

УДК / UDC: 340.5:004:351.746.1

DOI: [https://doi.org/10.37750/2616-6798.2026.1\(56\).357173](https://doi.org/10.37750/2616-6798.2026.1(56).357173)**Ігор Федорович Корж**Державна наукова установа “Інститут інформації, безпеки і права  
Національної академії правових наук України”

Київ, Україна

ORCID: <https://orcid.org/0000-0003-0446-5975>

## ЦИФРОВІЗАЦІЯ ТА ПРАВОВА БЕЗПЕКА В УКРАЇНІ

***Анотація.** В статті досліджено стан і результати здійснюваної в Україні цифровізації. Здійснюючи аналіз зазначених критеріїв, праці українських дослідників щодо зазначеної сфери, автором розкриваються результати процесу цифровізації за відповідними напрямками і сферами. Зазначається, що цифровізація кардинально позначилась на існуючих і виникаючих суспільних відносинах, розкривши широкі можливості та зручності для діяльності фізичних та юридичних осіб.*

*Зазначено, що поступальний розвиток цифровізації в Україні потребує постійного аналізування тенденцій інноваційних перетворень, вивчення напрямків зростання конкурентоспроможності нашої країни за рахунок прискореного підвищення рівня цифрових навичок громадян, розвитку цифрової економіки та цифрової держави.*

*Розкрито основні здобутки нашого суспільства в таких сферах суспільної діяльності, як : в державному управлінні, економіці, навчанні, науці тощо, а саме – інноваційність Дії, впровадження платформи “Трембіта”, Prozorro, DREAM, технологічні військові рішення та запуск GovTech-центру в Києві.*

*Акцентовано увагу на тому, що важливим кроком у здійсненні цифровізації в Україні стало створення національної LLM, яка являє собою нейромережу, що працює за принципом людського мозку і яка здатна розуміти, аналізувати, генерувати тексти, перекладати та писати код. Національна LLM буде навчена на українських даних, на нашій реальній історії та українських джерелах. Вона передбачатиме наукові роботи, дані з бібліотек та іншу інформацію, яку використовуватимемо для навчання цієї моделі.*

*Підкреслено, що надважлива роль в Україні відведена штучному інтелекту, за допомогою якого розвивається економіка, створюється різноманітна власна зброя, розвивається освіта і наука, здійснюється боротьба з ворогом тощо. Нині Україна має як готові ШІ-продукти, так й інструменти, що скоро запустяться. При цьому війна прискорила адаптацію та появу нових сервісів, що не були частиною початкового плану, але стали необхідними. Це військові облігації, чатбот єВорог, виплати єПідтримка, Міжнародний Реєстр збитків та інші проекти, пов'язані з потребами оборони, економіки й соціального захисту українців.*

*Водночас зазначений процес підштовхнув до виникнення ряду проблем правового характеру щодо його правового регулювання, утворивши відповідні прогалини, що створюють юридичну невизначеність, а й перешкоджають розвитку цифрової економіки, збільшивши ризики для бізнесу та громадян.*

*Здійснено концептуально-правовий аналіз взаємозв'язку цифровізації та правової безпеки держави (в частині правового регулювання цифровізації). Підкреслено, що між цифровізацією та правовою безпекою держави існує взаємно зумовлений, циклічний зв'язок, де кожен елемент є передумовою і наслідком кожного. Цифровізація виступає фактором трансформації правової безпеки і за умови, якщо цифровізація супроводжується належними правовими механізмами, то правова безпека постає умовою легітимної цифровізації, оскільки*

правова безпека забезпечує передбачуваність цифрової політики держави, сприяє захисту прав людини в цифровому середовищі, формуванню довіри до електронного врядування та державних цифрових сервісів.

Зазначено, що в українському контексті правова безпека покликана виконувати не лише захисну, а й коригувальну функцію, стримуючи абераційні викривлення права внаслідок алгоритмізації владних рішень та забезпечуючи збереження людиноцентричної природи публічної влади.

Наведене в дослідженні визначення “цифрової правової безпеки” принципово поєднує його стан і функцію, фіксує зв'язок між цифровими технологіями та якістю права, а також вводить правову аберацію, як системний ризик цифрової трансформації. Крім того, цифрова правова безпека може мати відповідне значення для української правової системи, оскільки вона має доктринальне значення, як новий напрям у теорії права. Також, вона має нормотворче значення, як критерій оцінки цифрових законопроектів, а також практичне значення, як інструмент контролю публічної влади в цифровому середовищі з боку громадянського суспільства.

**Ключові слова:** аберація; державне управління; дискреція; право; правова безпека; трансформація; цифрова правова безпека; цифровізація

**Ihor F. Korzh**

State Scientific Institution "Institute of Information, Security and Law  
of the National Academy of Legal Sciences of Ukraine"

Kyiv, Ukraine

ORCID: <https://orcid.org/0000-0003-0446-5975>

## DIGITALIZATION AND LEGAL SECURITY IN UKRAINE

**Summary.** *The article examines the state and results of digitalization in Ukraine. Analyzing the above criteria and the work of Ukrainian researchers in this area, the author reveals the results of the digitalization process in the relevant areas and spheres. It is noted that digitalization has had a fundamental impact on existing and emerging social relations, opening up wide opportunities and conveniences for the activities of individuals and legal entities.*

*It is noted that the progressive development of digitalization in Ukraine requires constant analysis of trends in innovative transformations, studying directions for increasing the competitiveness of our country through accelerated improvement of the level of digital skills of citizens, development of the digital economy and digital state.*

*The main achievements of our society in such areas of public activity as: public administration, economy, education, science, etc. are revealed, namely - the innovativeness of the Diia, the implementation of the Trembita platform, Prozorro, DREAM, technological military solutions and the launch of the GovTech center in Kyiv.*

*It is emphasized that an important step in implementing digitalization in Ukraine was the creation of a national LLM, which is a neural network that works on the principle of the human brain and is able to understand, analyze, generate texts, translate and write code. The national LLM will be trained on Ukrainian data, on our real history and Ukrainian sources. It will include scientific works, data from libraries and other information that we will use to train this model.*

