УДК: 340.12

https://doi.org/10.52058/3041-1254-2025-12(22)-235-255

Квик Вадим Володимирович аспірант кафедри прав людини та юридичної методології Національного юридичного університету імені Ярослава Мудрого, https://orcid.org/0009-0000-7477-6977

ВЕРХОВЕНСТВО ПРАВА В ІНФОРМАЦІЙНУ ЕРУ: ВИКЛИКИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ДЛЯ НАЦІОНАЛЬНОЇ ПРАВОВОЇ СИСТЕМИ УКРАЇНИ

Анотація. У статті досліджуються виклики цифрової трансформації для верховенства права та національних правових систем в інформаційну еру із фокусом на українському досвіді. У нових умовах верховенство права виступає критерієм оцінки як діяльності держави, так і поведінки приватних суб'єктів, що набули системного значення у цифровому просторі. Спираючись на концепцію digital era governance, проаналізовано чотири блоки викликів: забезпечення законності у кіберпросторі та розширення повноважень органів безпеки; цифрову трансформацію судової влади й загрози нерівного доступу до правосуддя; регулювання захисту персональних даних і штучного інтелекту в контексті балансу між правами людини та публічною владою; вплив цифрових інструментів на виборчі процедури, політичну конкуренцію та публічну підзвітність. Національна правова система України аналізується в контексті одночасного просування євроінтеграційного курсу та дії правового режиму воєнного стану, що посилює напруження між вимогами безпеки й стандартами верховенства права. Розвиток цифрової інфраструктури правосуддя й адміністративних послуг створює можливість для підвищення правової культури й доступу до правової інформації. Дослідження гарантій прав людини в Україні на основі практики ЄСПЛ підкреслюють, що саме прозорість, публічність і доступність правової інформації є передумовами реального, а не декларативного верховенства права. Основу дослідження становить контент-аналіз міжнародних стандартів, актів ЄС, практики ЄСПЛ і профільних аналітичних звітів. Обґрунтовано, що цифровізація може слугувати ефективним чинником зміцнення верховенства права лише за умови інституційного посилення гарантій прав людини, прозорості діяльності органів влади та послідовної імплементації європейських стандартів у сфері кібербезпеки, е-правосуддя й захисту даних.

Ключові слова: верховенство права; національна правова система України; цифрова держава; інформаційна ера; кібербезпека; е-правосуддя; персональні дані; штучний інтелект.

Kvyk Vadym Volodymyrovych PhD student, Department of Human Rights and Legal Methodology Yaroslav the Wise National Law University, https://orcid.org/0009-0000-7477-6977

THE RULE OF LAW IN THE INFORMATION AGE: CHALLENGES OF DIGITAL TRANSFORMATION FOR THE NATIONAL LEGAL SYSTEM OF UKRAINE

Abstract. The article examines the challenges of digital transformation for the rule of law and national legal systems in the information age, with a focus on the Ukrainian experience. In the new environment, the rule of law serves as a criterion for assessing both the activities of the state and the behaviour of private entities that have acquired systemic significance in the digital space. Based on the concept of digital era governance, four sets of challenges are analysed: ensuring legality in cyberspace and expanding the powers of security agencies; digital transformation of the judiciary and threats of unequal access to justice; regulation of personal data protection and artificial intelligence in the context of the balance between human rights and public authority; the impact of digital tools on electoral procedures, political competition and public accountability. Ukraine's national legal system is analysed in the context of the simultaneous promotion of European integration and the legal regime of martial law, which exacerbates tensions between security requirements and the rule of law. The development of digital infrastructure for justice and administrative services creates opportunities to improve legal culture and access to legal information. Research on human rights guarantees in Ukraine based on the practice of the European Court of Human Rights emphasises that transparency, publicity and accessibility of legal information are prerequisites for real, rather than declarative, rule of law. The study is based on content analysis of international standards, EU acts, the practice of the European Court of Human Rights and relevant analytical reports. It is argued that digitalisation can serve as an effective factor in strengthening the rule of law only if human rights guarantees are institutionally strengthened, the activities of public authorities are transparent, and European standards in the field of cybersecurity, e-justice and data protection are consistently implemented.

