КРАВЧУК В. О.,
orcid.org/0009-0003-6660-2952
аспірантка кафедри конституційного
і адміністративного права
*(Державний університет «Київський
авіаційний інститут»)*

УДК 342.9:004.738.5:004.056.5
DOI https://doi.org/10.32842/2078-3736/2025.6.29

МЕХАНІЗМИ ДЕРЖАВНОГО КОНТРОЛЮ ЗА ДОТРИМАННЯМ ПРАВ КОРИСТУВАЧІВ ПІД ЧАС ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ У ЦИФРОВИХ ПЛАТФОРМАХ

Статтю присвячено дослідженню механізмів державного контролю за дотриманням прав користувачів під час обробки персональних даних цифровими платформами в умовах стрімкої цифровізації суспільних відносин. Проаналізовано конституційні гарантії, положення спеціального законодавства України та міжнародні стандарти у сфері захисту персональних даних. Розглянуто європейський досвід, зокрема принципи Загального регламенту про захист даних (GDPR), модернізованої Конвенції № 108+ і Директиви (ЄС) 2016/680 щодо повноважень наглядових органів, санкційних механізмів і транскордонної взаємодії. Проаналізовано специфіку роботи соціальних мереж, сервісів електронної комерції, хмарних і освітніх платформ. Установлено, що вони створюють багаторівневу систему збору та обробки персональних даних користувачів для комерційного, політичного та технологічного використання. Виявлено основні ризики порушення прав, що підриває інформаційну автономію особи.

Проаналізовано чинну систему державного контролю за захистом даних в Україні, зокрема діяльність Уповноваженого Верховної Ради з прав людини та Департаменту із захисту персональних даних. Встановлено дефіцит технічної експертизи для алгоритмічного аудиту, відсутність санкційних повноважень і механізмів міжнародної координації. Окреслено напрями реформування – створення незалежного регулятора відповідно до законопроєктів № 6177 і № 8153, запровадження технологічного аудиту систем рекомендацій і таргетингу, публічного реєстру порушень та уніфікованих форматів інцидентних повідомлень. Розкрито триступеневу систему юридичної відповідальності (адміністративну, цивільно-правову, кримінальну) й обґрунтовано потребу надання майбутньому регулятору повноважень брати участь у судових провадженнях. На прикладі рішення Європейської ради із захисту даних про накладення штрафу на Meta Platforms Ireland показано дієвість незалежного нагляду та необхідність комплексної модернізації державного контролю для практичної реалізації цифрових прав людини.

Ключові слова: *персональні дані, цифрові платформи, обробка даних, інформаційна безпека, механізми контролю, приватність, правове регулювання.*

Kravchuk V. O. Mechanisms of state control over the protection of users' rights in the processing of personal data on digital platforms

The article is devoted to the study of state control mechanisms over the observance of users' rights during the processing of personal data by digital platforms in the context of rapid digitalization of social relations. The constitutional guarantees, provisions of Ukraine's special legislation, and international standards in the field of personal

data protection are analyzed. The European experience is examined, in particular the principles of the General Data Protection Regulation (GDPR), the modernized Convention No. 108+, and Directive (EU) 2016/680 concerning the powers of supervisory authorities, sanction mechanisms, and cross-border cooperation. The specifics of the functioning of social networks, e-commerce services, cloud, and educational platforms are analyzed. It is established that they form a multi-level system for collecting and processing users' personal data for commercial, political, and technological purposes. The main risks of rights violations have been identified, undermining the individual's informational autonomy.

The article is devoted to the study of state control mechanisms over the observance of users' rights during the processing of personal data by digital platforms in the context of rapid digitalization of social relations. The constitutional guarantees, provisions of Ukraine's special legislation, and international standards in the field of personal data protection are analyzed. The European experience is examined, in particular the principles of the General Data Protection Regulation (GDPR), the modernized Convention No. 108+, and Directive (EU) 2016/680 concerning the powers of supervisory authorities, sanction mechanisms, and cross-border cooperation. The specifics of the functioning of social networks, e-commerce services, cloud, and educational platforms are analyzed. It is established that they form a multi-level system for collecting and processing users' personal data for commercial, political, and technological purposes. The main risks of rights violations have been identified, undermining the individual's informational autonomy.