*It was emphasized that an extremely important role in Ukraine is assigned to artificial intelligence, with the help of which the economy is developing, various domestic weapons are being created, education and science are developing, the fight against the enemy is being carried out, etc. Currently, Ukraine has both ready-made AI products and tools that will be launched soon. At the same time, the war accelerated the adaptation and emergence of new services that were not part of the original plan, but have become necessary. These are military bonds, the chatbot eVorog, payments ePidrymka, the International Register of Losses and other projects related to the needs of defense, economy and social protection of Ukrainians.*

*At the same time, this process has given rise to a number of legal problems regarding its legal regulation, creating relevant gaps that not only create legal uncertainty, but also hinder the development of the digital economy, increasing risks for businesses and citizens.*

*A conceptual and legal analysis of the relationship between digitalization and the legal security of the state (in terms of legal regulation of digitalization) has been carried out. It is emphasized that there is a mutually conditioned, cyclical relationship between digitalization and the legal security of the state, where each element is a prerequisite and consequence of each. Digitalization acts as a factor in the transformation of legal security and, provided that digitalization is accompanied by appropriate legal mechanisms, legal security becomes a condition for legitimate digitalization, since legal security ensures the predictability of the state's digital policy, contributes to the protection of human rights in the digital environment, and the formation of trust in e-government and state digital services.*

*It is noted that in the Ukrainian context, legal security is designed to perform not only a protective, but also a corrective function, restraining aberrant distortions of law as a result of the algorithmization of government decisions and ensuring the preservation of the human-centric nature of public authority.*

*The definition of "digital legal security" given in the study fundamentally combines its state and function, fixes the connection between digital technologies and the quality of law, and also introduces legal aberration as a systemic risk of digital transformation. In addition, digital legal security may have a corresponding significance for the Ukrainian legal system, since it has doctrinal significance as a new direction in legal theory. It also has a regulatory significance as a criterion for evaluating digital draft laws, as well as practical significance as a tool for controlling public authorities in the digital environment by civil society.*

**Keywords:** *aberration; public administration; discretion; law; legal security; transformation; digital legal security; digitalization*

**Постановка проблеми.** Як зазначається в наукових дослідженнях, пов'язаних із здійсненням цифровізації в Україні, результати цифровізації в Україні вражають зростанням охоплення послугами (онлайн-запис до лікарів, електронна черга в садочки, волоконно-оптичні мережі, 4G), підвищенням цифрової грамотності (навіть під час війни) та розвитком цифрових навичок, хоча й залишаються виклики, особливо у цифровій економіці та повноцінній трансформації громад. У 2025 році в Україні кількість людей, що користувалися електронними державними послугами, зросла до 59%, що на 4% більше, ніж у 2024 році. Половина з користувачів обирали сервіси у "Дії". Водночас кількість людей, що не користувалися жодними електронними послугами, зменшилася із 42% до 38%.

"Найчастіше українці користувалися сервісами в "Дії". Про це зазначили 48% тих, хто користувалися державними послугами, - на 6% більше, порівняно з 2024 роком. Серед інших популярних сервісів у 2025-му були платне отримання інформації з держреєстрів чи цифрових витягів (15%), послуги з пенсійних питань (15%), щодо особистого транспорту (13%), отримання субсидій (12%) та з питань податків (12%)", - повідомив виконавчий директор Київського міжнародного інституту соціології Антон Грушецький [1].

У фокусі Мінцифри України також покращення вже працюючих сервісів і запуск нових, серед яких, зокрема, розлучення онлайн, продовження цифровізації послуг для водіїв та бізнесу. Тим самим можна стверджувати, що прогрес цифрових технологій на сьогоднішній день виводить сферу інтернет-технологій на передові позиції за використанням інновацій, за яких основною функцією цифрових технологій залишається обмін інформацією. Зазначене потребує чіткого правового врегулювання, оскільки поряд із позитивними зрушеннями в тій, чи іншій сфері, є і негативні факти впливу цифровізації на суспільне життя. Крім того, для отримання позитивних результатів здійснюваної в Україні цифровізації є необхідність у дослідженні причинно-

наслідкових зв'язків між механізмами правового регулювання процесу цифровізації та настанням його результатів, оскільки завжди є небезпека виникнення правової аберації внаслідок порушення взаємозв'язку між метою впровадження цифровізації та метою правового регулювання процесу її здійснення. Тому дослідження направлене на розкриття ймовірних загроз і викликів, як факторів можливого настання негативних наслідків здійснюваної цифровізації – правових, соціальних, економічних, безпекових тощо.

**Результати аналізу наукових публікацій (досліджень).** Питанню здійснення цифровізації в Україні, як пріоритетній державній трансформації, яка спрямована на створення “держави у смартфоні” через платформу та застосунок Дія, що забезпечує онлайн-послуги, електронні документи та участь у держуправлінні, присвячено ряд публікацій, як наукового, так публіцистичного характеру, в яких проглядається першочергове завдання – сприяти зробити країну зручною для кожного громадянина. Так, різні аспекти здійснюваної в Україні цифровізації досліджували Н. Амеліна, Г. Андрощук, С. Бублик, С. Грищенко, І. Дашко, О. Довгань, І. Доронін, М. Дубняк, М. Жушман, О. Золотар, Ю. Ірха, Ж. Кононенко, І Корж, С. Коробка, О. Костенко, С. Красніков, І. Кучерак, Д. Ланде, А. Марущак, О. Мех, Ю. Огренич, В. Пилипчук, О. Радзієвська, М. Хаустова, В.Хвостенко, В.Фурашев, А. Череп, та інші.

Водночас, на нашу думку, потребує більшої наукової уваги питання правового регулювання цифрової трансформації у відповідних сферах життєдіяльності, що є важливим аспектом адаптації законодавства до нових реалій сучасного світу та суттєво впливає на всі сфери суспільного життя, включаючи економіку, бізнес, право та соціальні відносини. Воно вимагає створення нових правових норм, що відображають реалії цифрової діяльності та стосується важливих аспектів, які стають ключовими в умовах глобальної цифровізації суспільства в цілому. Саме даному аспекту, тобто проблемним питанням правового регулювання цифровізації в Україні, причинно-наслідковому зв'язку, як взаємозв'язку між правовими нормами (причинами) та викликаними ними юридичними наслідками (виникненням, зміною, припиненням правовідносин та юридичних фактів), що спрямований на досягнення певних цілей суспільного розвитку та встановлення правопорядку, забезпечення правової безпеки, і присвячена дана стаття.

