УДК 342.7:341.17:004
DOI https://doi.org/10.32844/2618-1258.2026.1.38

МАЛЬЦЕВ С. Ю.

ПРАВОВІ БАР'ЄРИ ІНТЕГРАЦІЇ УКРАЇНИ ДО ЄВРОПЕЙСЬКИХ ПРОСТОРІВ ДАНИХ: ІНСТИТУЦІЙНІ КОЛІЗІЇ ТА ЗАХИСТ ПРИВАТНОСТІ

LEGAL BARRIERS TO UKRAINE'S INTEGRATION INTO EUROPEAN DATA SPACES: INSTITUTIONAL COLLISIONS AND PRIVACY PROTECTION

У статті здійснено системний аналіз нормативно-правових та інституційних перешкод, що виникають на шляху інтеграції України до Єдиного цифрового ринку ЄС, зокрема до Європейських просторів даних (Common European Data Spaces). Актуальність теми зумовлена необхідністю імплементації новітнього правового надбання ЄС (acquis communautaire) у сфері економіки даних, зокрема Акту про дані (Data Act) та Акту про управління даними (Data Governance Act), що вимагає від України перегляду фундаментальних підходів до правового регулювання інформаційної сфери.

На основі доктринальних джерел проаналізовано трансформацію традиційних прав людини в цифрову епоху та становлення так званих «прав четвертого покоління», які захищають «віртуальну особистість». Доведено, що в умовах воєнного стану виникає складна дилема між безпекою, свободою слова та захистом приватності, вирішення якої потребує чітких стандартів обмеження прав на основі критеріїв необхідності та пропорційності.

Особливу увагу приділено критичному аналізу інституційної спроможності системи захисту персональних даних в Україні. На підставі звітів Європейської Комісії (Ukraine Report 2023/2024/2025) та положень ст. 52 GDPR обґрунтовано, що чинна модель покладання функцій наглядового органу на Уповноваженого Верховної Ради з прав людини не відповідає критерію «повної незалежності» (complete independence).

Детально розглянуто правову колізію між вимогами антикорупційної прозорості (відкриті реєстри) та європейськими стандартами приватності. Через призму прецедентного рішення Суду ЄС у справі WM and Sovim SA (2022) доведено необхідність переходу від безумовної публічності даних до моделі доступу на основі «легітимного інтересу». Сформульовано пропозиції щодо гармонізації термінологічного апарату та реформи системи юридичної відповідальності.

Ключові слова: *Європейські простори даних (Common European Data Spaces), Data Governance Act, Data Act, права четвертого покоління, віртуальна особистість, інституційна незалежність регулятора, легітимний інтерес, баланс прозорості та приватності, GDPR.*

The article provides a systemic analysis of the regulatory and institutional barriers arising on the path of Ukraine's integration into the EU Digital Single Market, specifically into the Common European Data Spaces. The relevance of the study is driven by the need to implement the latest EU acquis (acquis communautaire) in the field of the data economy, particularly the Data Act and the Data Governance Act, which necessitates a revision of Ukraine's fundamental approaches to the legal regulation of the information sphere.

Based on doctrinal sources, the transformation of traditional human rights in the digital age and the emergence of so-called «fourth-generation rights» protecting the «virtual

© МАЛЬЦЕВ С. Ю. – аспірант кафедри міжнародного права та права Європейського Союзу (Державний податковий університет) https:// orcid.org/0009-0000-5732-1989

personality» are analyzed. It is demonstrated that under martial law, a complex dilemma arises between security, freedom of speech, and privacy protection, the resolution of which requires clear standards for restricting rights based on criteria of necessity and proportionality.

Particular attention is paid to a critical analysis of the institutional capacity of the personal data protection system in Ukraine. Based on European Commission reports (Ukraine Report 2023/2024/2025) and the provisions of Art. 52 of the GDPR, it is substantiated that the current model of assigning the functions of a supervisory authority to the Ukrainian Parliament Commissioner for Human Rights does not meet the criterion of «complete independence.»

The legal collision between anti-corruption transparency requirements (open registers) and European privacy standards is examined in detail. Through the lens of the precedent-setting CJEU ruling in the case of WM and Sovim SA (2022), the need to transition from unconditional data publicity to an access model based on «legitimate interest» is proven. Proposals are formulated for harmonizing the terminological apparatus and reforming the system of legal liability.