Keywords: rule of law; national legal system of Ukraine; digital state; information age; cybersecurity; e-justice; personal data; artificial intelligence.

Постановка проблеми. Цифрова трансформація державного управління, правосуддя та безпекового сектору радикально змінює способи реалізації й захисту прав людини, а також механізми функціонування публічної влади. В умовах інформаційної ери класичні уявлення про верховенство права зіштовхуються з новими явищами – масовим збором і обробкою даних, алгоритмічним прийняттям рішень, кіберзагрозами, цифровими інструментами участі та конт-

ролю. Для національних правових систем це означає потребу не лише оновити нормативну базу, а й переосмислити інституційні гарантії прав людини, прозорості та підзвітності влади. Українська правова система переживає ці трансформації в особливому контексті: поєднання повномасштабної збройної агресії Російської Федерації, тривалої дії правового режиму воєнного стану та євроінтеграційних зобов'язань посилює напруження між вимогами національної безпеки і стандартами верховенства права. Водночас саме цифрові інструменти стають ключовим ресурсом забезпечення стійкості держави, функціонування правосуддя та взаємодії громадян з публічною владою. За таких умов постає науково й практично значуще питання: за яких інституційних і правових передумов цифровізація сприяє зміцненню верховенства права, а не легітимізує нові форми його послаблення?

Аналіз останніх досліджень і публікацій. Проблематика трансформації публічного управління в умовах цифровізації активно розробляється в зарубіжній науковій літературі. У межах концепції digital era governance дослідники аналізують, як поєднання цифрових технологій, мережевих платформ та аналітики даних змінює структуру державного управління, режими підзвітності та взаємодію держави з громадянами (D. Ravšelj, L. Umek, L. Todorovski, A. Aristovnik та ін.). Окремий напрямок становлять праці, присвячені європейському «цифровому конституціоналізму» та впливу таких актів, як Digital Services Act і Digital Markets Act, на баланс між економічною свободою, свободою вираження поглядів та регуляторними повноваженнями держави (A. Rauhvargers, N. Delgado, M. Tisne).

Значна кількість досліджень присвячена впливу цифрового ринку та регулюванню даних на верховенство права. У цьому контексті аналізуються наслідки дії Загального регламенту ЄС про захист даних (GDPR) для глобальних регуляторних режимів (Brussels effect) (A. Bradford), тлумачення ключових положень GDPR у доктрині (K. Kuner та ін.), а також зв'язок між обробкою даних, прозорістю алгоритмів і вимогами до якості закону та правової визначеності (All-Party Parliamentary Group on the Rule of Law, Data Processing and the Rule of Law). Окремий блок становлять дослідження та політичні документи, присвячені Європейському актові про штучний інтелект (EU AI Act), які оцінюють його значення для захисту прав людини та запобігання ризикам високоризикових AI-систем. У сфері кібербезпеки та протидії кіберзлочинності ґрунтовно досліджуються стандарти Будапештської конвенції про кіберзлочинність, проблеми гармонізації законодавства та виклики для національних правових систем (J. Clough; Cybercrime Programme Office of the Council of Europe). Аналізуються також особливості криміналізації несанкціонованого доступу до комп'ютерної інформації та проблеми правової визначеності відповідних норм (Computer Fraud and Abuse Act, судова практика у справі Van Buren v. United States; O. Kerr). У європейському вимірі важливими орієнтирами

є щорічні Доповіді Європейської Комісії про верховенство права та інструменти «rule-of-law toolbox», які спрямовані на моніторинг стану правосуддя, антикорупційної політики та медіаплюралізму.

Український вимір проблематики представлений, передусім, роботами, що аналізують правові засади цифрової трансформації державного управління та публічної влади (В. Луценко; К. Мануілова, Ю. Норчук), гармонізацію національного законодавства із європейським правом у сфері цифровізації судової влади (Д. Кривцун), а також використання цифрових технологій у функціонуванні судової системи в умовах воєнного стану (О. Яновська). Питання національної системи кібербезпеки, інституційного дизайну органів, відповідальних за кіберзахист, та викликів для демократичного контролю аналізуються в дослідженнях О. Давидюка, О. Поїя та у звітах Державної служби спеціального зв'язку та захисту інформації України, які фіксують динаміку кіберінцидентів і атак на критичну інфраструктуру.