**Метою статті** є аналіз стану запровадження в Україні цифровізації, як системного процесу впровадження сучасних технологій у відповідні сфери життєдіяльності; виділення проблемних питань, що виникли у процесі згаданої діяльності, насамперед правового характеру, охарактеризувати причину їх виникнення.

**Виклад основного матеріалу.** Як зазначають дослідники, еволюційні зміни, які відбулися в Україні за останні кілька десятиліть, свідчать про інформаційну революцію, наслідком якої є впровадження цифрових технологій, нових продуктів та послуг, інше усвідомлення цінностей. Однак поступальний розвиток цифровізації в Україні потребує постійного аналізування тенденцій інноваційних перетворень, вивчення напрямків зростання конкурентоспроможності нашої країни за рахунок прискореного підвищення рівня цифрових навичок громадян, розвитку цифрової економіки та цифрової держави [2].

### ***І. Результати цифровізації в Україні.***

Фахівці “Вокс Україна”, аналізуючи результати здійснення цифровізації в Україні за 2019-2024 роки, зазначають, що “Цифрова трансформація в Україні – системний процес, який охопив майже всі сфери державного управління. Інноваційність Дії,

впровадження платформи “Трембіта”, Prozorro, DREAM, технологічні військові рішення та запуск GovTech-центру в Києві – усе це засвідчує, що Україна рухається в напрямі сучасної цифрової держави” [3].

Зазначимо, що платформа “Трембіта” – це українська система електронної взаємодії та інтеперабельності державних реєстрів, що дозволяє безпечно обмінюватися даними між різними державними інформаційними ресурсами, на основі естонської технології X-ROAD, і є ключовим елементом цифрової інфраструктури України для надання електронних послуг. Вона забезпечує обмін даними між реєстрами в режимі “кожен з кожним”, не централізуючи їх, а лише фіксуючи факт обміну, що гарантує високий рівень безпеки завдяки шифруванню та криптографії [4].

У свою чергу Prozorro (Прозорро) – це електронна система публічних закупівель в Україні, що забезпечує прозоре проведення тендерів, де державні замовники купують товари, роботи та послуги, а бізнес змагається за найнижчою ціною. Система працює за принципом “всі бачать все”, об’єднуючи державні органи та постачальників на авторизованих майданчиках, що зменшує корупцію та забезпечує ефективність. В ній постачальники подають пропозиції через електронні майданчики (наприклад, SmartTender, e-tender.ua, Zakupki.Prom, UUB) [5].

Наступна система DREAM (Digital Restoration Ecosystem for Accountable Management) [6] являє собою державну цифрову екосистему, яка забезпечує прозоре та підзвітне управління всіма проектами відбудови та модернізації України. Система працює як “єдине вікно”, охоплюючи повний життєвий цикл проектів від ініціації до фінансування та завершення. Основні характеристики системи DREAM:

- **Прозорість і підзвітність:** Забезпечує доступ до відкритої аналітики, що запобігає корупції та підвищує довіру донорів;
- **Єдиний банк проектів:** Створює реєстр проектів відновлення, що реалізуються на національному, регіональному та місцевому рівнях;
- **Відповідність стандартам:** Базується на протоколах міжнародних фінансових організацій (МФО);
- **Інструменти:** Функціонал включає електронну демократію, систему ризик-менеджменту та модуль аналітики.

Розробка фінансується за підтримки уряду Великобританії. Система дозволяє громадам завантажувати проекти, а інвесторам – відслідковувати ефективність використання коштів.

Система GovTech-центру в Києві – технологічний хаб, який об’єднує уряд, бізнес, стартапи та науковців, щоб знаходити нові цифрові рішення та створювати спільні проекти з міжнародними партнерами та обмінюватися досвідом. Український GovTech-центр є частиною мережі C4IR Всесвітнього економічного форуму [7].

Центр працює за такими напрямками:

- GovTech Observatory – відстеження трендів GovTech, проведення досліджень та аналітика;
- Innovation Gateway – пошук партнерів для розвитку інновацій, таких як штучний інтелект, EdTech, Defense Tech, Semiconductors, BioTech, Green Tech, AUV;
- FutureGov Education – навчання цифрових лідерів сучасним технологіям. Центр партнеруватиме з CDTO Campus для створення простору, де лідери зможуть тестувати та впроваджувати цифрові рішення.

GGTC Kyiv працює за підтримки Програми EGAP, яку фінансує Фонд Східна Європа за кошти Швейцарії, та з ініціативи та сприяння Міністерства цифрової трансформації України. Програма “Електронне урядування задля підзвітності влади та

участі громади” (EGAP) виконується Фондом Східна Європа за підтримки Швейцарії у співпраці з Мінцифрою та Фондом Innovabridge протягом 2015-2028 років. Компонентами Програми є :

– Е-Послуги, тобто впровадження зручних, швидких та прозорих державних електронних послуг для громадян та бізнесу. Завдяки цьому українці отримують онлайн-доступ до якісних адміністративних сервісів, органи влади – оптимізовані процеси та економію часу, а суспільство – мінімізацію корупційних ризиків та ефективне підзвітне врядування. Компонент охоплює вдосконалення законодавства, оптимізацію бізнес-процесів, освітні проєкти з цифрової грамотності та безпеки в інтернеті, а також інформаційні кампанії задля популяризації онлайн-сервісів серед українців;

– Е-Демократія, тобто створення онлайн-інструментів, що покращують комунікації між владою та громадою і дозволяють українцям брати участь в управлінні державою. У межах компоненту були здійснені кроки щодо створення Концепції розвитку електронної демократії в Україні та план заходів щодо її реалізації [8]. А також розроблено першу національну платформу е-демократії e-DEM, на якій є Місцеві петиції, Громадський бюджет, Консультації з громадськістю, Шкільний громадський бюджет та Відкрита громада;

– Цифровізація регіонів, пропонування численних рішень для органів місцевого самоврядування, які сприяють якісній взаємодії влади та громади та зменшують цифровий розрив на регіональному рівні. На місцях здійснюється співпраця з державними обласними адміністраціями, органами місцевого самоврядування та громадськими організаціями. Покращується робота ЦНАП завдяки е-сервісам, автоматизації та систематичному навчанню співробітників. На конкурсних засадах було обрано 86 цільових громад у дев'яти пілотних регіонах. Створюються шаблонні проєкти і алгоритми для легкого масштабування їх у різних регіонах – цифрова стратегія громади, мобільні валізи, розумний кол-центр, електронні щоденники та журнали, центри активності громадян, чат-бот СВОЇ [9].