The article analyzes the current system of state control over data protection in Ukraine, particularly the activities of the Verkhovna Rada Commissioner for Human Rights and the Department for Personal Data Protection. It identifies a lack of technical expertise for algorithmic audits, the absence of sanctioning powers, and limited mechanisms of international coordination. The directions for reform are outlined – the establishment of an independent regulatory authority in line with draft laws No. 6177 and No. 8153, the introduction of technological audits of recommendation and targeting systems, a public register of violations, and unified formats for incident reporting. The paper describes a three-tier system of legal liability (administrative, civil, and criminal) and substantiates the need to empower the future regulator to participate in judicial proceedings. Using the example of the European Data Protection Board's decision to impose a fine on Meta Platforms Ireland, the article demonstrates the effectiveness of independent oversight and underscores the need for comprehensive modernization of state control to ensure the practical realization of digital human rights.

Key words: *personal data, digital platforms, data processing, information security, control mechanisms, privacy, legal regulation.*

Вступ. Стрімка цифровізація суспільних відносин створює нові виклики для захисту прав людини. Одним із найважливіших залишається право на приватність і контроль над власною інформацією. Цифрові платформи, що стали невід'ємною частиною повсякденного життя мільйонів користувачів, здійснюють масштабне збирання, обробку та використання персональних даних, створюючи ризики несанкціонованого доступу, витоку інформації та маніпулятивного впливу на поведінку громадян. На думку дослідників, у глобальному інформаційному просторі людина стає особливо вразливою, тому потрібні дієві механізми захисту її інформаційних прав [1, с. 497]. Ефективність даної системи залежить від здатності держави забезпечити дієвий контроль за дотриманням законодавства про захист персональних даних. Масштаби та технічна складність порушень у цифровому середовищі часто перевищують можливості традиційного нагляду. Тому важливо оновити механізми державного контролю, які підтримуватимуть баланс

між інтересами цифрових операторів, національною безпекою та правом людини на приватне життя.

Постановка завдання. Метою статті є аналіз чинних механізмів державного контролю за дотриманням прав користувачів під час обробки персональних даних цифровими платформами та обґрунтування напрямів їх удосконалення відповідно до європейських стандартів.

Результати дослідження. Система правового регулювання захисту персональних даних в Україні має комплексний характер і поєднує конституційні гарантії з положеннями спеціального законодавства та міжнародних договорів. Конституція України у ст. 32 закріплює засадниче право кожної особи на повагу до приватного життя та забороняє будь-яке втручання в нього без належних правових підстав [2]. Розгорнуте нормативне регулювання забезпечує Закон України № 2297-VI від 01.06.2010 року «Про захист персональних даних» (далі – Закон), який визначає права фізичних осіб щодо контролю за власною інформацією (ст. 8), встановлює обов'язки володільців і розпорядників даних (ст. 11), а також окреслює механізми державного нагляду (ст. 22) [3]. Важливу роль відіграють також міжнародні стандарти, зокрема Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних № 108 від 28.01.1981 року та Додатковий протокол від 08.11.2001 року, які зобов'язують держави створювати незалежні органи контролю й гарантувати належний рівень захисту під час транскордонного обміну інформацією [4; 5]. У результаті формується цілісна модель правового захисту персональних даних, що узгоджує національні принципи законності й пропорційності з європейськими вимогами інформаційної безпеки та поваги до людської гідності.

Становлення української системи захисту персональних даних логічно вписується у ширший міжнародний контекст, сформований під впливом європейського права. Центральним документом є Загальний регламент про захист даних від 27.04.2016 року. Зазначений нормативно-правовий акт у ст. 5 закріплює ключові принципи обробки інформації: правомірність, добросовісність, пропорційність, цільове обмеження, мінімізацію та точність даних, а також безпеку й підзвітність. Подальші статті, зокрема 51 та 58, деталізують повноваження наглядових органів, передбачаючи їхню незалежність, контрольні та санкційні функції, включно з правом накладати штрафи до 20 млн євро або 4% від світового обороту компанії-порушника [6]. Важливим доповненням стала модернізована Конвенція № 108+ від 18.05.2018 року, яка розширила предмет регулювання, охопивши генетичні, біометричні й поведінкові дані, а також сфери автоматизованого ухвалення рішень і профілювання [7]. Окреме значення має Директива (ЄС) 2016/680 від 27.04.2016 року, що встановлює стандарти обробки персональної інформації у правоохоронній діяльності [8]. Імплементація міжнародних стандартів має враховувати національні правові особливості, рівень цифрової зрілості та інституційні можливості, забезпечуючи реальне, а не формальне дотримання принципу приватності.