Вагомий емпіричний контекст становлять аналітичні та моніторингові звіти міжнародних організацій: Індекс верховенства права World Justice Project, Індекс сприйняття корупції Transparency International, щорічні Звіти Європейської Комісії щодо прогресу України за розділом «Правосуддя та фундаментальні права», тіньові доповіді громадських організацій, а також висновки Венеційської комісії щодо українських реформ у сфері балансу гілок влади, боротьби з олігархічним впливом і захисту прав людини. Окремі дослідження присвячені впливу євроінтеграційного процесу та переговорів про вступ до ЄС на трансформацію інститутів верховенства права в Україні (Z. Darvas, M. Dabrowski, H. Grabbe та ін.).

Водночас, попри наявність розвиненої міжнародної та національної доктрини щодо цифровізації публічної влади, кібербезпеки, захисту даних і реформ правосуддя, комплексний аналіз того, як саме цифрова трансформація в українських умовах (повномасштабної війни, воєнного стану та євроінтеграції) впливає на реалізацію принципу верховенства права, залишається фрагментарним. Це й зумовлює потребу в даному дослідженні.

Методологічну основу статті становить поєднання формально-юридичного, порівняльно-правового, системного та структурно-функціонального методів. Формально-юридичний метод використано для аналізу нормативних актів ЄС та України у сфері кібербезпеки, захисту персональних даних, регулювання цифрових платформ і впровадження е-правосуддя. Порівняльно-правовий метод застосовано для зіставлення підходів ЄС, Ради Європи, США та України до врегулювання цифрових ризиків і забезпечення верховенства права. Системний і структурно-функціональний методи дозволили розглядати цифрову трансформацію як комплекс взаємопов'язаних змін у правовій системі, інституціях публічної влади та механізмах захисту прав людини. Додатково застосовано контент-аналіз міжнародних стандартів, актів ЄС, практики ЄСПЛ, аналітичних звітів та емпіричних даних щодо стану верховенства права й корупції в Україні.

Мета статті: висвітлити, яким чином цифрова трансформація впливає на реалізацію принципу верховенства права в Україні, виокремити ключові блоки викликів для національної правової системи в інформаційну еру та окреслити умови, за яких цифрові інструменти можуть посилювати, а не підривати гарантії прав людини й конституційний порядок.

Виклад основного матеріалу. ***Глобальні тенденції цифрової трансформації та виклики для верховенства права***. Інформаційна ера стала чинником докорінних трансформацій правових систем у світі. Згідно з бібліометричним дослідженням Ravšelj, Umek, Todorovski та Aristovnik (2022), яке охопило понад 9 тисяч наукових публікацій за два десятиліття, ці процеси послідовно аналізуються у межах концепції управління в цифрову епоху (Digital Era Governance, DEG). Сфера правового регулювання розширюється за рахунок нових об'єктів – цифрових технологій, глобальних платформ, штучного інтелекту, великих масивів даних та кіберпростору [1]. Водночас ця трансформація породжує якісно нові ризики для людини й суспільства. Як зазначає Європейська Комісія у своїй політичній рамці «Формування цифрового майбутнього Європи» (Shaping Europe's Digital Future, 2020), онлайн-платформи, що набули системного масштабу, фактично діють як приватні «воротарі» (gatekeepers) ринку та інформації, підриваючи справедливість, відкритість і сталість демократичних процесів [2]. У правовому значенні термін «gatekeepers» закріплений у Регламенті (ЄС) 2022/1925 «Про конкуренцію на цифрових ринках» (Digital Markets Act, DMA), де «воротарями» визнаються підприємства, які: - мають значний вплив на внутрішній ринок; - забезпечують ключову платформену послугу, яка є важливим шлюзом для бізнес-користувачів у доступі до кінцевих користувачів; - посідають укорінену та стійку позицію у своїй діяльності або, ймовірно, займуть таку позицію в недалекому майбутньому [3]. У цьому контексті актуалізується питання про межі допустимих змін, необхідних для того, щоб технологічний розвиток не призвів до підриву засадничих правових цінностей.

