

УДК 347:346.1:340

DOI <https://doi.org/10.51989/NUL.2026.2.7>

МОДЕРНІЗАЦІЯ ПРИВАТНО-ПРАВОВОГО РЕГУЛЮВАННЯ В УМОВАХ ВОЄННИХ ЗАГРОЗ ТА ЦИФРОВИХ РИЗИКІВ

Вінник Оксана Мар'янівна,

orcid.org/0000-0002-9397-5127

доктор юридичних наук, професор,
член-кореспондент Національної академії правових наук України,
головний науковий співробітник відділу приватноправових досліджень
Інституту правотворчості та науково-правових експертиз
Національної академії наук України



Стаття присвячена проблемі вдосконалення правового регулювання в умовах сучасних загроз (воєнних, екологічних, негативних наслідків прогалин в наукових дослідженнях щодо низки сучасних технологій) та цифрових ризиків на прикладі ЄС і України. Виявлено сучасні загрози благополуччю – як суспільному, так і приватному (збройні конфлікти, ризики цифровізації та використання новітніх технологій, критичний стан екології), що є результатом людської діяльності і потребують застосування адекватних правових засобів для їх (загроз) попередження та мінімізації пов'язаних з ними наслідків. Аналізується стан правового регулювання суспільних відносин, що зазнають впливу цих загроз, в ЄС та Україні, реакція ЄС на появу нових зловживань, пов'язаних з використанням новітніх технологій на ринках цифрової економіки, з метою уникнення закріплених в правових актах (DMA, DSA) обмежень/заборон, що зумовило прийняття Єврокомісією рішення про розробку та прийняття Акту про цифрову справедливість/Digital Fairness Act. З огляду на вплив сучасних викликів як на суспільне, так і на приватне життя членів суспільства правове забезпечення вирішення порушених проблем (зменшення їх негативних наслідків) передбачає комплексне регулювання сучасних суспільних відносин за допомогою як приватно-правових, так і публічно-правових механізмів. Зокрема це стосується врегулювання відносин міжнародного (на зразок закріпленого в Регламенті ЄС 2021/2085 від 19.11.2021) публічно-приватного партнерства, спроможного забезпечити об'єднання зусиль України та дружніх їй держав щодо зменшення сучасних ризиків та їх наслідків. Вдосконалення правового регулювання для вирішення порушених тут проблем в Україні варто здійснити на кількох рівнях: Конституції (закріплення положень про: роль держави щодо зменшення ризиків сучасних загроз; цифровий статус громадян); визначення специфіки суспільних відносин, що зазнали впливу цифровізації, в кодифікованому акті, яким може бути Цифровий закон/кодекс; врахування положень останнього при регулюванні певних видів відносин – приватних, господарських, екологічних тощо; закріплення в Цивільному кодексі/Кодексі приватного права положення про договір партнерства, а також про ризики, їх види, в тому числі неприйнятні як критерій заборони зловживання правом.

Ключові слова: загрози суспільному благополуччю, ризики цифровізації, вдосконалення правового регулювання, приватно-правові механізми, роль публічного права, зловживання правом, партнерство.

Vinnyk Oksana. Modernization of private law regulation in the context of military threats and digital risks

The article is devoted to the problem of improving legal regulation in the conditions of modern threats (military, environmental, negative consequences of gaps in scientific research on a number of modern technologies) and digital risks using the example of the EU and Ukraine. Modern threats to well-being, both public and private (armed conflicts, risks of digitalization and the use of new technologies, critical state of the environment), which are the result of human activity and require the application of adequate legal means to prevent them (threats) and minimize the consequences associated with them, have been identified. The state of legal regulation of public relations affected by these threats in the EU and Ukraine is analyzed, as well as the EU's response to the emergence of new abuses related to the use of new technologies in the digital economy markets, in order to avoid restrictions/prohibitions enshrined in legal acts

(DMA, DSA), which led to the European Commission's decision to develop and adopt the Digital Fairness Act. Given the impact of modern challenges on both the public and private lives of members of society, legal provision for resolving the problems raised (reducing their negative consequences) involves comprehensive regulation of modern public relations using both private and public law mechanisms. In particular, this concerns the regulation of international (such as that enshrined in EU Regulation 2021/2085 of 11/19/2021) public-private partnership relations, capable of ensuring the joining of efforts of Ukraine and friendly states to reduce modern risks and their consequences. Improving legal regulation to solve the problems raised here in Ukraine should be carried out at several levels: the Constitution (consolidation of provisions on: the role of the state in reducing the risks of modern threats; digital status of citizens); determining the specifics of public relations affected by digitalization in a codified act, which may be a Digital Law/Code; taking into account the provisions of the latter when regulating certain types of relations – private, economic, environmental, etc.; enshrining in the Civil Code/Code of Private Law provisions on a partnership agreement, as well as on risks, their types, including unacceptable ones as a criterion for prohibiting abuse of law.