Keywords: *Common European Data Spaces, Data Governance Act, Data Act, fourth-generation rights, virtual personality, institutional independence of the regulator, legitimate interest, balance of transparency and privacy, GDPR.*

Вступ. Інтеграція України до європейського правового простору вимагає не лише декларативного визнання європейських цінностей, а й глибокої імплементації технічних та юридичних стандартів ЄС. Розвиток цифрової реальності призвів до появи нової категорії прав людини – так званих прав четвертого покоління (інформаційних прав), які формують та захищають «віртуальну особистість» людини. Як зазначають дослідники О. О. Барабаш та Д. В. Яцків, дотримання і повага цих прав є однією з найбільш важливих ознак правової держави, а їх забезпечення вимагає нових підходів, що виходять за межі традиційних національних юрисдикцій [1, с. 27].

Ключовим елементом Стратегії єдиного цифрового ринку ЄС на 2024–2030 роки є створення Європейських просторів даних (Common European Data Spaces) – у сферах охорони здоров'я, енергетики, фінансів. Для повноцінної участі в них Україна має гарантувати, що дані її громадян та бізнесу захищені так само надійно, як і в ЄС.

Однак на цьому шляху виникають системні перешкоди: застарілість національного законодавства про захист персональних даних, інституційна слабкість регулятора та колізія між курсом на тотальну відкритість даних (open data) та жорсткими вимогами приватності (GDPR).

Аналізуючи останні дослідження і публікації стосовно предмету дослідження слід зазначити, що теоретико-правовий фундамент дослідження складають праці вчених, які розглядають інформаційну безпеку та приватність у комплексі. Зокрема, В. Г. Пилипчук та В. М. Брижко обґрунтовують концепцію балансу інтересів, зазначаючи, що інформаційна безпека особистості є станом захищеності її життєво важливих інтересів в інформаційному середовищі [2, с. 16; 3, с. 62].

Важливий внесок у дослідження стандартів обмеження інформаційних прав та їх відповідності міжнародним нормам зробила Н. П. Капітаненко. Авторка слушно зауважує, що будь-які обмеження, навіть продиктовані необхідністю захисту національної безпеки, повинні відповідати критеріям законності, необхідності та пропорційності [4, с. 54].

Певний внесок у дослідження еволюції прав людини був зроблений І. В. Захарчук, яка розглядає становлення четвертого покоління прав крізь призму глобальних технологічних змін та цифровізації міжнародного права. Дослідниця обґрунтовує виділення цифрових прав в окрему категорію, що включає право на доступ до Інтернету та захист віртуальної ідентичності [5, с. 354].

Питання адміністративно-правового захисту персональних даних та невідповідності українського законодавства європейським стандартам ґрунтовно проаналізовані у монографіях Т. О. Гуржія та А. Л. Петрицького [6, с. 15]. Проте більшість існуючих праць фокусуються на загальних положеннях GDPR, залишаючи поза увагою новітні інструменти цифрової політики ЄС (Data Governance Act, Data Act) та свіжу практику Суду ЄС щодо балансу публічності та приватності, що зумовлює мету цієї статті.

Постановка завдання. Інтеграція України до Єдиного цифрового ринку ЄС перейшла у фазу практичної імплементації, що вимагає від національної правової системи не лише адаптації до вимог GDPR, а й готовності до участі у транскордонних екосистемах обміну даними.

Враховуючи динамічне оновлення законодавства ЄС та специфіку функціонування правової системи України в умовах війни, виникає нагальна потреба у переосмисленні існуючих підходів до регулювання інформаційної сфери.

Метою статті є здійснення комплексного правового аналізу нормативно-правових та інституційних бар'єрів, що перешкоджають повноцінній інтеграції України до Європейських просторів даних (Common European Data Spaces), а також обґрунтування шляхів їх подолання з урахуванням новітніх стандартів захисту «віртуальної особистості» та вимог стратегічної автономії.

Для досягнення поставленої мети у роботі вирішуються такі завдання:

1. З'ясувати правову природу «прав четвертого покоління» та їх роль у формуванні статусу «віртуальної особистості» в умовах цифрової трансформації.

