: 20.09.2025).
11. Бєлова М.В., Бєлов Д.М. Виклики та загрози захисту персональних даних у роботі зі штучним інтелектом. *Науковий вісник УжНУ. Серія «Право»*. Випуск 79(5). 2023. С. 289–294. (дата звернення: 20.09.2025).
12. 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. 122–129. (дата звернення: 20.09.2025).
13. 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). *Відомості*

Верховної Ради України. 2016. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 20.09.2025).

14. Що таке блокчейн і як він працює? *Binance Academy*. 2023. URL: https://academy.binance.com/uk-UA/articles/what-is-blockchain-and-how-does-it-work (дата звернення: 20.09.2025).