GGTC Kyiv та “Вокс Україна” разом створили “Радар реформ” – перший системний аналітичний огляд цифрової трансформації України у 2019–2024 роках. Мета – відстежити нормативно-правові зміни, зафіксувати прогрес в реалізації цифрових рішень у публічному секторі. Цей звіт створено як орієнтир для урядовців, дослідників, медіа, громадського сектору й міжнародних партнерів. Він дозволяє не лише оцінити прогрес, а й зрозуміти, де є прориви, а де – недоопрацювання.

Ще одним важливим кроком у здійсненні цифровізації в Україні, як заявляє вже колишній міністр Міністерства цифрової трансформації України М. Федоров [10], це створення національної LLM, яка дасть змогу вирішувати безліч питань. Вона являє собою нейромережу, що працює за принципом людського мозку. Вона здатна розуміти, аналізувати, генерувати тексти, перекладати чи навіть писати код. Тобто це не умовний ChatGPT, а технологія, на якій побудовані такі сервіси, як ChatGPT, AI-асистенти, чатботи, голосові помічники.

Завдяки LLM, можна буде запускати сервіси в державі, не зберігаючи даних за кордоном або в інших місцях, які є сумнівними або можуть бути враженими. Натомість зберігати дані можна буде на власній інфраструктурі, використовуючи власну LLM.

Крім того, можна буде працювати із сектором Defense Tech. Сьогодні збирається унікальна кількість даних з поля бою, яких немає у світі. І цю інформацію можна буде обробляти та генерувати певні рішення завдяки LLM, що важливо з точки зору безпеки держави.

Національна LLM буде навчена на українських даних, на нашій реальній історії та українських джерелах. Вона передбачатиме наукові роботи, дані з бібліотек та іншу інформацію, яку використовуватимемо для навчання цієї моделі. Також дані з державного сектору, але які не міститимуть сенситивної інформації. Також LLM зможуть використовувати різні організації, бізнеси для своїх цілей, для створення продуктів і сервісів. Першу версію української національної LLM заплановано запустити в бета-тестування навесні 2026 року. Модель буде навчена на унікальних даних і зможе конкурувати з іншими мовними моделями у відкритих рейтингах.

Надважлива роль в Україні відведена штучному інтелекту (ШІ, англ. - AI), за допомоги якого розвивається економіка, створюється різноманітна власна зброя, розвивається освіта і наука, здійснюється боротьба з ворогом тощо. У цьому напрямку поставлена амбітна ціль – до 2030 року потрапити в топ-3 країни світу за розробкою й інтеграцією ШІ в публічний сектор. Це державне управління, оборона тощо. І вже зараз закладається фундамент, який дасть змогу створювати інноваційні продукти на кшталт тих, які розробляє Mistral AI або OpenAI.

Як зазначає М. Федоров, для досягнення зазначеної мети був створений WINWIN AI Center of Excellence, який реалізує цілі України з розвитку AI в межах Стратегії цифрового розвитку інновацій України до 2030 року – WINWIN. Центр не лише допомагає розвивати AI всередині країни, а й робить Україну впливовим гравцем на глобальному ринку, упроваджує AI в усю державу.

Уже нині Україна має як готові ШІ-продукти, так й інструменти, що скоро запусяться. Один з найголовніших – AI-асистент на порталі Дія, який стане помічником в отриманні державних послуг і дасть старт новому етапу розвитку цифрової держави. У Міністерстві цифрової трансформації України також використовуються AI-інструменти для аналізу НПА та перекладу європейського законодавства, здійснюється інтеграція AI у Мрію, створюються внутрішні AI-інструменти в Міністерстві, інтегрується AI і у дефенс-тек.

Defence Tech – оборонні технології, сфера розробки та впровадження інноваційних технологічних рішень для військових потреб: дронів, РЕБ/РЕР, систем зв'язку та навігації. Вона спрямована на автоматизацію процесів на полі бою, швидке R&D (Research and Development – дослідження та розробка), створення модульних платформ та підвищення ефективності захисту. Окремо почали формувати національну AI-стратегію, яка має бути розроблена до кінця цього року. У свою чергу Мрія – державна освітня екосистема для учнів, батьків і вчителів, яка надихає вчитися та допомагає знайти себе в сучасному світі. Вона відкриває доступ до персоналізованого навчання, спрощує адміністрування освітнього процесу та підтримує дітей на шляху до самореалізації.

Зазначимо, що Україна швидко просунулась у розвитку цифровізації. Війна прискорила адаптацію та появу нових сервісів, що не були частиною початкового плану, але стали необхідними. Це військові облігації, чатбот «Ворог», виплати «Підтримка», Міжнародний Реєстр збитків та інші проекти, пов'язані з потребами оборони, економіки й соціального захисту українців. Водночас, зазначений процес підштовхнув до виникнення ряду проблем правового характеру щодо його правового регулювання, утворивши відповідні прогалини, що створюють юридичну невизначеність, а й перешкоджають розвитку цифрової економіки, збільшивши ризики для бізнесу та громадян, ускладнюючи інтеграцію України до цифрового простору Європейського Союзу (ЄС).

Доцільно виділити наступні проблемні питання :

- неповнота та фрагментарність регулюючого правового поля. Багато сфер цифровізації – електронне урядування, цифрові сервіси, блокчейн-технології, цифрові активи – ще не мають комплексного законодавчого врегулювання або мають лише часткові, розрізнені норми. Це створює правову невизначеність для бізнесу та громадян;
- відсутність єдиних визначень і стандартів. Українське законодавство не визначило чітко базових категорій цифровізації, таких як “цифрові активи”, “віртуальні цінності”, “штучний інтелект” тощо, що ускладнює адекватне правове регулювання;
- відсутність регулювання цифрових активів і криптовалют. Відсутність уніфікованих стандартів та правил створює ризики для інвесторів, регуляторів і користувачів, а також утруднює оподаткування та контроль за обігом таких активів;
- регулювання функціонування штучного інтелекту (ШІ) [11]. Відсутній рамковий закон про ШІ; для ШІ немає окремих правових режимів або правил щодо відповідальності, використання даних, етики та безпеки – що становить складність у забезпеченні захисту прав людини і запобіганні зловживань;
- кібербезпека. Законодавство щодо захисту інформаційних систем і кібербезпеки потребує оновлення з урахуванням сучасних викликів цифрової трансформації, а також узгодження з міжнародними стандартами і практиками;
- правове забезпечення інновацій і стартапів. В Україні існує недостатня координація та відсутність чітких процедур підтримки цифрових інновацій, що створює бар’єри для технологічного підприємництва;
- проблеми регулювання даних та приватності. Поряд з цифровізацією зростає значення правового захисту даних, але норма захисту персональних даних та правил їх обробки часто не встигає за темпами цифрової трансформації, особливо щодо великих даних (Big Data) та хмарних технологій;
- галузеві прогалини (наприклад, транспорт, публічні сервіси). У конкретних сферах цифровізації (автомобільна галузь, електронні сервіси з перетину кордону тощо) правові норми не завжди відповідають технічним реаліям або є недостатніми для ефективної інтеграції цифрових сервісів.