Key words: threats to public well-being, risks of digitalization, improvement of legal regulation, private law mechanisms, role of public law, abuse of law, partnership.

Відомо, що ефективність правового регулювання залежить від ступеня врахування сучасного стану суспільних відносин. Зміни в останніх зумовлюють і необхідність адекватного на це реагування законодавця.

Наразі маємо стрімкий розвиток суспільних відносин, зумовлений поширенням новітніх технологій (цифрових та пов'язаних з їх застосуванням в різних сферах життя як приватного, так і суспільного, інших сучасних технологій). Незаперечно, що надбання цифровізації забезпечили можливість створення та запровадження технологій з грандіозним потенціалом, який, однак, може бути використаний з різною метою – доброю чи навпаки, що викликає занепокоєння в суспільстві [1] та необхідність вжиття адекватних превентивних заходів, включно з правовими¹.

Ірини Наумець в своїй статті наводить вислів фізика із фільму «Парк Юрського періоду»: «Науковці були настільки захоплені тим, що можуть зробити, що вони ні на хвилину не подумали, чи повинні вони це робити», підсумовуючи: «маємо багато відкриттів, але з якою метою ми їх використовуємо. Справа не у генетиці чи ядерній енергії, але в людській мотивації, з якою ціллю ми використовуємо наукові відкриття. Щоб правильно використовувати, треба мати правильні моральні дороговкази» [3]. Проте ефективність моральних чинників не завжди

висока і вимагає підкріплення відповідним правовим регулюванням, що встановлює межі для використання небезпечних (потенційно небезпечних) технологій, прикладом чого став Регламент ЄС про штучний інтелект/AI Act [4], що встановлює межі щодо технологій штучного інтелекту/ШІ, забороняючи їх використання, якщо ступінь ризику є неприйнятним.

Не менш проблемними є і біотехнології, в тому числі пов'язані з дослідженням смертельно-небезпечних вірусів: брак заходів безпеки при цьому загрожує пандеміями на зразок коронавірусної, наслідки яких для людства можуть бути катастрофічними. У зв'язку з цим постає проблема відповідальності науковців щодо розробки технологій, які потенційно є небезпечними [5], якщо ці (небезпечні) наслідки застосування технологій ігноруються, замовчуються чи недостатньо досліджуються, натомість акцент робиться лише на перевагах для суспільства.

Попри грандіозні можливості цифрових та інших сучасних технологій, використання яких забезпечує прогрес в різних сферах суспільного життя, але може застосовуватися і з недобросовісною метою² (зловживання монопольним ста-

¹ Тут і надалі наводяться результати дослідження, оприлюдненого в 2025 р. [2].

² Як свого часу зазначив досить відомий підприємець Джон Макафі, кримінал історично завжди був першим в застосуванні новітніх технологій на фоні відставання влади щодо запобігання недобросовісному їх використанню [6]. Це стосується не лише криміналу, а й підприємців, які використовують прогалини в чинному законодавстві щодо застосування новітніх технологій без урахування ступеня їх ризику для споживачів.

новищем з боку цифрових гігантів на цифрових та цифровізованих ринках з метою отримання надприбутків, кібератаки на урядові та бізнесові сайти, цифрове шахрайство, маніпулювання громадською думкою тощо), чому сприяє їх (технологій) малодослідженість з точки зору наслідків застосування, що, відповідно, зумовлює і брак ефективного правового забезпечення з метою запобігання шкідливих наслідків таких зловживань: все це викликає занепокоєння, що охоплює дедалі більшу кількість вчених [1].

Відповідно, постає проблема встановлення бар'єрів, включно з правовими, щодо використання подібних технологій. Попри реакцію українського законодавця на ймовірність негативних наслідків застосування певних видів сучасних технологій з відповідним встановленням вимог щодо їх використання [7; 8] (не обмежуючись лише сподіванням на етичні норми, про які зазвичай згадують дослідники [5; 9]), то стосовно інших новітніх потенційно небезпечних технологій правове регулювання запізнюється, хоча і з певними кроками щодо його вдосконалення з урахуванням досвіду ЄС шляхом затвердження цього року Національної програми адаптації законодавства України до права ЄС [10].