Вважаємо, що ефективний правовий захист персональних даних неможливий без поєднання нормативних засад і технологічних гарантій їх реалізації. Законодавчі приписи набувають практичного змісту лише тоді, коли принципи законності, мінімізації та прозорості відображені у самій логіці функціонування цифрових систем. Так, концепція «захисту даних за призначенням і за замовчуванням», закріплена у ст. 25 Загального регламенту про захист даних, вимагає інтеграції безпекових механізмів у процеси проєктування, експлуатації та адміністрування інформаційних платформ. Водночас технічна частина захисту передбачає впровадження багаторівневої аутентифікації, шифрування, автоматичного контролю дій користувачів і незалежного аудиту систем обробки даних [6]. У такий спосіб правове регулювання набуває системного характеру, коли норми закону підкріплюються технічними засобами превенції порушень. Така інтеграція забезпечує стабільність функціонування інформаційного простору, підвищує довіру користувачів до цифрових сервісів і сприяє формуванню культури відповідального використання персональних даних.

Характеристика цифрових платформ із погляду обробки персональних даних свідчить про виражену гетерогенність і розмаїття підходів до збору та використання інформації про користувачів. Так, TikTok систематично збирає поведінкові, контентні та біометричні дані, використовуючи їх для персоналізації рекомендацій і прогнозування дій користувачів, що підвищує ризики порушення приватності [9; 10]. Подібні методи збору та аналізу даних застосовують й інші глобальні соціальні мережі, зокрема Instagram і Facebook, де алгоритми формують психографічні профілі користувачів на основі відстеження інтересів, локації, часу активності та взаємодії з контентом [11; 12]. Водночас платформи електронної комерції (наприклад, Amazon) аналізують історію покупок, пошукові запити, перегляди товарів для персоналізації рекомендацій і прогнозування поведінки споживачів [13]. Майданчики спільної економіки – як-от Uber – в обігу мають дані про переміщення, фінансові транзакції, рейтинги учасників, що дозволяє будувати систему довіри між користувачами й оптимізувати ціноутворення [14]. Окрім того, хмарні сервіси типу Google Drive оперують як із корпоративними, так і з особистими файлами користувачів, через що зростають ризики несанкціонованого доступу та витоку інформації [15]. У сфері освітніх платформ (наприклад, Coursera) формується новий тип даних – про навчальний прогрес, результати тестування, час виконання завдань, який використовується для аналізу ефективності процесу і видачі сертифікатів [16].

Так, цифрові платформи формують складну екосистему збирання персональних даних, у якій взаємодіють як активні, так і пасивні механізми спостереження. Користувачі добровільно залишають інформацію під час реєстрації, заповнення профілю чи пошукових запитів, тоді як основний масив даних збирається непомітно – через файли cookie, пікселі відстеження, відбитки пристроїв і браузерів. Отримані відомості об'єднуються за допомогою єдиних облікових записів, вбудованих рекламних модулів та посередників із торгівлі даними, що дозволяє створювати цілісні поведінкові профілі. Зберігання інформації у розподілених дата-центрах різних держав ускладнює визначення юрисдикції й контроль за законністю обробки. Надалі зазначені дані використовують не лише для вдосконалення сервісів, а й для комерційного продажу, політичного мікротаргетингу чи навчання алгоритмів штучного інтелекту. Подібні процеси породжують суттєві ризики для конфіденційності та інформаційної безпеки користувачів.

На наш погляд, потенційні ризики порушення прав користувачів цифрових платформ охоплюють широкий спектр загроз, що безпосередньо впливають на приватність і свободу людини. Витоки персональних даних унаслідок кібератак чи технічної недбалості стали системним явищем. Згідно з даними звіту про розслідування витоків даних 2025 року, інформація про фізичних осіб була розкрита у 37 % випадків порушень безпеки [17, с. 71]. Такі інциденти нерідко призводять до крадіжки ідентичності, фінансових збитків і втрати контролю над власною інформацією. Не менш небезпечними є алгоритмічне профілювання, мікротаргетинг і приховані моделі впливу, які здатні маніпулювати поведінкою користувачів, формувати залежності та викликати соціальну поляризацію. Сукупний ефект зазначених явищ породжує ефект тотального спостереження. Усвідомлення постійного контролю спричиняє самоцензуру, знижує критичність мислення та підриває автономію особистості.