2. Проаналізувати новели законодавства ЄС у сфері економіки даних, зокрема положення Data Governance Act та Data Act, та оцінити їх вплив на зобов'язання України.

3. Ідентифікувати інституційні вади національної системи захисту персональних даних, зокрема щодо відповідності статусу наглядового органу критерію «повної незалежності» (complete independence).

4. Дослідити колізію між вимогами публічності (відкриті реєстри) та правом на приватність крізь призму прецедентної практики Суду справедливості ЄС.

5. Сформулювати пропозиції щодо гармонізації українського законодавства для забезпечення доступу до захищених хмарних середовищ та ринків даних ЄС.

Результати дослідження

1. Трансформація інституту прав людини: феномен «віртуальної особистості» та права четвертого покоління. Інтеграція України до цифрового простору ЄС вимагає переосмислення класичної антропоцентричної моделі права. В умовах тотальної цифровізації відбувається трансформація традиційної правосуб'єктності: фізична особа набуває цифрової проекції, яку в сучасній доктрині визначають як «віртуальну особистість». Як слушно зауважує І. В. Захарчук, цей процес зумовлює необхідність формування четвертого покоління прав людини, які не замінюють, а доповнюють класичні громадянські, політичні та соціальні права [5, с. 353].

Якщо перші три покоління прав формувалися під впливом буржуазних революцій та соціальних рухів XX ст., то четверте покоління є відповіддю на виклики інформаційного суспільства та біотехнологічного прогресу. Аналіз міжнародно-правових актів, зокрема практики ООН та ЄС, дозволяє виокремити ключові елементи цієї групи прав:

Право на доступ до Інтернету (Right to Internet access): розглядається не як технічна можливість, а як фундаментальна передумова реалізації інших прав (на освіту, працю, інформацію). У контексті Єдиного цифрового ринку ЄС це право трансформується у вимогу забезпечення універсального широкосмугового доступу, без якого цифрова інклюзія є неможливою.

Право на інформаційне самовизначення та «цифрове забуття» (Right to be forgotten): ці права складають основу захисту «віртуальної особистості». О. О. Барабаш та Д. В. Яцків підкреслюють, що в умовах, коли цифрова історія людини стає товаром, держава зобов'язана гарантувати контроль особи над її цифровим слідом [1, с. 27].

Право на кібербезпеку: в умовах гібридних загроз, як зазначають дослідники, це право виходить за межі особистої безпеки і стає питанням національного суверенітету.

«Віртуальна особистість» потребує специфічного режиму правової охорони, оскільки вона вразлива до загроз, нехарактерних для фізичного світу: крадіжки цифрової ідентичності, алгоритмічної дискримінації та несанкціонованого профайлінгу. Саме тому І. В. Захарчук наголошує, що міжнародне право в умовах цифровізації зміщує акцент з декларування прав на створення дієвих механізмів їх захисту в транскордонному просторі [5, с. 357].

Для України визнання прав четвертого покоління на законодавчому рівні є не просто теоретичним завданням, а необхідною умовою гармонізації. Європейські регламенти, такі як GDPR (захист даних) та AI Act (регулювання штучного інтелекту), базуються саме на презумпції існування та пріоритеті цих новітніх прав. Без імплементації цієї філософії у національну правову свідомість будь-які технічні євроінтеграційні зміни будуть поверхневими.

2. Гармонізація регулювання: від GDPR до Європейських просторів даних. Реалізація прав четвертого покоління, окреслених вище, на практиці відбувається через імплементацію конкретних нормативних режимів ЄС. Сучасна правова доктрина ЄС розглядає вільний рух даних як «п'яту свободу» єдиного ринку, що доповнює класичні свободи руху товарів, осіб, послуг та капіталу. Ця концепція матеріалізується через створення Європейських просторів даних (Common European Data Spaces) – децентралізованих екосистем, що об'єднують правові норми та технічну

інфраструктуру для безпечного обміну даними у стратегічних секторах (охорона здоров'я, енергетика, агропромисловість, фінанси).

Особливої актуальності це набуває в енергетичному секторі. Г. В. Дугінець та співавтори наголошують, що цифрова трансформація європейської енергетики створює нові виклики для сталого розвитку, вимагаючи від України інтеграції своїх даних до енергетичних балансів ЄС в режимі реального часу, що неможливо без сумісних протоколів обміну [7, с. 108].