Сучасні технології зазвичай вдосконалюються з використанням штучного інтелекту (далі – ШІ), всі наслідки застосування якого невідомі навіть його розробникам³, що викликає занепокоєння і навіть засторогу щодо його застосування з огляду на небезпеку для людства [1]. Незаперечні переваги для України щодо використання надбань цифровізації, включно зі штучним інтелектом, в період розв'язаної російською державою війни, які допомагають вирішувати складні проблеми на фронті (впровадження повітряних й наземних безпілотні системи у бойові дії [12; 13] і в тилу [14; 15]). Разом з тим, ризики використання зазначених технологій можуть бути значно більшими, ніж переваги у їх засто-

суванні. ЄС відреагував на пов'язані із застосуванням ШІ проблеми, прийнявши Регламент 2024/1689 від 13.06.2024 р. (AI Act), який покликаний регулювати використання штучного інтелекту залежно від ступеня ризику (системи ШІ *неприйнятної ризику під заборону*, системи ШІ з *високим рівнем ризику* підлягають суворим вимогам, перш ніж їх можна буде вивести на ринок; менш небезпечні ШІ *обмеженого ризику* пов'язані з необхідністю прозорості щодо їх використання, натомість для застосування ШІ *мінімального або відсутнього ризику* обмеження не передбачені [4; 16]).

Україна реагує на пов'язані з використанням ШІ ризики, про що свідчать нормативно-правові акти [17], підписання Україною Рамкової конвенції про штучний інтелект та права людини [18], що визначає принципи, яких держава має дотримуватися у формуванні законодавства та застосуванні ШІ-продуктів у публічному секторі, аналітичні матеріали Міністерства цифрової трансформації щодо оптимального підходу до регулювання технологій штучного інтелекту в Україні [19], а також затвердження 1 квітня 2026 року Національної програми адаптації законодавства України до права Європейського Союзу [10] зі згадкою в ній про врахування положень AI Act.

Проблема використання цифрових технологій з точки зору їх впливу на суспільні відносини багатоаспектна. Одним з них (аспектів) є вплив надбань цифровізації на ринки цифрової економіки (далі – ЦЕ) з точки зору зміни умов конкуренції та необхідності посилення захисту прав споживачів.

Переваги застосування цифрових технологій цінні для тих учасників суспільних відносин, які добре на них знаються, володіють відповідними ресурсами та кваліфікованим кадрами, спроможними застосовувати ці технології для досягнення поставленої мети. Зазвичай це крупні корпорації, так звані цифрові гіганти, що нерідко створюють нові цифрові ринки і, відповідно, стають їхніми монополістами, використовуючи свій вплив на власну користь, що обертається проти тих учасників суспільних відносин (менш потужних підприємств

³ Одним із непередбачуваних результатів розвитку цифрових технологій стало відкриття, що «квантовий комп'ютер зламає криптовалюти раніше ніж очікувалося» [11], що становить загрозу для цього виду цінностей, використання яких стрімко поширюється.

і споживачів), які не володіють необхідним обсягом цифрових знань/компетенцій та ресурсів для безпечного спілкування в онлайн просторі цифрового/цифровізованого ринку. Занепокоєння ймовірними негативними наслідками для суспільства подібної поведінки зумовили активізацію наукових досліджень [20–23] та необхідність посилення правового регулювання пов'язаних з цим відносин в ЄС [24] на додаток до раніше прийнятих актів щодо цивілізованого (з урахуванням потреб громадянського суспільства і його членів) правового забезпечення сучасних інформаційних відносин на ринках цифрової економіки з відповідними механізмами захисту прав та правомірних інтересів учасників зазначених відносин, що не мають відповідних цифрових можливостей та компетенцій для реалізації/відстоювання своїх прав та інтересів у разі їх порушення цифровими гігантами-монополістами. Йдеться про регламенти, спрямовані на захист (1) економічної конкуренції – DMA [25] (має забезпечити запобігання зловживанням ринковою владою великими платформами (такими, як Apple, Google тощо) та (2) цифрових споживачів – DSA [26] (спрямований на створення безпечного цифрового простору з відповідними вимогами щодо прозорості реклами, захисту прав споживачів), а також AI Act [4], що має захистити суспільство та його членів від ризиків використання штучного інтелекту, які можуть мати навіть катастрофічні для людства наслідки [1].