Відповіддю на цей виклик є принцип верховенства права, який зберігає статус фундаментальної засади у цифрову добу. Саме він забезпечує передбачуваність, доступність і справедливість права, що є основою довіри суспільства до правових інститутів. У нових умовах верховенство права виступає критерієм оцінки як діяльності держави, так і поведінки приватних суб'єктів, що набули системного значення у цифровому просторі. Воно вимагає належних процедурних гарантій, ефективного захисту прав людини та механізмів контролю над використанням цифрових технологій [4]. Особливого значення ці вимоги набувають в умовах алгоритмічного врядування та автоматизованого прийняття рішень. Як підкреслюється в Європейській етичній хартії щодо використання штучного інтелекту у судових системах (CEPEJ Ethical Charter, 2018), системи ШІ повинні застосовуватися «з належною повагою до принципів верховенства права та незалежності суддів» [5].

Перші відповіді на виклики цифрової доби формувалися у національних правових системах у вигляді точкових змін до законодавства. Так, у США ще ~~у~~ 1986 р. було ухвалено Закон США «Про комп'ютерне шахрайство та зловживання» (Computer Fraud and Abuse Act, CFAA), що криміналізував несанкціонований доступ до комп'ютерних систем. Цей акт став спробою забезпечити правову визначеність у новій сфері суспільних відносин, заклавши основу для захисту цифрової інфраструктури від посягань [6]. Водночас широта його формулювань, зокрема поняття «несанкціонований доступ», викликала гострі дискусії щодо відповідності принципам верховенства права. Як підкреслює О. Керр, нечіткість термінів «несанкціонований доступ» («without authorization») та «перевищує надані повноваження доступу» («exceeds authorized access») створювала простір для довільного тлумачення: навіть порушення корпоративних політик могло кваліфікуватися як злочин, що ставило під сумнів передбачуваність і пропорційність правового регулювання [7], а отже – підривало вимогу правової визначеності як складової верховенства права.

Питання тлумачення положень CFAA врешті-решт стало предметом розгляду Верховного Суду США у справі «Ван Бюрен проти Сполучених Штатів» (Van Buren v. United States, 2021). Суд вперше прямо висловився щодо меж застосування понять «without authorization» та «exceeds authorized access». У своєму рішенні він відкинув надмірно широке тлумачення, за яким будь-яке порушення внутрішньої політики роботодавця могло б вважатися злочином. Верховний Суд постановив, що CFAA не охоплює випадків, коли особа має законний доступ до інформаційної системи, але використовує дані не з тією метою, яка передбачена політикою чи контрактом. Таким чином, Суд звузив сферу дії закону, підтвердивши, що його положення мають тлумачитися з урахуванням принципу передбачуваності та пропорційності, які є складовими верховенства права [8]. Втім, національні відповіді, навіть за підтримки судової практики, виявилися недостатніми для комплексного реагування на виклики інформаційної доби. Це зумовило посилення ролі міжнародних та наднаціональних механізмів правового регулювання, серед яких особливе місце посідають ініціативи Ради Європи та Європейського Союзу. Саме вони виробили перші системні рамки цифрового права, які згодом стали орієнтирами для національних законодавств поза межами Європи.

Європейська модель цифрового регулювання і «цифровий конституціоналізм». Зокрема, Будапештська конвенція Ради Європи про кіберзлочинність (2001) становить перший багатосторонній обов'язковий договір, що комплексно врегульовує питання кіберзлочинності і вважається у сфері "наріжним каменем" міжнародного кіберправа (cornerstone of international cybercrime law) [9]. Її універсальний характер підтверджується звітом C-PROC Ради Європи, згідно з яким близько 79 % країн-членів ООН застосували конвенцію як модель під час удосконалення національного законодавства, а

понад 55 % прийняли аналогічні криміналізуючі норми [10]. Таким чином, саме в межах Будапештської конвенції вперше було закладено модель поєднання посилення кібербезпеки з процедурними гарантіями прав людини, що надалі стала орієнтиром для інших актів цифрового права.