Для України інтеграція в ці простори є не просто технічним завданням, а питанням доступу до високотехнологічних ринків. Однак, на відміну від попередніх етапів гармонізації, де домінував захисний підхід (GDPR), нова хвиля acquis communautaire спрямована на стимулювання економіки даних. Критично важливою є імплементація положень двох фундаментальних регламентів, які формують «правила гри» на цьому ринку:

1. **Акт про управління даними (Data Governance Act, DGA – Regulation (EU) 2022/868).** Цей нормативний акт [8] вирішує проблему дефіциту довіри при обміні даними шляхом створення нових правових інститутів, які наразі відсутні в законодавстві України:

Інститут посередників даних (Data Intermediaries)*:* Акт про управління даними (DGA) запроваджує жорстке регулювання для нейтральних третіх сторін (провайдерів послуг з обміну даними), які виступають гарантами транзакцій між власниками даних та їх користувачами. Для українських IT-компаній це означає необхідність проходження спеціальної сертифікації в ЄС, без якої вони не зможуть обслуговувати європейські потоки даних.

Концепція «альтруїзму даних» (Data Altruism): Регламент створює легальний механізм, за яким фізичні особи або компанії можуть добровільно надавати свої дані для цілей загального суспільного інтересу (наприклад, для медичних досліджень або боротьби зі зміною клімату). Для України це вкрай актуально в контексті вивчення наслідків війни та реабілітації, проте без імплементації DGA використання таких масивів даних у спільних з ЄС проектах буде юридично заблоковане.

Повторне використання публічних даних: Акт про управління даними (DGA) відкриває доступ до захищених даних публічного сектору (що містять комерційну таємницю або інтелектуальну власність) через захищені середовища обробки, що вимагає від України модернізації законодавства про доступ до публічної інформації.

2. **Акт про дані (Data Act – Regulation (EU) 2023/2854).** Якщо GDPR захищає персональні дані, то Акт про дані (Data Act) [9] регулює економічний обіг промислових та неперсональних даних, генерованих пристроями «Інтернету речей» (IoT). Цей акт має революційне значення для українського агросектору та промисловості:

Право користувача на доступ до даних: Акт встановлює баланс між виробником обладнання (наприклад, «розумного» комбайна чи верстата) та користувачем (фермером чи заводом). Він зобов'язує виробників відкривати дані, які генерує техніка, що дозволяє користувачам передавати ці дані третім сервісним компаніям для ремонту або аналітики. Без імплементації цих норм українські аграрії залишатимуться у «цифровому рабстві» іноземних виробників техніки.

Усунення бар'єрів для зміни хмарних провайдерів: Акт про дані (Data Act) забороняє практику залежності від постачальника (vendor lock-in), спрощуючи перенесення даних між різними хмарними сервісами. Це критично важливо для кіберстійкості української інфраструктури, яка значною мірою залежить від іноземних хмарних рішень.

Зазначені законодавчі ініціативи не є випадковими, а відображають фундаментальну зміну парадигми цифрового врядування в ЄС. Як зазначає С. Гайдебрехт, Брюссель переходить від політики «ринкового лібералізму» до «публічного інтервенціонізму», де держава бере на себе роль архітектора цифрових екосистем задля забезпечення стратегічної автономії [10, с. 206]. Саме тому імплементація цих регламентів в Україні вимагатиме не лише дерегуляції, а й створення нових, сильних регуляторних інституцій.

Відсутність в Україні аналогічного регулювання створює системний ризик «правової несумісності». Навіть за наявності технічних каналів зв'язку, українські медичні дані (для European Health Data Space) або енергетичні дані не зможуть легально перетинати кордон ЄС, оскільки в Україні відсутні інституційні гаранти довіри (сертифіковані посередники) та правові механізми захисту прав на неперсональні дані. Гармонізація із зазначеними актами є безальтернативною умовою для перетворення України з «цифрової колонії» (постачальника сирих даних) на повноправного учасника Єдиного цифрового ринку.

Втім, практична реалізація цього завдання наштовхується на низку системних перешкод. Процес інтеграції ускладнюється не лише необхідністю формальної рецепції нових регламентів,

а й наявністю глибоких розривів між європейською та українською правовими моделями. Як слушно зауважують дослідники [11, с. 10], фрагментарні зміни часто призводять до конфлікту між застарілою національною системою та динамічним правом ЄС.

