

ТИМАШОВ В. О.,

orcid.org/0000-0001-8368-8856

доктор юридичних наук, професор,
професор кафедри адміністративного,
фінансового та інформаційного права
(Державний торговельно-економічний
університет)

ЦАРИК Д. В.,

orcid.org/0009-0004-0820-4232

студентка IV курсу факультету
міжнародної торгівлі та права
(Державний торговельно-економічний
університет)

УДК 342.951

DOI <https://doi.org/10.32842/2078-3736/2025.6.19>

ПРАВОВІ ОСНОВИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

У статті здійснено комплексний аналіз правових основ захисту персональних даних в Україні, з акцентом на їх відповідність сучасним викликам цифровізації, глобалізації інформаційних потоків і міжнародним стандартам. Досліджено ключові нормативно-правові акти, зокрема Конституцію України, Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI та Закон «Про інформацію», які формують правову базу захисту приватності. Проаналізовано цивільно-правові інструменти, що забезпечують право на спростування недостовірної інформації та відшкодування шкоди, а також кримінально-правові механізми, які встановлюють відповідальність за незаконне поводження з даними.

Особливу увагу приділено порівняльному аналізу українського законодавства з міжнародними стандартами, зокрема Загальним регламентом із захисту даних (GDPR) Європейського Союзу, секторальним законодавством США (наприклад, California Consumer Privacy Act) та канадським Законом про захист персональних даних і електронні документи (PIPEDA). Це дозволило виявити прогалини в регулюванні чутливих даних, автоматизованої обробки та інституційного нагляду. Висвітлено практичні аспекти захисту, включаючи технічні заходи, такі як шифрування та контроль доступу, а також ключову роль згоди суб'єкта даних у процесі обробки.

Окреслено виклики, пов'язані з недостатньою інституційною спроможністю, неузгодженістю норм і слабким контролем за виконанням законодавства. Запропоновано шляхи вдосконалення, зокрема створення незалежного наглядового органу, запровадження оцінок впливу на приватність для високоризикових операцій і посилення відповідальності за порушення.

Дослідження підкреслює необхідність гармонізації українського законодавства з міжнародними стандартами, зокрема Конвенцією Ради Європи № 108, для забезпечення ефективного захисту прав людини в інформаційному суспільстві.

Окремо розглянуто вплив кіберзагроз на безпеку даних і потребу в етичному регулюванні використання сучасних технологій, таких як штучний інтелект, для моніторингу обробки даних. Теоретичні висновки доповнено практичними



рекомендаціями щодо адаптації правового регулювання до цифрових реалій, включаючи впровадження автоматизованих систем моніторингу для підвищення прозорості й безпеки обробки даних.

Ключові слова: *персональні дані, захист приватності, правове регулювання, цифровізація, GDPR, кібербезпека, інформаційне суспільство.*

Timashov V. O., Tsaryk D. V. Legal basis of personal data protection in Ukraine

This article provides an in-depth analysis of the legal framework governing personal data protection in Ukraine, emphasizing its alignment with contemporary challenges posed by digitalization, global information flows, and international standards. The study examines key legislative acts, including the Constitution of Ukraine, the Law of Ukraine «On Personal Data Protection» of June 1, 2010, No. 2297-VI, and the Law «On Information», which collectively form the foundation for privacy protection. It explores civil law mechanisms that enable individuals to rectify inaccurate information and seek compensation for damages, as well as criminal law provisions that establish liability for unlawful data handling.

Particular attention is devoted to a comparative analysis of Ukrainian legislation with international benchmarks, such as the European Union's General Data Protection Regulation (GDPR), the sectoral legislation of the United States (e.g., the California Consumer Privacy Act), and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). This comparison highlights deficiencies in the regulation of sensitive data, automated processing, and institutional oversight.

The article addresses practical aspects of data protection, including technical measures such as encryption and access controls, as well as the pivotal role of data subject consent in processing activities. It identifies challenges stemming from inadequate institutional capacity, inconsistent legal norms, and weak enforcement mechanisms.