Загальний регламент про захист даних (General Data Protection Regulation, GDPR, 2016) став одним із ключових нормативних актів цифрової доби, що визначив новий глобальний стандарт у сфері обробки та захисту персональних даних. Його ухвалення мало на меті уніфікувати правові норми в межах ЄС та адаптувати систему захисту приватності до викликів інформаційної ери. Регламент закріпив низку фундаментальних принципів, серед яких прозорість та підзвітність, «privacy by design» і «privacy by default», а також розширені права суб'єктів даних (право на забуття, право на портативність даних, право на ефективний засіб захисту) [11].

Особливе значення GDPR полягає в його екстериторіальній дії (ст. 3), що поширює юрисдикцію ЄС на будь-які компанії, які обробляють дані резидентів Союзу, навіть якщо вони розташовані поза його межами. Саме ця особливість зумовила явище, яке в науковій літературі отримало назву *Brussels Effect*: ЄС став «нормативною державою» (normative power), чиї стандарти де-факто поширюються на глобальному рівні [12]. Дослідницькі та інституційні оцінки загалом сходяться на тому, що GDPR досягнув своїх ключових завдань — посилив захист права на приватність і водночас забезпечив вільний обіг персональних даних у межах Союзу. Як зазначається у «Коментарі до GDPR» [13], практика Суду ЄС (Google v CNIL, Schrems II) підтвердила дієвість механізмів координації та узгодженості, закладених у Регламенті, що є запорукою його ефективного та уніфікованого застосування в усіх державах-членах. У результаті положення GDPR стали зразком для законодавців багатьох країн — від Бразилії та Японії до Індії та Південної Кореї, що підтверджує його статус «золотого стандарту» цифрового права.

GDPR став не лише нормативною інновацією у сфері захисту даних, а й прикладом того, як принцип верховенства права реалізується у цифрову добу. Його положення щодо прозорості, підзвітності та передбачуваності права забезпечують гарантії від свавільного застосування дискреції у сфері обробки даних. Як підкреслюється у дослідженнях та інституційних оцінках, включно з брифінгом Міжпарламентської групи з питань верховенства права (All-Party Parliamentary Group on the Rule of Law, 2019), механізми GDPR — зокрема оцінка впливу на захист даних (Data Protection Impact Assessment, DPIA) — спрямовані на забезпечення пропорційності та рівності перед законом у випадках автоматизованого прийняття рішень [14]. Отже, верховенство права поступово перетворюється на центральний критерій оцінки ефективності та легітимності цифрового регулювання.

Втім, розвиток цифрових технологій і посилення впливу великих онлайн-платформ поставили перед ЄС нові виклики, що виходили за межі сфери захисту

персональних даних. Якщо GDPR забезпечував фундамент приватності та довіри у цифровому середовищі, то наступним кроком стало врегулювання більш комплексних аспектів цифрової екосистеми — прозорості алгоритмів, конкуренції та захисту користувачів від зловживань з боку платформ-«воротарів». Таким чином, важливим етапом розвитку європейського права у сфері цифрового врядування стали Регламент (ЄС) 2022/2065 «Про єдиний ринок цифрових послуг» (Digital Services Act, DSA)[15] та Регламент (ЄС) 2022/1925 «Про конкуренцію на цифрових ринках» (Digital Markets Act, DMA)[3], ухвалені 2022 р. Ці акти були спрямовані на врегулювання діяльності великих онлайн-платформ, які виконують функції «воротарів» цифрового ринку та інформаційного простору. У них закріплено низку вимог, що безпосередньо втілюють принципи верховенства права: - передбачуваність і прозорість — зобов'язання платформ розкривати правила модерації контенту, рекламні механізми та алгоритмічні системи; - рівність перед законом — спеціальні обов'язки для платформ-«воротарів» (gatekeepers), що запобігають зловживанню ринковою владою; - підзвітність і контроль — створення механізмів нагляду з боку Європейської комісії та національних органів, ефективні санкційні інструменти.