На основі проведеного аналізу виокремлено три групи ключових бар'єрів – інституційні, доктринальні та технологічні, що унеможливлюють ефективну інтеграцію на даному етапі.

3. Інституційна неспроможність та проблема незалежного регулятора. Інституційна незалежність наглядового органу є базовою вимогою європейського права. Відповідно до ст. 52 Регламенту GDPR, наглядовий орган має бути повністю незалежним від зовнішнього впливу. В Україні ці функції виконує Уповноважений Верховної Ради з прав людини. Така модель інституційно поєднує функцію парламентського контролю із функцією адміністративного регулювання, що у науковій доктрині оцінюється як потенційно вразлива до політичного впливу та недостатньо забезпечена ресурсно.

За оцінкою експертів, такий статус містить потенційні ризики політичного впливу, що не узгоджується з вимогою «повної незалежності» (complete independence). Ця системна вада, виявлена ще на етапі становлення національної системи захисту даних [12, с. 5], залишається критичним бар'єром і на сучасному етапі євроінтеграції. У офіційних звітах Європейської Комісії в рамках Пакета розширення за 2023–2025 роки (Ukraine Report) прямо вказується на необхідність посилення інституційної спроможності наглядового органу. Єврокомісія послідовно наголошує, що чинна модель не забезпечує достатнього рівня незалежності та ресурсного забезпечення, а у звіті за 2025 р. окремо акцентовано на потребі приведення законодавства у повну відповідність до європейських стандартів [13, с. 32; 14, с. 28; 15].

4. Термінологічна та концептуальна несумісність. Базовий Закон України «Про захист персональних даних» (2010) побудований на застарілій Директиві 95/46/ЄС. В. М. Брижко у своїх дослідженнях вказував на наявність суттєвих розбіжностей між українським законодавством та європейськими стандартами ще на етапі становлення системи захисту даних [12, с. 8].

Ключова проблема стосується інституту «згоди суб'єкта», яку українське право розглядає як основну підставу обробки даних, тоді як GDPR надає пріоритет «законному інтересу» контролера. Крім того, відсутнє чітке розмежування між поняттями «контролер» та «оператор», що ускладнює розподіл відповідальності [6, с. 110].

5. Система юридичної відповідальності: адміністративні, кримінальні та цивільно-правові санкції є диспропорційними та не забезпечують належного превентивного ефекту. Т. О. Гуржій слушно зауважує, що чинна система відповідальності в Україні є неефективною [6, с. 166–167].

6. Колізія правових режимів: «публічність» vs «приватність». На практиці згаданий пошук балансу виливається у гострий конфлікт між вимогами антикорупційної прозорості та стандартами захисту персональних даних (GDPR compliance). В. Г. Пилипчук наголошує, що в умовах інформаційного суспільства надмірна відкритість систем суттєво загострює ризики для приватності особи [2, с. 108].

Поки національне законодавство України про запобігання корупції та доступ до публічної інформації вимагає безумовної відкритості реєстрів (зокрема, щодо даних бенефіціарів), Суд справедливості ЄС ухвалив прецедентне рішення у об'єднаних справах C-37/20 та C-601/20 (WM and Sovim SA v Luxembourg Business Registers, 2022) [16]. Суд визнав, що необмежений публічний доступ до інформації про бенефіціарних власників є непропорційним втручанням у фундаментальні права людини.

Мова йде не про повне закриття даних, а про перехід від безумовної публічності до моделі доступу на основі легітимного інтересу (legitimate interest), як це практикується в ряді країн ЄС після рішення Суду. Така розбіжність підходів ставить суб'єктів цифрової економіки, орієнтованих на внутрішній ринок ЄС, у ситуацію правової невизначеності: виконання імперативних внутрішньодержавних вимог щодо розкриття інформації створює прямий ризик порушення регламенту GDPR. У підсумку, цей дисбаланс стає системною перешкодою для інтеграції України до Єдиного цифрового ринку ЄС, створюючи додаткові бар'єри для транскордонного обміну даними та знижуючи конкурентоспроможність вітчизняного бізнесу [3, с. 67].