## ***II. Концептуально-правовий аналіз взаємозв’язку цифровізації та правової безпеки держави (правового регулювання цифровізації)***

Між цифровізацією та правовою безпекою держави існує взаємно зумовлений, циклічний зв’язок, де кожен елемент є передумовою і наслідком кожного [12]. Насамперед, ***цифровізація виступає фактором трансформації правової безпеки***. Насамперед вона змінює об’єкти правового захисту (дані, цифрову ідентичність, алгоритми, платформи), джерела загроз (кібератаки, маніпуляції даними, алгоритмічну дискримінацію) та суб’єктів впливу (приватні ІТ-корпорації, транснаціональні платформи). У цьому сенсі цифровізація підвищує вразливість правової системи, якщо вона не супроводжується належними правовими механізмами.

Якщо цифровізація супроводжується належними правовими механізмами, то правова безпека постає ***умовою легітимної цифровізації***, оскільки правова безпека забезпечує передбачуваність цифрової політики держави, сприяє захисту прав людини в цифровому середовищі, формуванню довіри до електронного урядування та державних цифрових сервісів. Без правової безпеки цифровізація втрачає свою легітимність і перетворюється на інструмент свавільного контролю, створює своєрідний ефект “технологічного насильства” над правом.

Таким чином “цифровізація” і “правова безпека” у співвідношенні між собою створюють своєрідну взаємозалежну форму “замкненого контуру”, яку як систему можна подати наступним чином:

***цифровізація → нові правові ризики → потреба в правовій безпеці → формування адаптивного права → безпечна цифровізація.***

Тобто права безпека структурує цифровий розвиток, а їхня взаємозалежність проявляється на наступних рівнях:

- нормативному, тобто мова йде про якість цифрового законодавства;
- інституційному, тобто мова йде про спроможність органів державної влади діяти належним чином в цифровому середовищі;
- ціннісному, тобто має надаватися пріоритет людиноцентризму;
- безпековому, має забезпечуватися стійкість правопорядку до цифрових загроз.

Таким чином, якщо сприймати “правову безпеку” як критерій функціонування публічної влади, то цифровізацію можна сприймати як каталізатор правової безпеки держави, але лише за умови, що сама права безпека виступає її системним обмежувачем і гарантом. Тому цілком є логічним, що цифровізація публічної влади перебуває у тісному взаємозв’язку з правовою безпекою держави, виступаючи водночас чинником її посилення та джерелом нових правових ризиків.

Запровадження цифрових технологій трансформує механізми здійснення владних повноважень, змінює характер правового регулювання та висуває підвищені вимоги до передбачуваності, прозорості й підконтрольності управлінських рішень. За відсутності належного рівня правової безпеки цифровізація може призвести до звуження процесуальних гарантій, підміни права алгоритмічними рішеннями та зростання технократичної дискреції публічної влади. Водночас ефективна права безпека забезпечує нормативне окреслення меж цифрового втручання, гарантує захист прав і свобод людини в цифровому середовищі та формує довіру до електронного врядування. Таким чином, цифровізація і права безпека перебувають у відносинах структурної взаємозалежності, де права безпека виступає системною умовою легітимної цифрової трансформації держави, а цифровізація – індикатором її реального стану та спроможності.

Якщо цифровізацію розглядати у філософсько-правовому вимірі, то вона постає не лише як технологічний процес, а й як форма раціоналізації публічної влади, що змінює сам спосіб її буття та здійснення. Вона трансформує право з нормативно-текстуальної системи у гібридну регулятивну реальність, у межах якої правові норми дедалі частіше інкорпорується в алгоритмічні процедури та цифрові інфраструктури.

Однак за умов недостатнього рівня правової безпеки така трансформація несе загрозу підміни права технічною доцільністю, редукції правосуб’єктності людини та втрати ціннісної автономії права як соціального регулятора. Водночас права безпека виконує функцію онтологічного та аксіологічного обмежувача цифровізації, утверджуючи пріоритет людської гідності, процедурної справедливості та відповідальності публічної влади. Саме у цій взаємодії права безпека постає не лише гарантією стабільності правопорядку, а й умовою збереження права як смислової та ціннісної основи державності в умовах цифрової трансформації.

Необхідно зазначити, що у контексті цифрової трансформації держави особливої актуальності набуває феномен правової аберації як викривлення змісту, функцій і ціннісних орієнтирів права під впливом позаправових, насамперед технологічних, чинників. Цифровізація публічної влади, будучи формою раціоналізації управління, здатна за відсутності належної правової безпеки спричинити абераційні процеси, у межах яких право поступово редукується до інструмента технічного забезпечення алгоритмічних рішень. У такій ситуації нормативна регуляція втрачає автономний

характер, а принципи справедливості, пропорційності та юридичної відповідальності підмінюються логікою ефективності й технічної доцільності.

Правова безпека в цьому вимірі постає як концептуальний механізм запобігання правовій аберації, оскільки саме вона забезпечує збереження ціннісно-сислової природи права, встановлює межі алгоритмізації владних процесів і утверджує людину як центральний елемент правового порядку. Таким чином, взаємодія цифровізації та правової безпеки набуває не лише інституційного, а й глибинного філософсько-правового значення, визначаючи, чи залишатиметься право носієм смислу й міри влади, чи перетвориться на технічну оболонку управління.