Контроль за дотриманням законодавства у сфері захисту персональних даних в Україні реалізується через поєднання інституційних і процесуальних механізмів, передбачених розділом VI Закону України № 2297-VI від 01.06.2010 року «Про захист персональних даних». Згідно зі ст. 22 зазначеного нормативно-правового акту, нагляд за дотриманням прав користувачів здійснюють Уповноважений Верховної Ради України з прав людини та суди. У межах наданих повноважень Омбудсмен є єдиним органом контролю, уповноваженим на здійснення перевірок суб'єктів обробки інформації. Відповідно до ст. 23 Закону, наглядові функції включають аналіз скарг, ініціювання перевірок, доступ до приміщень та документів володільців даних, а також можливість видавати обов'язкові приписи щодо усунення порушень [3]. Вважаємо, що централізація контролю у руках одного суб'єкта дозволяє уникнути дублювання функцій. Водночас така модель обмежує ефективність реагування у цифровому

середовищі, де масштаби порушень та їх технічна складність часто перевищують інституційні ресурси Омбудсмена.

Нормативне підґрунтя перевірок деталізовано у наказі Уповноваженого № 1/02-14 від 08.01.2014 року «Про затвердження Порядку здійснення контролю за додержанням законодавства про захист персональних даних» [18]. Відповідно до п. 2.1 даного акту, контроль реалізується у формах планових і позапланових, виїзних і безвиїзних перевірок. За результатами перевірки, згідно з п. 4.1–4.3 Порядку, складається акт перевірки, який може містити вимогу про припинення незаконної обробки персональних даних, їх видалення або знищення, а також рекомендації щодо усунення виявлених порушень. У разі невиконання приписів або виявлення грубих порушень законодавства Уповноважений має право скласти протокол про адміністративне правопорушення. Такі дії тягнуть за собою адміністративну відповідальність, передбачену статтями 188[39] та 188[40] Кодексу України про адміністративні правопорушення, які встановлюють штрафи за неповідомлення або несвоєчасне повідомлення Уповноваженого про обробку персональних даних, а також за невиконання його законних вимог [19].

Важливою формою державного контролю, що поєднує аналітичний і профілактичний підходи, є моніторинг у сфері персональних даних. Відповідно до п. 12 ст. 23 Закону, моніторинг охоплює постійне відстеження тенденцій, технологічних рішень і практик обробки персональної інформації [3]. Зазначену функцію виконує Департамент з питань захисту персональних даних у структурі Секретаріату Уповноваженого Верховної Ради України з прав людини. На наш погляд, діяльність згаданого підрозділу має ключове значення для реалізації принципу підзвітності, оскільки він забезпечує аналітичний супровід політики у сфері захисту даних, проводить перевірки, готує щорічні звіти про стан дотримання законодавства, а також здійснює роз'яснювальну роботу серед суб'єктів обробки та громадськості [20].

Попри відносну стабільність нагляду, вважаємо, що чинна модель не забезпечує повного циклу примусу та міжнародної координації. Департамент із питань захисту персональних даних фактично виконує аналітичні, методичні й інспекційні функції, проте не наділений владними повноваженнями для ухвалення обов'язкових рішень і накладення санкцій. Подібна організація роботи зберігає залежність від подальших дій інших органів, що сповільнює реагування на інциденти, зокрема при транскордонній обробці. Законопроєкт № 6177 від 18.10.2021 р. «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації» пропонує логічне інституційне продовження: незалежну колегіальну комісію зі спеціальним процесуальним механізмом перевірок, приписів і штрафів, а також з правом міжнародної взаємодії з європейськими наглядовими органами [21]. Така модель наближає Україну до вимог ст. 51 і ст. 58 Загального регламенту про захист даних у частині незалежності, підзвітності та ефективного примусу [6]. Доцільно також прямо закріпити технічну спроможність майбутнього регулятора: лабораторію цифрових доказів, центр алгоритмічного аудиту та публічний портал інцидентних повідомлень.

Паралельно законопроєкт № 8153 від 25.10.2022 р. «Про захист персональних даних» модернізує матеріально-правову базу. Він оновлює терміни, уточнює обов'язки контролера й оператора, запроваджує 72-годинний строк для повідомлення про порушення безпеки, деталізує оцінку впливу на захист даних і правила міжнародних передач. Узгодження з положеннями Загального регламенту про захист даних простежується у принципах підзвітності, мінімізації, прозорості та безпеки [6; 22]. Водночас бракує чіткого визначення високоризикових сценаріїв для великих платформ, які мають масову аудиторію та здійснюють глибоке профілювання користувачів. На наш погляд, доцільно закріпити обов'язковий щорічний технологічний аудит систем рекомендацій і таргетингу. Його результати мають оформлюватися у вигляді публічного звіту з обмеженим обсягом відомостей для користувача. Варто також установити мінімальні вимоги до журналювання доступів і змін налаштувань безпеки, які повинні зберігатися щонайменше два роки. Запровадження зазначених механізмів забезпечить процесуальну базу для швидкого доказування у справах про витоки й маніпулятивні практики та підсилить взаємну довіру між ринком і державою. На практичному рівні