7. Технологічні бар'єри. Локалізація даних та хмарні сервіси: в умовах війни Україна змушена була швидко легалізувати використання хмарних сервісів (Закон «Про хмарні послуги», 2022). Однак сучасні регламенти ЄС (Data Act, Data Governance Act) стимулюють вільний рух даних, тоді як українська система КСЗІ (комплексна система захисту інформації) часто вимагає фізичного контролю над інфраструктурою. Архаїчні вимоги до побудови КСЗІ, що базуються на

парадигмі фізичного захисту периметра, вступають у протиріччя з віртуалізованою природою хмарних сервісів. Це створює ситуацію, яку В. П. Кононенко, С. С. Здоровко та А. Є. Корольова описують як проблему забезпечення стану інформаційної безпеки без втрати функціональності систем [17, с. 248], та обмежує доступ до захищених європейських хмарних середовищ.

Цей процес ускладнюється феноменом, який Ф. Бланкато визначає як «зв'язок хмарного суверенітету» (cloud sovereignty nexus). Політика ЄС спрямована на зменшення залежності від неєвропейських провайдерів (насамперед США та Китаю) шляхом створення суверенних хмарних федерацій, таких як Gaia-X [18, с. 3]. Для України це означає, що доступ до європейських хмар вимагатиме не лише юридичної сумісності, а й відповідності жорстким критеріям імунітету від екстериторіального доступу третіх країн.

Узагальнюючи аналіз інституційних, доктринальних та технологічних перешкод, слід констатувати, що фрагментарна адаптація окремих норм права ЄС вже вичерпала свій ресурс. Структурна реформа національного законодавства є системною передумовою повноцінної інтеграції України до Єдиного цифрового ринку та участь у Європейських просторах даних. Ця реформа має вийти за межі декларацій і вирішити фундаментальні протиріччя між застарілою пострадянською моделлю захисту інформації та динамічним підходом acquis communautaire.

Висновки. На основі проведеного дослідження сформульовано авторські пропозиції щодо гармонізації термінологічного апарату та реформи системи юридичної відповідальності, які є необхідними для забезпечення повноцінної інтеграції України до цифрового простору ЄС:

1. **Реформа термінологічного апарату.** Необхідно внесення змін до Закону України «Про захист персональних даних» щодо відмови від концепції «згоди суб'єкта» як універсальної підстави для обробки даних. Пропонується імплементувати європейську конструкцію «легітимного інтересу» (legitimate interest) контролера, що дозволить розблокувати розвиток ринку Великих даних (Big Data) та Інтернету речей (IoT). Також слід законодавчо закріпити чітке розмежування статусів та зон відповідальності «контролера» (data controller) та «оператора» (data processor) відповідно до дефініцій GDPR, усунувши наявну правову невизначеність.

2. **Трансформація інституту відповідальності.** Чинна система адміністративних штрафів в Україні не виконує превентивної функції через їх незначний розмір. Пропонується реформувати систему юридичної відповідальності шляхом запровадження механізму «стримуючих санкцій» (dissuasive penalties), аналогічних тим, що передбачені ст. 83 GDPR (штрафи, прив'язані до річного обігу компанії). Це створить економічну мотивацію для бізнесу інвестувати у захист даних, а не лише формально виконувати вимоги закону.

3. **Інституційне розмежування.** Для забезпечення критерію «повної незалежності» (complete independence) за ст. 52 GDPR, необхідно виокремити функцію нагляду за захистом даних з мандату Уповноваженого Верховної Ради з прав людини. Пропонується створення окремого незалежного регулятора (за моделлю європейських органів із захисту даних (Data Protection Authorities)), який матиме повноваження не лише моніторингу, а й накладення санкцій та проведення технічних аудитів.

4. **Баланс прозорості та приватності.** Враховуючи практику Суду ЄС (справа WM and Sovim SA), необхідно переглянути законодавство про доступ до публічних реєстрів. Пропонується замінити принцип «абсолютної відкритості» персональних даних бенефіціарів на принцип «доступу на основі підтвердженого інтересу». Це дозволить зберегти інструменти громадського контролю та журналістських розслідувань, водночас захистивши фундаментальне право на приватність законослухняних громадян в умовах цифрової економіки.