Якщо звернутися до української цифрової практики публічного управління, зокрема впровадження електронного врядування, державних реєстрів та платформи “Дія”, то вона наочно демонструє амбівалентний вплив цифровізації на стан правової безпеки держави. З одного боку, вона сприяє підвищенню доступності публічних послуг, прозорості управлінських процедур та зниженню корупційних ризиків, а з іншого – за умов фрагментарного нормативного регулювання й недостатньої процедурної визначеності створює передумови для виникнення правової аберації. Остання проявляється у схильності ототожнення технічної коректності цифрового рішення з його юридичною правомірністю, а також у зсуві акценту з правових гарантій особи на ефективність і швидкість адміністративних процесів.

В українському контексті правова безпека покликана виконувати не лише захисну, а й коригувальну функцію, стримуючи абераційні викривлення права внаслідок алгоритмізації владних рішень та забезпечуючи збереження людиноцентричної природи публічної влади. Саме в цьому вимірі цифровізація в Україні виступає не лише інструментом модернізації держави, а й своєрідним індикатором здатності правової системи протистояти трансформаціям, що загрожують її ціннісній і нормативній автономії.

З огляду на зазначене, можна навести ключові ціннісні ризики цифровізації в Україні крізь призму правової аберації. Ними можуть бути:

– редукція права до технічної процедури, тобто існує ризик ототожнення юридичної правомірності з коректністю роботи цифрового сервісу або алгоритму, внаслідок чого право втрачає свій ціннісно-нормативний зміст і перетворюється на допоміжний елемент технічної інфраструктури управління;

– зсув від людиноцентризму до системоцентризму. У цифрових практиках може простежуватися тенденція пріоритету зручності та ефективності системи над індивідуальними правами особи, що створює передумови для маргіналізації людської гідності як фундаментальної правової цінності;

– підміна юридичної відповідальності алгоритмічною нейтральністю, за якою автоматизовані рішення у сфері публічного управління можуть спричиняти розмивання персональної та інституційної відповідальності, коли негативні правові наслідки пояснюються “логікою системи”, а не волею та діями суб’єктів владних повноважень;

– ерозія процедурної справедливості, за якої прискорення та автоматизація адміністративних процесів створюють ризик звуження процесуальних гарантій, зокрема права на пояснення, оскарження та індивідуалізований розгляд справи, що є класичним проявом правової аберації;

– інструменталізація права в умовах безпекових викликів. Наприклад, в умовах воєнного стану та підвищених безпекових загроз цифрові технології можуть використовуватися як засіб надмірного контролю, що за відсутності чітких правових меж призводить до знецінення свободи як конституційної цінності.

Тим самим ціннісні ризики цифровізації в Україні свідчать про те, що правова аберація постає не як випадкове відхилення, а як системна загроза, що виникає на перетині технологічної раціональності та недостатньо інституціоналізованої правової безпеки.

Наведемо ключові гіпотетичні правові аберації цифровізації публічної влади в Україні.

1. **Аберація нормативної легітимності.** Вона може проявлятися при регулюванні суспільних відносин цифровими рішеннями без належної нормативної основи. Цифрова практика починає випереджати право, а згодом підміняти його, створюючи ілюзію правового регулювання там, де фактично діє управлінська або технічна доцільність. Тим самим, право втрачає властивість первинного регулятора і переходить у режим постфактум-легалізації.

2. **Аберація процедурності.** Вона може проявитися у редукції або “згортанні” класичних адміністративних процедур під впливом автоматизації (повідомлення замість рішення, статус замість акта, дія замість процедури). Цифрова форма витісняє юридичну логіку процесу. Тобто, процедура перестає бути гарантією, а перетворюється на технічний етап.

3. **Аберація суб’єктності.** Вона полягає у розмиванні юридичної відповідальності між суб’єктом владних повноважень, розробником цифрового рішення та самою системою. У результаті людина стикається не з носієм владної волі, а з “безособовим інтерфейсом”. Таким чином, влада втрачає персоніфікований характер, а відповідальність — чітку адресність.

4. **Аберація правового смислу.** Вона може виникнути тоді, коли технічна коректність цифрового результату ототожнюється з його правомірністю. Алгоритмічно “правильне” рішення сприймається як юридично бездоганне, навіть за наявності порушень принципів справедливості, пропорційності чи розумності. За таких дій право втрачає ціннісний вимір і редукується до функції.

5. **Аберація людиноцентризму.** Може проявитися у формі зсуву фокусу з прав і свобод людини на ефективність, швидкість та зручність сервісу. Людина розглядається не як носій гідності й прав, а як користувач цифрової послуги. Тим самим, відбувається трансформація правового статусу особи у статус “об’єкта цифрової обробки”.

6. **Аберація контролю.** Вона полягає в ускладненні або втраті ефективного юридичного контролю за цифровими рішеннями публічної влади. Традиційні механізми нагляду, оскарження й відповідальності не адаптовані до алгоритмічних форм управління. Право формально зберігається, але функціонально не спрацьовує.

Таким чином правові аберації цифровізації полягають не у збоях технологій, а у зміщенні смислового центру права – від міри влади до технічного інструмента управління. Саме тому правова безпека має розглядатися не як супровід цифровізації, а як антиабераційний механізм, що зберігає автономію, цінність і людиноцентричну природу права.

У зв’язку із зазначеним вище, цілком логічно постає питання: Чим викликана можлива фрагментарність нормативного регулювання цифровізації, тобто ефект нормативної асиметрії? Насамперед, зазначене пояснюється тим, що цифровізація в Україні розвивається швидше, ніж її правове забезпечення. Норми, що регулюють цифрові процеси, розпорошені між різними галузями права (адміністративне, інформаційне, фінансове, цивільне), не утворюючи цілісного регулятивного механізму. Це породжує нормативну асиметрію, за якої технологічні практики випереджають правові гарантії, а отже – знижують рівень правової безпеки як об’єктів, так і суб’єктів.

У філософсько-правовому сенсі йдеться про порушення принципу передбачуваності права як базового елементу правопорядку [11, С. 58].

Наступне, концептуальна невизначеність згаданих вище базових категорій цифрового права створює семантичну нестабільність права, що є різновидом правової аберації – зміщення змісту правових норм у процесі їх застосування. Тобто, право втрачає здатність адекватно “описувати” соціальну реальність, що трансформується технологіями.