Попри наявні в ЄС правові механізми захисту економічної конкуренції та споживачів в умовах ЦЕ [DMA, DSA], зловживання цифровими технологіями в цій сфері вдосконалюються, що і призвело до появи нових схем їх використання, не врахованих в раніше прийнятих актах. На підставі проведеного аналізу ринків ЦЕ та виявлення нових видів зловживань Єврокомісією прийнято рішення про розробку та прийняття нового акту, що має забезпечити цифрову справедливість [24]. Проте процес модернізації правового регулювання відносин цифровізації, включно з економічною сферою, досить складний і має бути постійним з огляду на вдосконалення застосування циф-

рових технологій як з добросовісною, так і сумнівною (або відверто злочинною) метою, в тому числі для отримання переваг за рахунок ігнорування інтересів слабо захищених в цифровому відношенні учасників суспільних відносин (споживачів, дрібних та середніх суб'єктів підприємництва).

Досвід ЄС щодо покращення правового забезпечення відносин цифровізації корисний і для України, оскільки цифрова економіка – транснаціональна, і, відповідно, проблеми захисту конкуренції та прав споживачів на її ринках притаманні і нашій країні, яка (з огляду на перспективу набуття членства в ЄС) має забезпечити євроінтеграційну складову вдосконалення правового регулювання відносин в цій сфері, включно з урахуванням положень DMA і DSA. Певні кроки у цьому напрямку вже здійснено (прийнято новий Закон «Про захист прав споживачів», набуття чинності яким відкладено до завершення війни [27], а в Проекті Цивільного кодексу України/Кодексі права приватного [28] визначається правовий статус споживача (ст. 29), закріплюється низка прав, спрямованих на захист прав цифрових споживачів/користувачів (право на цифрове вирізнення (ст. 322), право на інформацію (ст. 326) та інші правові механізми, що можуть використовуватися для захисту прав та правомірних інтересів споживачів в умовах цифрової економіки), проте потребують відповідного корегування положення Закону «Про захист економічної конкуренції» [29], а головне – *закріплення* (1) в Конституції України [30] (а) положень про роль держави щодо сучасних загроз та пов'язаних з ними ризиків, (б) цифрового статусу громадян України (цифрових прав та цифрових обов'язків), а також (2) визначення специфіки правового регулювання цифровізованих суспільних відносин в окремому кодифікованому акті, яким може бути Цифровий закон/кодекс, про що згадувалося кілька років тому [31].

Вкрай актуальною для України і останнім часом – для більшості країн світу є екологічні [32] (в першу чергу – пов'язана з результатами людської діяльності зміна клімату) та воєнні загрози [33], подолання / зменшення негативних наслідків

яких потребує колосальних ресурсів, що зазвичай одна країна не подужає і, відповідно, потребує міжнародної допомоги (про що свідчить ситуація в Україні, змушеній захищатися від російського агресора та долати пов'язані з цим наслідки, покладаючись не лише на власні зусилля/ресурси, який критично бракує, але й на дружню допомогу). Разом з тим, безоплатна допомога обтяжлива для країн-донорів, які за сучасного стану справ у світі мають дбати про посилення своєї національної безпеки, що потребує значних витрат. Виходом з цієї ситуації є міжнародне (за участі кількох дружніх держав) та бізнесу публічно-приватне партнерство (далі – ППП) на зразок передбаченого в ЄС [34]. Відповідно, така форма співпраці потребує правового закріплення в Законі України «Про публічно-приватне партнерство» [35] (можливість участі в ППП на боці публічних партнерів не лише України, а й дружніх їй держав за наявності між ними відповідних міжнародних угод). Приклад подібного (досить своєрідного, без визначення всіх його складових) партнерства є укладена минулого року між Україною і США так звана «угода про обмежене партнерство» [36; 37; 38] (проте без визначенні в законодавстві поняття такої угоди), а також запланована у формі партнерства співпраця нашої держави з дружніми країнами щодо використання отриманого Україною досвіду для посилення колективної безпеки [39].