Proposed solutions include the establishment of an independent supervisory authority, the introduction of privacy impact assessments for high-risk operations, and strengthened accountability for violations. The study underscores the necessity of harmonizing Ukrainian legislation with international standards, particularly the Council of Europe's Convention 108, to ensure robust protection of human rights in the information society.

Additionally, it examines the impact of cyber threats on data security and the need for ethical regulation of emerging technologies, such as artificial intelligence, in data processing. Theoretical insights are complemented by practical recommendations for adapting legal frameworks to digital realities, including the adoption of automated monitoring systems to enhance transparency and security in data processing.

Key words: *personal data, privacy protection, legal regulation, digitalization, GDPR, cybersecurity.*

Вступ. Захист персональних даних в Україні є критично важливим елементом забезпечення прав людини в умовах швидкого розвитку інформаційних технологій і цифровізації суспільства. Персональні дані, що включають відомості про фізичну особу, від базової інформації, як ім'я чи адреса, до чутливих даних, таких як відомості про здоров'я чи релігійні переконання, стають об'єктом підвищених ризиків через зростання кіберзагроз, масову обробку даних і глобалізацію інформаційних потоків. Незважаючи на наявність конституційних гарантій і спеціалізованого законодавства, захист персональних даних в Україні стикається з проблемами, пов'язаними з невідповідністю нормативної бази сучасним технологічним реаліям, недостатньою інституційною спроможністю та обмеженою гармонізацією



з міжнародними стандартами, такими як Загальний регламент із захисту даних (GDPR). Удосконалення правового регулювання та практичних механізмів захисту є нагальною потребою в контексті розвитку інформаційного суспільства.

Питання правового регулювання захисту персональних даних в Україні активно досліджується з огляду на сучасні виклики та міжнародні стандарти. Звіт 2023 року, підготовлений експертами, аналізує стан українського законодавства, вказуючи на прогалини в регулюванні чутливих даних і необхідність посилення наглядових механізмів для забезпечення ефективного захисту [1]. Бем М.В. і Городиський І.М. у своєму науково-практичному посібнику розглядають практичні аспекти обробки даних, акцентуючи на важливості згоди суб'єкта та технічних засобів захисту, таких як шифрування [2].

Биков О.М. і Савченко В.В. досліджують виклики кібербезпеки, пропонуючи інтеграцію штучного інтелекту для моніторингу обробки даних із дотриманням етичних стандартів, що є актуальним для України в умовах зростання цифрових транзакцій [3]. Головацький Н.Т. проводить порівняльний аналіз українського законодавства з нормами GDPR, США та Канади, наголошуючи на необхідності адаптації до глобальних стандартів для підвищення ефективності захисту [4].

Головченко В. аналізує проблеми неузгодженості норм і недостатнього контролю за обробкою даних, пропонуючи створення незалежного наглядового органу для посилення правозастосування [5]. Кардаш А.В. досліджує співвідношення інформації про особу та персональних даних, підкреслюючи важливість чіткого правового розмежування для захисту державних реєстрів [6]. Обухівська Т.І. акцентує на міжнародних стандартах, зокрема Конвенції Ради Європи № 108 «Про захист осіб щодо автоматизованої обробки персональних даних», і необхідності уніфікації норм для забезпечення прав на доступ і виправлення даних [7]. Питання інтеграції сучасних технологій захисту, таких як блокчейн чи автоматизовані системи моніторингу, у правове поле України залишаються недостатньо дослідженими, що потребує додаткової уваги.

Постановка завдання. Мета статті є аналіз правових основ захисту персональних даних в Україні, оцінка їх відповідності сучасним викликам цифровізації та міжнародним стандартам, а також визначення шляхів удосконалення законодавства і практичних механізмів для забезпечення ефективного захисту прав людини в інформаційному суспільстві.

Результати дослідження. Захист персональних даних є ключовим елементом забезпечення права на приватність у контексті цифровізації, яка трансформує суспільні відносини. Персональні дані охоплюють відомості, що дозволяють ідентифікувати фізичну особу, включаючи не лише ім'я, адресу чи контактну інформацію, але й чутливі дані, такі як відомості про здоров'я, етнічне походження чи політичні переконання. В Україні правові основи захисту персональних даних базуються на конституційних нормах, спеціалізованому законодавстві та спробах гармонізації з міжнародними стандартами. Однак сучасні виклики, пов'язані з обробкою великих обсягів даних у цифрових системах, зокрема через електронне врядування, соціальні мережі та комерційні платформи, вимагають удосконалення нормативної бази та практичних механізмів для запобігання витокам і зловживанням.