Проблема алгоритмічної влади та юридичної відповідальності, яка виникла внаслідок того, що цифровізація публічного управління дедалі більше спирається на автоматизовані рішення (реєстри, скоринг – автоматизована система оцінки платоспроможності, надійності або поведінки клієнта (фізичної чи юридичної особи) за допомогою статистичних методів та аналізу даних, цифрові сервіси). Водночас не визначено правовий статус алгоритму як інструменту владного впливу:

- хто несе відповідальність за помилкове рішення;
- чи може алгоритм бути об’єктом правового контролю;
- де межа між технічним і владним рішенням. Це формує ризик трансформації демократичної влади у технократичну, позбавлену належного правового контролю.

Здійснюється “ерозія” прав людини, оскільки попри сервісну орієнтацію цифрових реформ, створюються системні загрози:

- зниження рівня захисту персональних даних;
- непрозорість обробки великих масивів інформації;
- обмеження доступу до прав у разі “цифрового виключення” окремих соціальних груп. У цьому контексті цифровізація може перетворитися з інструменту розширення прав у механізм їх фактичного звуження.

На сьогодні немає чіткого правового підходу щодо:

- визначення правової природи даних як об’єкта правового захисту;
- опрацювання співвідношення публічного інтересу та приватної власності на цифрові ресурси;
- чіткого визначення режиму відповідальності у сфері віртуальних активів. Це створює зону підвищеного ризику для економічної та правової безпеки держави.

Відсутність доктрини цифрової правової безпеки в Україні є значною проблемою, за якої цифровізація в Україні не осмислена як фактор правової безпеки, а розглядається переважно як техніко-адміністративний процес. Також відсутні:

- системна оцінка правових ризиків цифрових реформ;
- механізми превенції цифрових правопорушень;
- доктринальна модель “безпечної цифрової держави”. Зазначене безпосередньо корелюється з концепцією правової безпеки як критерію функціонування публічної влади.

Тим самим, проблеми правового регулювання цифровізації в Україні мають не лише нормативний, а й філософсько-правовий характер. Йдеться про трансформацію самої природи публічної влади, права та відповідальності в умовах цифрового суспільства. Без формування цілісної доктрини цифрової правової безпеки цифровізація ризикує стати джерелом нових форм правової аберації та зниження легітимності публічної влади.

Таким чином, концепція цифрової правової безпеки держави постає як самостійний філософсько-правовий феномен, що виникає на перетині:

- правової безпеки;
- цифровізації публічної влади;

- інформаційного та адміністративного права;
- доктрини прав людини в умовах технологічної трансформації.

На відміну від техніко-інформаційного підходу, цифрова правова безпека не зводиться до кібербезпеки, а охоплює здатність правової системи зберігати нормативну визначеність [12], легітимність і керованість влади в цифровому середовищі. Тому терміну **“цифрова правова безпека держави”** можна дати наступне визначення: **це стан і здатність правової системи забезпечувати стабільне, передбачуване та контрольоване громадянським суспільством функціонування публічної влади й реалізацію прав людини в умовах цифровізації, мінімізуючи ризики правової аберації, алгоритмічної влади та нормативної деградації.**

Зазначене визначення принципово поєднує його стан і функцію, фіксує зв'язок між цифровими технологіями та якістю права, а також вводить правову аберацію, як системний ризик цифрової трансформації.

В цифровій правовій безпеці держави можна виділити відповідні структурні елементи. Так, першим елементом можна зазначити **“нормативну безпеку”**, що передбачає концептуальну цілісність цифрового законодавства, єдність термінології та ієрархічну узгодженість правових норм. Водночас в зазначеному елементі можуть виникати такі ризики, як фрагментація правових норм, виникнення правової аберації та правової невизначеності.

Наступним елементом є **“інституційна безпека”**, що охоплює спроможність органів публічної влади діяти в цифровому середовищі правомірно; наявність механізмів демократичного контролю над цифровими рішеннями; інституційний баланс між технічними адміністраторами та суб'єктами владних повноважень. Ризиком може бути зміщення центру прийняття рішень від публічної влади до алгоритмів.

Такий елемент, як **“процедурна безпека”**, може гарантувати прозорість алгоритмічних процедур; право особи на пояснення автоматизованого рішення, а також можливість ефективного оскарження цифрових управлінських актів. Ризиком може стати формування **“неоскаржуваної”** цифрової влади.

Елемент **“правозахисна безпека”** спрямована на збереження реальності, а не декларативності прав людини; на недопущення цифрового виключення та на захист персональних даних і приватності. Ризиком може бути трансформація цифрових сервісів у механізм обмеження доступу до прав.

Елемент **“ціннісно-легітимаційної безпеки”** полягає : у збереженні довіри до права в цифрову епоху; в узгодженості цифрових реформ із принципами верховенства права; в запобіганні девальвації правових цінностей через технократичний дискурс. Ризиком може бути підміна права ефективністю.

Необхідно зазначити, що цифровізація виступає відповідним каталізатором правової аберації, оскільки змінює спосіб формування та застосування правових норм, одночасно знижуючи роль юридичної інтерпретації та посилюючи формалізм та автоматизм.

У свою чергу цифрова правова безпека є антиабераційним механізмом, який направлений на корегування цифрової практики через застосування права. Вона відновлює змістовний зв'язок між нормою, цінністю та справедливістю, одночасно стримуючи деградацію юридичної відповідальності.

Цифровій правовій безпеці притаманні відповідні функції. Ними є :

- превентивна, призначена для виявлення правових ризиків цифровізації;
- стабілізаційна, призначення якої полягає у збереженні правопорядку в умовах технологічних змін;

- гарантійна, що полягає забезпеченні реалізації прав людини;
- легітимаційна, призначена для підтримки довіри до публічної влади;
- корекційна, що полягає у подолання правових аберацій цифрового походження.

Цифрова правова безпека може мати відповідне значення для української правової системи, оскільки вона має доктринальне значення, як новий напрям у теорії права. Також, вона має нормотворче значення, як критерій оцінки цифрових законопроектів, а також практичне значення, як інструмент контролю публічної влади в цифровому середовищі з боку громадянського суспільства.

Тим самим цифрова правова безпека держави є не похідною від цифровізації, а умовою її легітимності. За відсутності такої безпеки цифрові трансформації призводять не до модернізації права, а до його аберації, що може підірвати засади демократичного врядування.