Список використаних джерел:

1. Барабаш О. О., Яцків Д. В. Інформаційні права як складова четвертого покоління прав людини. *Часопис Київського університету права*. 2021. № 1. С. 27–31. DOI: https://doi.org/10.36695/2219-5521.1.2021.03

2. Пилипчук В. Г. Актуальні проблеми становлення і розвитку правової науки в інформаційній сфері. *Інформація і право*. 2012. № 1(4). С. 15–21.

3. Пилипчук В. Г., Брижко В. М. Інформаційна безпека та приватність у сфері захисту персональних даних. *Інформація і право*. 2016. № 4(19). С. 60–70.

4. Капітаненко Н. П. Стандарти обмеження інформаційних прав: міжнародний та національний вимір. *Ірпінський юридичний часопис*. 2025. Вип. 1 (18). С. 52–61. DOI: https://doi.org/10.33244/2617-4154.1(18).2025.52-66

5. Захарчук І. В. Міжнародне право в умовах цифровізації: становлення четвертого покоління прав людини. *Науковий вісник Ужгородського національного університету. Серія Право*. 2025. Вип. 5, ч. 3. С. 353–358. DOI: https://doi.org/10.24144/2788-6018.2025.05.3.52

6. Гуржій Т. О., Петрицький А. Л. Правовий захист персональних даних: монографія. Київ: КНТЕУ, 2019. 256 с.

7. Дугінець Г. В., Генералов О. В., Ніжейко К. А. Цифрова трансформація європейського енергетичного сектору: виклики сталого розвитку під час геополітичних криз. *Економіка та суспільство*. 2025. № 76. DOI: https://doi.org/10.32782/2524-0072/2025-76-108

8. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). *Official Journal of the European Union*. 03.06.2022. Vol. L 152. P. 1–44. URL: http://data.europa.eu/eli/reg/2022/868/oj.

9. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act). *Official Journal of the European Union*. 22.12.2023. Vol. L. URL: http://data.europa.eu/eli/reg/2023/2854/oj.

10. Heidebrecht S. From Market Liberalism to Public Intervention: Digital Sovereignty and Changing European Union Digital Single Market Governance. *Journal of Common Market Studies*. 2024. Vol. 62, No. 1. P. 205–223. DOI: https://doi.org/10.1111/jcms.13488

11. Бондаренко О. С., Малетов Д. В. Гармонізація ІТ-права України з правом ЄС. *Південноукраїнський правничий часопис*. 2022. № 4. С. 9–16. DOI: https://doi.org/10.32850/sulj.2022.4.1.2

12. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних / В. М. Брижко та ін. Київ: Тріумф, 2006. 256 с.

13. Ukraine Report 2023. Commission Staff Working Document. European Commission. Brussels, 08.11.2023. SWD(2023) 699 final. URL: https://neighbourhood-enlargement.ec.europa.eu/ukraine-report-2023_en (дата звернення: 12.02.2026).

14. Ukraine Report 2024. Commission Staff Working Document. European Commission. Brussels, 30.10.2024. SWD(2024) 300 final. URL: https://neighbourhood-enlargement.ec.europa.eu/ukraine-report-2024_en (дата звернення: 12.02.2026).

15. Ukraine Report 2025. Commission Staff Working Document. European Commission. Brussels, 04.11.2025. SWD(2025) 759 final. URL: https:// enlargement.ec.europa.eu/ukraine-report-2025_en (дата звернення: 15.02.2026).

16. Judgment of the Court (Grand Chamber) of 22 November 2022. WM and Sovim SA v Luxembourg Business Registers. Joined Cases C-37/20 and C-601/20. ECLI:EU:C:2022:912.

17. Кононенко В. П., Здоровко С. С., Корольова А. Є. Інформаційна безпека як стан. *Науковий вісник Ужгородського національного університету. Серія Право*. 2023. № 76, ч. 2. С. 244–250. DOI: https://doi.org/10.24144/2307-3322.2022.76.2.39

18. Blancato F. G. The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem. *Policy & Internet*. 2023. DOI: https://doi.org/10.1002/poi3.358

Дата першого надходження статті до видання: 08.01.2026
Дата прийняття статті до друку після рецензування: 27.01.2026
Дата публікації (оприлюднення) статті: 27.05.2026