доцільно запровадити уніфікований формат інцидентних повідомлень. Такий стандартизований шаблон має містити обов'язкові реквізити: тип інциденту (витік, несанкціонований доступ, технічний збій), обсяг скомпрометованих даних, категорії суб'єктів, часові рамки виявлення та початкові заходи реагування. Уніфікація дозволить регулятору швидко оцінити масштаб загрози, порівняти інциденти між платформами та сформувати статистичну базу для превентивної політики. Варто також визначити чітку матрицю критеріїв, що розмежовує випадки обов'язкового інформування суб'єктів і допустимого відтермінування за умови негайної нейтралізації ризику. Зокрема, критеріями можуть бути: 1) чутливість даних (медичні, фінансові, біометричні відомості вимагають негайного повідомлення); 2) кількість постраждалих осіб (масові витоки не підлягають відкладенню); 3) характер загрози (потенціал шахрайства або шкоди для здоров'я, тощо); 4) можливість оперативного усунення вразливості без розголошення технічних деталей, що могли б бути використані зловмисниками. Така матриця забезпечить баланс між правом людини знати про ризики та необхідністю захистити інфраструктуру від подальших атак.

Окремої уваги потребує система юридичної відповідальності, яка має стати реальним інструментом забезпечення виконання норм оновленого законодавства. Адміністративний рівень, згаданий раніше, передбачає санкції за перешкоджання перевіркам, невиконання приписів і порушення строків інформування Уповноваженого про обробку персональних даних. Цивільно-правовий рівень дає потерпілій особі право вимагати відшкодування матеріальної або моральної шкоди в судовому порядку. Підставами є ст. 16, 23, 277–280 Цивільного кодексу України, ст. 32 Конституції України та ст. 28 Закону «Про захист персональних даних» [2; 3; 23]. Кримінальний рівень, закріплений у ст. 182 Кримінального кодексу України. Норма охоплює як активні дії (збирання, поширення, використання), так і бездіяльність, що призвела до порушення права на приватність. За такі порушення передбачено штраф, виправні роботи, пробаційний нагляд або позбавлення волі до 5 років залежно від тяжкості наслідків. При цьому закон визначає поріг істотної шкоди та робить виняток для публічного розголошення інформації про правопорушення, здійсненого в межах закону [24]. Триступенева модель узгоджується з правом Європейського Союзу, проте в Україні бракує швидкого доведення порушень і сталої судової практики. Доцільно надати майбутній комісії повноваження ініціювати адміністративні провадження, передавати матеріали до правоохоронних органів у разі кримінальних правопорушень і брати участь у цивільних справах як експертний суб'єкт. Розширення компетенції даного органу створить підґрунтя для реальної невідворотності відповідальності та перетворить нагляд на дієвий механізм реагування.

Показовим прикладом ефективної практики контролю у сфері захисту персональних даних є рішення Європейської ради із захисту даних від 13 квітня 2023 року. На його підставі ірландський регулятор застосував до Meta Platforms Ireland фінансову санкцію у розмірі 1,2 млрд євро. Порушення полягало у систематичному й тривалому передаванні персональних даних користувачів до Сполучених Штатів без належного правового обґрунтування [25]. Прецедент продемонстрував, що серйозні порушення у сфері приватності тягнуть за собою значні фінансові наслідки, а незалежні наглядові органи відіграють вирішальну роль у забезпеченні законності у цифровому середовищі. Досвід Європейського Союзу переконливо доводить потребу створення в Україні повноцінного регулятора з реальними інституційними важелями, здатного забезпечити не лише фіксацію порушення, а і його повне усунення відповідно до принципів справедливості та верховенства права.

Висновки. Дослідження показало, що результативність державного контролю за дотриманням прав користувачів цифрових платформ залежить не лише від законодавчої бази, а й від здатності наглядового органу швидко реагувати на порушення у складному технологічному середовищі. Нинішня українська модель, у якій контрольні функції зосереджені в Омбудсмана, є малоефективною через відсутність санкційних повноважень і фахових ресурсів для аналізу алгоритмів. Потрібен незалежний регулятор, який матиме реальні повноваження впливу. Реформа має включати превентивні заходи – аудит високоризикових технологій, відкритий реєстр порушень, стандартизовані протоколи реагування

та міжнародну координацію. Лише комплексне оновлення системи дасть змогу перейти від формального контролю до реального захисту цифрових прав і забезпечити підзвітність великих платформ перед суспільством і державою.