Висновки:

Збільшення загроз суспільному благополуччю (поява нових, що зумовлено цифровізацією, та посилення традиційних (війни)) пов'язано з людським фактором: агресивна політика низки держав та їх лідерів; негативний вплив людської діяльності на довкілля, що викликало несприятливу для людства зміну клімату; винайдення та застосування новітніх технологій, негативні наслідки використання яких слабо досліджені (або взагалі проігноровані), що зумовлює значні ризики при їх використанні не лише для окремих категорій членів суспільства (споживачів, дрібних та середніх підприємців як учасників відносин на ринках цифрової економіки), а й для людства в цілому.

Сучасні виклики впливають як на суспільне, так і на приватне життя членів суспільства. Відповідно, правове забезпечення вирішення порушених тут проблем передбачає комплексне врегулювання сучасних суспільних відносин за допомогою як приватно-правових, так і публічно-правових механізмів.

Крім того, глобальність проблем зумовлює об'єднання зусиль міжнародної спільноти (принаймні миролюбної її частини, що дбає про загальне для людства благо) щодо вирішення згаданих проблем, що не зменшує ролі національного (на рівні певної країни) регулювання. Стосовно України ці проблеми потребують врегулювання на кількох рівнях: Конституції (про роль держави щодо сучасних загроз та пов'язаних з ними ризиків, цифрового статусу громадян); визначення специфіки суспільних відносин, що зазнали впливу цифровізації в кодифікованому акті, яким може бути Цифровий закон/кодекс; врахування положень останнього при регулюванні певних видів відносин – приватних, господарських, екологічних тощо; закріплення положень про міжнародне публічно-приватне партнерство, з використанням потенціалу якого можуть бути вирішені (або принаймні зменшені) згадані проблеми транснаціонального значення (колективної безпеки в широкому розумінні, що враховує не лише воєнні загрози, а й екологічні, пов'язані з ризиками цифровізації тощо) у відповідному законі [35]; закріплення в Цивільному кодексі [40] / Кодексі приватного права [28] положення про договір партнерства, а також про ризики, їх види, в тому числі неприйнятні як критерій заборони зловживання правом.

Глобальність та виключна важливість для людства (а не лише України) порушених тут проблем зумовлює доцільність осмислення на теоретичному рівні впливу згаданих проблем на правове регулювання, в тому числі визначення особливостей суспільних відносин, що зазнали цифровізації (суб'єктний та об'єктний склади, форми взаємодії, ризики та способи їх мінімізації, особливості відповідальності), та їх правового регулювання, що передбачає комплексне використання як приватно-правових та публічно-правових механізмів.

ЛІТЕРАТУРА:

1. Найкращі програмісти світу заговорили про кінець світу через ШІ – лишилося два роки. URL: <https://novosti-n.org/ua/analytic/Najkrashhi-programisty-svitu-zagovoryly-pro-kinez-svitu-cherez-II-lyshylosya-dva-roky-6045> (дата звернення: 15.02.2026).
2. Вінник О. Інтелектуальна власність в цифрову епоху: проблема безпеки використання новітніх технологій та її правове забезпечення. *Реформування права інтелектуальної власності в умовах рекодифікації цивільного законодавства України* : Збірник матеріалів Всеукраїнської науково-практичної конференції (м. Київ, 2 жовтня 2025 року). Одеса : видавництво «Юридика», 2025 р. С. 42–46 (184 с.).
3. Наумець І.. «Генетична модифікація може бути небезпечніша, ніж атомна зброя». URL: https://lb.ua/society/2018/03/03/391610_genetichna_modifikatsiya_mozhe_buti.html (дата звернення: 25.09.2025).
4. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689> (дата звернення: 06.04.2026).
5. Оксана Чурсінова. Небезпеки неконтрольованого розвитку біотехнологій: етичний аспект. *Вісник Львівського університету. Серія філос.-політолог. студії*. 2024. Вип. 52. С. 280–285. DOI <https://doi.org/10.30970/PPS.2024.52.35/>.
6. Макафи: использование криминалом анонимных криптовалют предвещает их широкое принятие. URL: <https://forklog.com/dzhon-makafi-ispolzovaniekriminalom-anonimnyh-kriptoalyut-predveshhaet-ih-shirokoe-prinyatie/> (дата звернення: 22.02.2020).
7. Про державну систему біобезпеки при створенні, випробуванні, транспортуванні та використанні генетично модифікованих організмів : Закон України від 31 травня 2007 року. URL: <https://zakon.rada.gov.ua/laws/show/1103-16#Text> (дата звернення: 06.09.2025).
8. Про державне регулювання генетично-інженерної діяльності та державний контроль за розміщенням на ринку генетично модифікованих організмів і продукції : Закон України від 23 серпня 2023 року. URL: <https://zakon.rada.gov.ua/laws/show/3339-20#Text> (дата звернення: 06.09.2025).
9. Біоетика: від теорії до практики. Київ : ВД «Авіцена», 2021. 144 с.
10. Про затвердження Національної програми адаптації законодавства України до права Європейського Союзу (acquis ЕС) : Постанова Кабінет Міністрів України від 01 квітня 2026 р. № 438. URL: <https://www.kmu.gov.ua/npas/pro-zatverdzhennia-natsionalnoi-prohramy-adaptatsii-zakonodavstva-ukrainy-do-prava-t10426> (дата звернення: 04.04.2026).
11. Квантовий комп'ютер зламає криптовалюти раніше ніж очікувалося. URL: https://internetua.com/kvantovii-komp-uater-zlamaye-kriptovaluati-ranishe-nij-ocsiku-valosya?utm_source=ukrnet_news (дата звернення: 17.04.2026).
12. Роботизація війська: як змінюється сучасна війна на суходолі. URL: <https://www.ukrinform.ua/rubric-ato/4112450-robotizacia-vijska-ak-zminuetsa-sucasna-vijna-na-suhodoli.html> (дата звернення: 17.04.2026).
13. Федоров анонсував запуск центру "А1": ШІ інтегрують у бойові системи. URL: <https://glavnoe.in.ua/news/fedorov-anonsuvav-zapusk-czentru-a1-shi-intehruyut-u-bojovi-systemy> (дата звернення: 18.04.2026).
14. ДТЕК Київські регіональні електромережі повністю оцифрував мережі Київщини. URL: <https://www.dtek-krem.com.ua/ua/news/dtek-kijivski-regionalni-elektromerezh-povnistyu-ocifruvav-merezhi-kijivshchini> (дата звернення: 18.04.2026).
15. Перша цифрова підстанція України: уряд Франції оцінив внесок ДТЕК в енергобезпеку. URL: <https://www.rbc.ua/rus/news/persha-tsifrova-pidstantsiya-ukrayini-uryad-1770653769.html> (дата звернення: 18.04.2026).
16. Забокрицький І. І. Акт про штучний інтелект (artificial intelligence act, ai act) як основа правового регулювання штучного інтелекту в ЄС: огляд основних положень. *Аналітично-порівняльне правознавство*. Том 3. 2025. с. 282-286. DOI <https://doi.org/10.24144/2788-6018.2025.03.3.44> .

17. Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025–2027 роках : Розпорядження Кабінету Міністрів України від 31.12.2024 р. № 1351-р. URL: <https://zakon.rada.gov.ua/laws/show/1351-2024-p#Text> (дата звернення: 14.02.2025).
18. Безпечний ШІ для мільйонів українців: Україна підписала Рамкову конвенцію про штучний інтелект та права людини. URL: <https://www.kmu.gov.ua/news/bezpechnyi-shi-dlia-milioniv-ukraintsiv-ukraina-pidpysala-ramkovu-konventsiiu-pro-shtuchnyi-intelekt-ta-prava-liudyny> (дата звернення: 08.09.2025).
19. Біла книга з регулювання ШІ в Україні: бачення Мінцифри. Липень 2024. 30 с. URL: <https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs/Регулювання%20ШІ.pdf> (дата звернення: 08.09.2025).
20. Li Gaoge. The Challenges and Responses of Consumer Rights Protection Law in the Digital Economy Era. *Frontiers in Economics and Management*. 2024. № 5 (11). P. 1–5. [https://doi.org/10.6981/FEM.202411_5\(11\).0001](https://doi.org/10.6981/FEM.202411_5(11).0001).
21. Christine RIEFA. Consumer protection and electronic commerce : protection against unsafe products bought online. Preface by Emmanuel MAUREL, European deputy. Bruxelles, Belgique. 2021. 172 p. URL: https://emmanuelmaurel.eu/wp-content/uploads/2021/04/Consumer_protection_and_electronic_commerce_Protectection_against.pdf (дата звернення: 16.01.2026).
22. Заставний В. С. Аналіз глобального ринку цифрових продуктів під впливом цифрової трансформації. *Академічні візії*. 2025. Вип. 40. DOI: <https://doi.org/10.5281/zenodo.14974849>
23. Вінник О. Цифрова економіка в ракурсі захисту прав споживачів та підтримання справедливої конкуренції в ринковому середовищі. *Збірник наукових праць «Приватне право і підприємництво»*. 2025. Вип. 25. С. 17–24. <https://doi.org/10.32849/2409-9201.2025.25.2>
24. Digital Fairness Act. URL: <https://www.digital-fairness-act.com/> (дата звернення: 20.02.2026).
25. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on competitive and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925> (дата звернення: 20.12.2025).
26. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act). URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng> (дата звернення: 18.01.2026).
27. Про захист прав споживачів : Закон України від 10.06.2023. URL: <https://zakon.rada.gov.ua/laws/show/3153-20/stru2#Stru> (дата звернення: 18.01.2026).
28. Проект Цивільного кодексу України (Кодексу права приватного). URL: <https://itd.rada.gov.ua/billinfo/Bills/Card/69528>; blob:<https://itd.rada.gov.ua/06196cf4-ab76-4aef-927b-4d567888f688> (дата звернення: 11.03.2026).
29. Про захист економічної конкуренції : Закон України від 11 січня 2001 року. URL: <https://zakon.rada.gov.ua/laws/show/2210-14#Text> (дата звернення: 20.02.2026).
30. Конституція України. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
31. В Україні з'являться медичний і цифровий кодекси (25 лютого 2020). URL: <https://ua.korrespondent.net/amp/4197351-v-ukraini-ziavliatsia-medychnyi-i-tsyfrovyi-kodeksy> (дата звернення: 19.04.2026).
32. Малишева Н. Р., Вінник О. М. Екологія, економіка, цифровізація: правові проблеми взаємодії. *Вісник НАПРН України*. 2022. № 2. С. 238–260. DOI: 10.31359/1993-0909-2022-29-2-238.
33. Нова війна в Ірані. Її траєкторія та вплив на Україну і Тихоокеанський регіон – Мік Раян. URL: https://ipress.ua/articles/nova_viyna_v_irani_yii_traiektoriya_ta_vplyv_na_ukrainu_i_tyhookeanskyu_region__mik_rayan_382778.html (дата звернення: 03.04.2026).
34. Council Regulation (EU) 2021/2085 of 19 November 2021 establishing the Joint Undertakings under Horizon European and repealing Regulations (EC) No 219/2007, (EU) No 557/2014, (EU) No 558/2014, (EU) No 559/2014, (EU) No 560/2014, (EU) No 561/2014

and (EU) No 642/2014 . ST/12156/2021/INIT. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02021R2085-20230921> (дата звернення: 01.04.2026).

35. Про публічно-приватне партнерство: Закон України від 19.06.2025. URL: <https://zakon.rada.gov.ua/laws/show/4510-20#Text> (дата звернення: 31.03.2026).

36. Угода між Урядом України та Урядом Сполучених Штатів Америки про створення Американсько-українського інвестиційного фонду відбудови. URL: https://zakon.rada.gov.ua/laws/show/840_001-25#Text (дата звернення: 03.03.2026).

37. «В угоді з США 26 разів згадується «угода про обмежене партнерство», але текст документа не оприлюднений», – Геращенко. URL: <https://politarena.ua/v-uhodi-z-ssha-26-raziv-zghaduietsia-uhoda-pro-obmezhenе-partnerstvo-ale-tekst-dokumenta-ne-opryliudnenyyu-URL: herashchenko-100646/> (дата звернення: 04.04.2026).

38. Угода про надра: ризики та можливості. URL: <https://niss.gov.ua/sites/default/files/2025-07/ugoda-pro-nadra-az.pdf> (дата звернення: 01.04.2026).

39. Партнерство на десятиліття: Україна та ЄС готують спільні проекти у сфері дронів, ППО та далекобійного озброєння (ВІДЕО). URL: <https://uatv.ua/uk/partnerstvo-na-desyatylittya-ukrayina-ta-yes-gotuyut-spilni-proyekty-u-sferi-droniv-ppo-ta-dalekobijnogo-ozbroyennya-video/> (дата звернення: 04.04.2026).

40. Цивільний кодекс України: Закон від 16.01.2003. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text> (дата звернення: 25.03.2026).



Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)

Дата першого надходження статті до видання: 20.04.2026

Дата прийняття статті до друку після рецензування: 15.05.2026

Дата публікації (оприлюднення) статті: 21.05.2026