Конституція України встановлює фундамент для захисту приватності, гарантуючи недоторканність особистого життя та забороняючи втручання в нього без згоди особи, за винятком випадків, передбачених законом, таких як захист національної безпеки чи прав інших осіб. Право на таємницю листування, телефонних розмов і кореспонденції, а також доступ до інформації про себе в органах влади створюють правову основу для регулювання обробки персональних даних. Ці норми забезпечують баланс між індивідуальними правами та суспільними інтересами, створюючи передумови для розвитку спеціалізованого законодавства [8].

Основним нормативним актом у сфері захисту персональних даних є Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI. Він визначає персональні дані як відомості про ідентифіковану або ідентифіковану особу, встановлює



принципи їх обробки, зокрема законність, цільову визначеність, мінімальність обсягу даних і захист від несанкціонованого доступу. Закон регулює збір, зберігання, використання та поширення даних, які дозволяються лише за згодою суб'єкта або на підставі закону. Крім того, вводяться поняття володільця та розпорядника даних, на яких покладаються обов'язки щодо забезпечення конфіденційності та повідомлення про мету обробки [9].

Закон України «Про інформацію» доповнює регулювання, класифікуючи персональні дані як конфіденційну інформацію. Він встановлює права суб'єктів на доступ до своїх даних, їх виправлення чи видалення, а також механізми захисту від незаконного поширення. У контексті розвитку цифрових сервісів, таких як електронне врядування чи онлайн-платформи, цей закон підкреслює необхідність балансу між відкритістю інформації та захистом приватності, що є особливо актуальним у сучасних умовах зростання кіберзагроз [10].

Цивільне законодавство України розглядає захист персональних даних як частину особистих немайнових прав. Фізична особа має право вимагати спростування недостовірної інформації про себе, заборони її поширення без згоди та відшкодування моральної чи матеріальної шкоди, завданої порушенням. Ці норми створюють цивільно-правові інструменти для судового захисту, що посилюють відповідальність за зловживання даними, зокрема в комерційних чи державних сферах [11].

Кримінальний кодекс України встановлює відповідальність за порушення у сфері персональних даних. Незаконне збирання, використання чи поширення конфіденційної інформації може кваліфікуватися як злочин проти приватності, передбачаючи санкції у вигляді штрафів або позбавлення волі. Такий підхід має превентивний ефект, стримуючи порушення в чутливих галузях, таких як медицина, банківська справа чи державні реєстри, де обробляються значні обсяги даних [12].

Міжнародний досвід захисту персональних даних пропонує цінні уроки для України. У Європейському Союзі Загальний регламент із захисту даних (GDPR) встановлює високі стандарти, включаючи принципи прозорості, згоди, права на забуття та обов'язкове призначення офіцерів із захисту даних для великих організацій. GDPR має екстериторіальну дію, впливаючи на компанії за межами ЄС, і передбачає значні штрафи за порушення, що стимулює дотримання стандартів. У Сполучених Штатах регулювання є секторальним, без єдиного федерального закону. Наприклад, California Consumer Privacy Act надає права на доступ і видалення даних, але захист залежить від конкретної галузі чи штату. Такий фрагментований підхід ускладнює уніфікований захист, але окремі закони, як Закон про захист конфіденційності дітей в Інтернеті, демонструють ефективність у специфічних сферах. Канада застосовує комплексний підхід через Закон про захист персональних даних та електронні документи (PIPEDA), який регулює комерційну обробку даних із акцентом на згоду та прозорість. Незалежний наглядовий орган забезпечує контроль за дотриманням норм, що може слугувати прикладом для України в контексті посилення інституційного нагляду [4, с. 292].