Список використаних джерел:

1. Токарєва К. Проблема захисту персональних даних у сфері охорони здоров'я в умовах інформатизації. *Юридичний науковий електронний журнал*. 2022. № 11. С. 496-499.

2. Конституція України : від 28.06.1996 № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 22.10.2025).

3. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 14 черв. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 22.10.2025).

4. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Конвенція Ради Європи від 28.01.1981 : станом на 6 лип. 2010 р. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 22.10.2025).

5. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних : Протокол Ради Європи від 08.11.2001 : станом на 6 лип. 2010 р. URL: https://zakon.rada.gov.ua/laws/show/994_363#Text (дата звернення: 22.10.2025).

6. 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) : Регламент Європ. Союзу від 27.04.2016 № 2016/679. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 22.10.2025).

7. Convention 108+: Convention for the protection of individuals with regard to the processing of personal data. *Council of Europe*. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (дата звернення: 23.10.2025).

8. On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA : Directive (EU) of 27.04.2016 no. 2016/680. URL: http://data.europa.eu/eli/dir/2016/680/oj (дата звернення: 23.10.2025).

9. Exploring and Analyzing the Data Practices of Tiktok / N. Çömezoğlu, B. Okudurlar, D. Barışkan, D. Barışkan. 2024. URL: https://www.researchgate.net/publication/380577142_Exploring_and_Analyzing_the_Data_Practices_of_Tiktok (дата звернення: 23.10.2025).

10. TikTok. *Офіційний веб-сайт*. URL: https://www.tiktok.com (дата звернення: 23.10.2025).

11. Instagram. *Офіційний веб-сайт*. URL: https://www.instagram.com/ (дата звернення: 23.10.2025).

12. Facebook. *Офіційний веб-сайт*. URL: https://www.facebook.com (дата звернення: 23.10.2025).

13. Amazon. *Офіційний веб-сайт*. URL: https://www.amazon.com/ (дата звернення: 23.10.2025).

14. Uber. *Офіційний веб-сайт*. URL: https://www.uber.com/ (дата звернення: 23.10.2025).

15. Google Drive. *Google Workspace*. URL: https://drive.google.com/drive/ (дата звернення: 23.10.2025).

16. Coursera. *Офіційний веб-сайт*. URL: https://www.coursera.org/ (дата звернення: 23.10.2025).

17. 2025 Data Breach Investigations Repor / C. David Hylender, P. Langlois, A. Pinto, S. Widup. 2025. 115 p. URL: https://www.verizon.com/business/resources/Tf24/reports/2025-dbir-data-breach-investigations-report.pdf (дата звернення: 23.10.2025).

18. Про затвердження документів у сфері захисту персональних даних : Наказ Уповноваж. Верхов. Ради України з прав людини від 08.01.2014 № 1/02-14 : станом на 19 верес. 2018 р. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text (дата звернення: 24.10.2025).

19. Кодекс України про адміністративні правопорушення: Кодекс України від 07.12.1984 № 8073-X : станом на 1 верес. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення: 24.10.2025).

20. Інформація про Департамент у сфері захисту персональних даних. *Омбудсман України*. URL: https://ombudsman.gov.ua/uk/informaciya-pro-pidrozdil-zpd (дата звернення: 24.10.2025).

21. Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації : проект Закону України від 18.10.2021 № 6177. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/27996 (дата звернення: 24.10.2025).

22. Про захист персональних даних : проект Закону України від 25.10.2022 № 8153. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/40707 (дата звернення: 24.10.2025).

23. Цивільний кодекс України : Кодекс України від 16.01.2003 № 435-IV : станом на 5 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 24.10.2025).

24. Кримінальний кодекс України : Кодекс України від 05.04.2001 № 2341-III : станом на 17 лип. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 24.10.2025).

25. 1.2 billion euro fine for Facebook as a result of EDPB binding decision. *EDPB*. URL: https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en (дата звернення: 27.10.2025).

Дата першого надходження рукопису до видання: 06.11.2025
Дата прийнятого до друку рукопису після рецензування: 15.12.2025
Дата публікації: 31.12.2025