У сучасній доктрині DSA та DMA розглядаються як ключові елементи формування європейського «цифрового конституціоналізму»: їх мета полягає не лише в оновленні правового режиму цифрових послуг і конкуренції, а й у запровадженні матеріальних та процесуальних гарантій, які обмежують владу великих онлайн-платформ і захищають фундаментальні права та демократичні цінності [16]. Вимоги щодо прозорості модерації контенту, підзвітності платформ і справедливих умов на ринку демонструють, як конституційні принципи — зокрема повага до прав людини та верховенства права — імплементуються через конкретні регуляторні механізми.

Подальший розвиток наднаціонального цифрового права в Європі демонструє прагнення поєднати інновації з верховенством права. Якщо GDPR став «золотим стандартом», то Регламент ЄС про штучний інтелект (AI Act, 2024) визнається першим у світі комплексним нормативним актом щодо ШІ [17]. Він встановлює ризик-орієнтовані правила від заборони соціального скорингу до суворих вимог для систем високого ризику; у такий спосіб він формує новий глобальний еталон регулювання ШІ [18]. AI Act закріплює низку гарантій, які безпосередньо відображають принципи верховенства права: - передбачуваність — чітка класифікація категорій ризику і вимог для розробників та користувачів; - пропорційність — обов'язкові оцінки впливу та механізми контролю для систем високого ризику; - підзвітність і контроль — створення незалежного наглядового органу (Європейське бюро з питань ШІ) і санкційного механізму, що запобігають свавільному застосуванню технологій[19]. Завдяки екстериторіальній дії, AI Act, подібно до GDPR, поширює свій вплив далеко за межі ЄС. Це не лише зміцнює позицію ЄС як «нормативної держави» (normative power), але й підтверджує, що

верховенство права стає центральним критерієм легітимності цифрового регулювання у глобальному масштабі[20]. Отже, досвід провідних правових систем засвідчує, що цифрова доба вимагає не лише розширення сфер правового регулювання, а й переосмислення фундаментальних засад — насамперед верховенства права, яке стає ключовим критерієм легітимності цифрових практик.

Цифрова трансформація та верховенство права в Україні: досягнення й контекст війни. Водночас у кожній державі ці процеси набувають специфічних рис, що визначаються інституційними традиціями, політичним контекстом і безпековими викликами. Україна в цьому сенсі є показовим прикладом: з одного боку, вона активно інтегрується в європейський правовий простір, адаптуючи національне законодавство до стандартів ЄС, зокрема Загального регламенту про захист даних (GDPR) та Будапештської конвенції про кіберзлочинність. Важливим кроком на цьому шляху став законопроєкт № 8153 «Про захист персональних даних» [21], ухвалений за основу у 2024 р., головною метою якого є гармонізація українського законодавства з вимогами GDPR та Конвенції 108+. Як зазначають експерти Ради Європи, положення законопроєкту загалом відповідають європейським стандартам, хоча окремі норми потребують уточнень і доопрацювання [22]. Тим самим українська модель захисту даних формально вбудовується в європейську нормативну архітектуру цифрового права, але її реальна ефективність залежить від інституційної спроможності забезпечити дотримання прийнятих стандартів.

З іншого боку, розвиток української правової системи відбувається в умовах повномасштабної війни, що висуває на перший план питання інформаційної безпеки, протидії кіберзагрозам і захисту персональних даних. За даними Державного центру кіберзахисту Держспецзв'язку, лише 2023 р. система виявлення вразливостей і реагування на кіберінциденти та кібератаки опрацювала понад 18 мільярдів подій інформаційної безпеки, зафіксувала 133 мільйони підозрілих подій та зареєструвала 1105 підтверджених кіберінцидентів, що на 62,5 % більше, ніж 2022 р. [23]. Такі тенденції зумовили ухвалення низки стратегічних рішень у сфері кібербезпеки, зокрема затвердження Плану заходів на 2025 р. із реалізації Стратегії кібербезпеки України, який передбачає створення кібервійськ, посилення контррозвідувального захисту, розбудову центрів реагування на кібератаки та поглиблення співпраці з ЄС і НАТО у сфері кібероборони [24]. Таким чином, у безпековому вимірі цифрова трансформація в Україні безпосередньо поєднується з потребою забезпечити стійкість держави до кіберзагроз, що посилює напруження між вимогами безпеки та гарантіями прав людини.