Аналіз українського законодавства у сфері захисту персональних даних, проведений у звіті 2023 року, свідчить про існування значних прогалин, які обмежують ефективність правового регулювання [1]. Зокрема, відсутнє детальне регулювання обробки чутливих даних, таких як відомості про здоров'я, релігійні переконання чи етнічне походження, що потребують особливого захисту через їхню високу вразливість. Крім того, недостатньо розвинені механізми регулювання автоматизованої обробки даних, яка стає дедалі поширенішою в умовах цифровізації. Обмежена незалежність наглядового органу знижує ефективність контролю за дотриманням законодавства. Для гармонізації з міжнародними стандартами, зокрема з GDPR, пропонується запровадити обов'язкову оцінку впливу на приватність для операцій із високим ризиком порушення прав суб'єктів даних. Такі оцінки допоможуть ідентифікувати потенційні загрози ще на етапі планування обробки даних. Крім того, необхідно посилити інституційні механізми, включаючи створення чітких процедур нагляду та підвищення кваліфікації фахівців, відповідальних за захист даних [1].



Практичні аспекти захисту персональних даних в Україні охоплюють низку обов'язкових процедур, спрямованих на забезпечення безпеки інформації. Законодавство вимагає реєстрації баз персональних даних у відповідних органах, що сприяє прозорості їх обробки. Призначення відповідальних осіб, які контролюють дотримання вимог законодавства, є ще одним важливим елементом. Технічні заходи, такі як шифрування, двофакторна аутентифікація та системи контролю доступу, відіграють ключову роль у запобіганні несанкціонованому доступу до даних. Згода суб'єкта даних залишається центральним принципом обробки, причому володільці баз даних зобов'язані чітко інформувати суб'єктів про цілі, обсяг і строки використання їхніх даних. Ці заходи допомагають організаціям, як державним, так і приватним, уникати порушень у повсякденній діяльності. Однак сучасні виклики, такі як зростання обсягів даних і поява нових технологій обробки, вимагають постійного вдосконалення цих механізмів, включаючи впровадження новітніх технологій захисту, таких як блокчейн, та регулярне оновлення процедур для відповідності динамічним стандартам безпеки [2, с. 150].

Цифровізація суспільства, яка супроводжується швидким зростанням онлайн-сервісів, електронного врядування та цифрових транзакцій, значно підвищує ризики кіберзагроз, таких як витоки даних, хакерські атаки та фішинг. Для України, де обсяг цифрових операцій невіддільно зростає, це створює додаткові виклики для законодавства та практики захисту даних. Використання штучного інтелекту для моніторингу обробки даних може суттєво підвищити ефективність виявлення порушень і прогнозування ризиків. Наприклад, алгоритми машинного навчання здатні аналізувати великі масиви даних у реальному часі, виявляючи підозрілі дії. Проте таке використання технологій потребує чіткого етичного регулювання, щоб уникнути зловживань, таких як надмірне стеження чи дискримінація. Впровадження етичних стандартів для використання штучного інтелекту в обробці даних має стати пріоритетом, щоб забезпечити баланс між технологічними інноваціями та захистом прав людини [3, с. 95].

Питання співвідношення інформації про особу та персональних даних є важливим для вдосконалення правового регулювання. У державних реєстрах, де накопичуються значні обсяги даних, таких як реєстри виборців чи медичні бази, відсутність чіткого правового розмежування між цими категоріями створює передумови для зловживань. Наприклад, недостатньо захищені реєстри можуть стати об'єктом атак або незаконного використання. Тому необхідне чітке законодавче визначення меж обробки таких даних і посилення механізмів їх захисту, включаючи обов'язкове шифрування та аудит доступу [6, с. 120].

Розвиток інформаційного суспільства підкреслює необхідність уніфікації українського законодавства з міжнародними стандартами, зокрема з Конвенцією Ради Європи № 108 «Про захист осіб щодо автоматизованої обробки персональних даних». Ця конвенція акцентує на правах суб'єктів даних, таких як доступ до власної інформації, її виправлення чи видалення. Ці права є критично важливими для запобігання дискримінації, зокрема в контексті автоматизованого прийняття рішень, яке може базуватися на обробці персональних даних. Наприклад, у фінансовій чи медичній сферах помилкові дані можуть призвести до несправедливих рішень, таких як відмова у кредиті чи лікуванні. Уніфікація з міжнародними стандартами сприятиме не лише захисту прав громадян, але й підвищенню конкурентоспроможності України на міжнародній арені, адже відповідність таким стандартам є умовою співпраці з багатьма іноземними партнерами [7, с. 100].