**Висновок.** Здійснювана цифровізація в Україні – це пріоритетний процес, що активно впроваджується через ініціативу “Держава у смартфоні” під керівництвом Мінцифри України, з ключовими досягненнями в “Дії” (державні послуги онлайн), запуском електронних сервісів для бізнесу, освіти та медицини, впровадженням ШІ, а також затвердженням стратегій розвитку цифрової економіки, спрямованих на інтеграцію в європейський простір, підвищення прозорості та ефективності держсектору. Зроблено вже чимало – цифровізація охоплює модернізацію державних інституцій, впроваджуються цифрові інструменти у фінанси, в податкову систему та митну справу, створюючи “безпаперовий” режим взаємодії та потужну цифрову екосистему, що має на меті економічне відновлення. Зазначене сприяє підвищенню ефективності, прозорості та підзвітності державного управління.

Водночас, існуючі та виникаючі проблеми правового регулювання цифровізації, наявні правові прогалини, виклики різного характеру, а також можливе виникнення правової аберації здійснення цифровізації, що полягає у зміщенні смислового центру права – від міри влади до технічного інструмента управління, потребує подальшого дослідження даного процесу, приділення належної уваги з боку управлінців та науковців. Саме тому правова безпека має розглядатися не як супровід цифровізації, а як антиабераційний механізм, що зберігає автономію, цінність і людиноцентричну природу права.

**ПОДЯКИ:** Немає

**КОНФЛІКТ ІНТЕРЕСІВ:** Немає

### Список використаної літератури

1. УКРІНФОРМ. URL: <https://www.ukrinform.ua/rubric-society/4083601-vze-59-ukrainciv-koristuutsa-cifrovimi-derzavnimi-poslugami-najcastise-u-dii.html> (дата звернення: 27.01.2026).
1. Галушак О., Галушак М., Машлій Г. Цифровізація : еволюційні перетворення. *Галицький економічний вісник*. 2023. № 2 (81). С.155-164.
2. Державна цифрова трансформація: аналіз за 2019-2024 роки. URL: <https://voxukraine.org/derzhavna-tsyfrova-transformatsiya-analiz-za-2019-2024-roky> (дата звернення: 27.01.2026).
3. Система «Трембіта». Архітектура системи інтегрованості. URL: <https://egov.dp.gov.ua/services/sistema-trembita> (дата звернення: 27.01.2026).
4. Держзакупівлі. Онлайн. URL: [https://news.dzo.com.ua/pro-kompaniyu/?\\_gl=1\\*1tkjv8\\*\\_gcl\\_aw\\*R0NMLjE3Njk2OTIyNTcuRUFJYUIRb2JDae1JakpfSS0taXdrZ](https://news.dzo.com.ua/pro-kompaniyu/?_gl=1*1tkjv8*_gcl_aw*R0NMLjE3Njk2OTIyNTcuRUFJYUIRb2JDae1JakpfSS0taXdrZ)

01Wcm15UkJSMU5LQ0RIRUFBUFTQUFFZ0lkanZEX0J3RQ..\*\_gcl\_au\*MTQzNDM4ODQ5MS4xNzY5NjkyMTUy\*\_ga\*MTY3Nzc3MzQ3MS4xNzY5NjkyMTUy\*\_ga\_P9Q3FG735B\*czE3Njk2OTIxNTIkbzEkZzEkdDE3Njk2OTIyODUkajMxJGwwJGgw (дата звернення: 27.01.2026).

5. DREAM – система управління публічними інвестиціями. URL: [https://www.facebook.com/DREAMUkraineDigital/?locale=uk\\_UA](https://www.facebook.com/DREAMUkraineDigital/?locale=uk_UA) (дата звернення: 27.01.2026).

6. У Києві відкрили другий у світі Global Government Technology Centre. URL: <https://www.kmu.gov.ua/news/u-kyievi-vidkryly-druhyi-u-sviti-global-government-technology-centre> (дата звернення: 27.01.2026).

7. Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації : Розпорядження Кабінету Міністрів України від 08 листопада 2017 р. № 797-р. URL: <https://www.kmu.gov.ua/nras/250417925> (дата звернення: 27.01.2026).

8. Про EGAP. URL: <https://egap.in.ua/about> (дата звернення: 27.01.2026).

9. Навіщо Україні власна LLM? URL: <https://digitalstate.gov.ua/uk/news/govtech/navishcho-ukrayini-vlasna-llm> (дата звернення: 27.01.2026).

10. Баранов О.А. Особливості визначення правового статусу робота із штучним інтелектом. Інформація і право. 2023. № 4(47). С.40-54. URL: <file:///C:/Users/Admin/Downloads/291581-Текст%20статті-673646-1-10-20231126%20> (дата звернення: 20.08.2025).

11. Корж І. Ф. Правова безпека як критерій стану правового життя: монографія. Київ: Видавництво Політія, 2024. 408 с.

12. Андрусів У.Б., Федик С.Є. Елементи принципу юридичної визначеності. *Часопис Київського університету права*. 2019. № 1. С. 19-25.

### **Ігор Федорович Корж**

доктор юридичних наук, старший науковий співробітник  
заступник керівника наукового центру цифрової трансформації і права Державної наукової установи “Інститут інформації, безпеки і права Національної академії правових наук України”

04053, Україна, м. Київ, пров. Несторівський, 4

*email: garry52@ukr.net*

### **Ihor F. Korzh**

Doctor of Law, Senior Research Fellow

Deputy Head of the Scientific Center for Digital Transformation and Law

State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"

4 Nestorivskyi Lane, Kyiv, 04053, Ukraine

*email: garry52@ukr.net*

**Рекомендоване цитування:** Корж І.Ф. Цифровізація та правова безпека в Україні. *Інформація і право*. № 1(56)/2026. 2026. С. 27-41. [https://doi.org/10.37750/2616-6798.2026.1\(56\).357173](https://doi.org/10.37750/2616-6798.2026.1(56).357173)

**Suggested Citation:** Korzh I.F. (2026) Digitalization and Legal Security in Ukraine. *Information and Law*. 1(56)/2026. 27-41. [https://doi.org/10.37750/2616-6798.2026.1\(56\).357173](https://doi.org/10.37750/2616-6798.2026.1(56).357173)

Дата надходження статті до редакції: 01.02.2026 р.

Дата прийняття статті до друку після рецензування: 23.02.2026 р.

Дата публікації (оприлюднення): 01.04.2026 р.