Однією з ключових проблем українського законодавства залишається недостатня узгодженість норм і слабкий контроль за їх виконанням. Наявні механізми нагляду не забезпечують належного рівня відповідальності за порушення, а наглядовий орган потребує більшої автономії та ресурсів. Створення спеціалізованого органу з захисту персональних даних, подібного до європейських інституцій, могло б значно підвищити ефективність правозастосування. Такий орган мав би повноваження проводити аудити, накладати санкції та надавати консультації організаціям щодо дотримання законодавства. Крім того, це сприятиме підвищенню довіри громадян до системи захисту даних, що є важливим у контексті



зростання цифрових сервісів і масового використання персональних даних у повсякденному житті [5].

Висновки. Правові основи захисту персональних даних в Україні базуються на конституційних нормах і спеціалізованих законах, але потребують комплексного оновлення для відповідності сучасним викликам цифровізації. Гармонізація з міжнародними стандартами, зокрема з GDPR і Конвенцією Ради Європи № 108 «Про захист осіб щодо автоматизованої обробки персональних даних», посилення відповідальності за порушення та впровадження сучасних технологій захисту, таких як блокчейн і штучний інтелект, сприятимуть розвитку інформаційного суспільства з повагою до прав людини. Необхідно також створити незалежний наглядовий орган із достатніми повноваженнями та ресурсами для ефективного контролю за дотриманням законодавства. Крім того, підвищення обізнаності громадян і організацій щодо захисту даних та впровадження етичних стандартів для використання новітніх технологій є важливими кроками для забезпечення безпеки інформації в умовах цифрової трансформації.

Список використаних джерел:

1. Аналіз законодавства про захист персональних даних України: звіт. 10 жовтня 2023 р. URL: https://ecpl.com.ua/wp-content/uploads/2023/10/UKR_10102023_CEP_Finalnyy-zvit.pdf (дата звернення: 07.10.2025).
2. Бем М.В., Городиський І.М. Захист персональних даних: правове регулювання та практичні аспекти: науково-практичний посібник. Київ: К.І.С., 2015. 220 с.
3. Биков О.М., Савченко В.В. Захист персональних даних у сучасному законодавстві. *Вісник юридичної науки*. 2024. № 14. С. 89–100.
4. Головацький Н.Т. Правове регулювання захисту персональних даних: GDPR та законодавство США, Канади й України. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Т. 2, № 85. С. 288–292.
5. Головченко В. Правові основи захисту персональних даних. *Юридична газета онлайн*. 2018. № 36. URL: <https://yur-gazeta.com/publications/practice/inshe/pravovi-osnovi-zahistu-personalnih-danih.html> (дата звернення: 07.10.2025).
6. Кардаш А.В. Інформація про особу та персональні дані: окремі аспекти співвідношення. Конституційно-правовий захист інформації про особу (порівняльно-правовий аспект). Харків, 2019. 228 с.
7. Обухівська Т.І. Захист персональних даних в умовах розвитку інформаційного суспільства: передумови, принципи та міжнародне законодавство. *Вісник Національної академії державного управління при Президентові України*. 2014. № 1. С. 95–103.
8. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254k/96-vr#Text> (дата звернення: 07.10.2025).
9. Про захист персональних даних: Закон України від 1 червня 2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 07.10.2025).
10. Про інформацію: Закон України від 2 жовтня 1992 р. № 2657-XII (у редакції від 16.07.2020). *Відомості Верховної Ради України (ВВР)*. 1992. № 48. Ст. 650. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата звернення: 07.10.2025).
11. Цивільний кодекс України: Закон України від 16 січня 2003 р. № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text> (дата звернення: 07.10.2025).
12. Кримінальний кодекс України: Закон України від 5 квітня 2001 р. № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення: 07.10.2025).

Дата першого надходження рукопису до видання: 14.11.2025

Дата прийнятого до друку рукопису після рецензування: 15.12.2025

Дата публікації: 31.12.2025