Паралельно з безпековим виміром, цифровізація державного управління стала одним із ключових інструментів стійкості правової системи. Як зазначає Гарвардська школа Кеннеді (2025), ще до повномасштабного вторгнення Україна

цілеспрямовано розбудовувала модель «держави у смартфоні», усуваючи бюрократію, впроваджуючи безпаперові сервіси та підвищуючи прозорість. У воєнних умовах ця трансформація набула стратегічного значення: цифрова інфраструктура забезпечила безперервність функцій держави, доступ громадян до базових послуг та стійкість публічного управління навіть за умов масових кібератак і руйнування інфраструктури [25].

У березні 2025 р. платформа дістала високе міжнародне визнання — Time Magazine включив «Дію» до списку Найкращих винаходів 2024 р., відзначивши, зокрема, запровадження першої у світі онлайн–реєстрації шлюбу («world's first online marriage») та те, що Україна стала першою країною, де цифровий паспорт має повну юридичну силу[26]. Ці оцінки фіксують не лише технологічний рівень українських сервісів, а й зростаюче сприйняття України як лабораторії цифрової державності в умовах війни. Отже, досвід України демонструє, що цифровізація державного управління — від кіберзахисту до екосистеми «Дія» — стає не лише інструментом підвищення ефективності та стійкості держави, а й важливим критерієм її демократичної легітимності. У цифрову добу верховенство права виявляється не лише в межах класичного правозастосування, але й у здатності держави гарантувати прозорість, підзвітність та доступність цифрових сервісів навіть в умовах війни. Український досвід підкреслює, що саме дотримання принципів верховенства права — правової визначеності, рівності перед законом та ефективного захисту прав — є ключовою умовою успішності цифрової держави й запорукою довіри суспільства до інституцій у часи трансформацій.

Ключові виклики верховенству права в українській цифровій державі. Попри значний поступ у цифровізації державного управління та інтеграції до європейського правового простору, українська правова система залишається вразливою з точки зору верховенства права. Міжнародні показники свідчать про амбівалентну картину: з одного боку, за Індексом верховенства права World Justice Project за 2024 рік Україна демонструє поступове зростання і посідає 88-ме місце серед 142 країн; з іншого – загальний бал залишається нижчим за 0,5, що вказує на суттєві проблеми із незалежністю судової влади, ефективністю правозастосування та рівнем корупції [27]. Аналогічну картину дає Індекс сприйняття корупції: 36 балів зі 100 і 104-те місце зі 180 держав, хоч і є найкращим результатом України, однак свідчить про системний характер корупційних практик [28].

У науковій та інституційній оцінці підкреслюється, що ключові ризики для верховенства права полягають не стільки у відсутності сучасних законів, скільки у розриві між нормативною модернізацією та реальним правозастосуванням. У звітах Європейської Комісії щодо України акцентується на тому, що, попри просування у реформі Вищої ради правосуддя, створенні Вищого антикорупційного суду та оновленні антикорупційного законодавства, залишаються нерозв'язаними проблеми виконання судових рішень, в тому числі рішень

ЄСПЛ, та забезпечення фактичної незалежності суддів від політичного й олігархічного впливу [29, 30]. Таким чином формується стійкий «інституційний дефіцит», коли якісне законодавство не підкріплене належними гарантіями його неупередженого й послідовного застосування. Цей «інституційний дефіцит» безпосередньо відображається на цифровій сфері. Дослідження правового забезпечення цифрової трансформації в Україні підкреслюють фрагментарність законодавства, колізії між загальними нормами про інформацію, персональні дані, кібербезпеку та спеціальними актами, що регулюють окремі платформи чи реєстри [31].У результаті формально проголошені стандарти прозорості, підзвітності та захисту даних не завжди підкріплені достатніми процедурами контролю, ефективними механізмами оскарження та реальними санкціями. Окремим слабким місцем в умовах воєнного стану є ризик вибіркового застосування права. Як зауважує Венеційська комісія у своїх висновках щодо законодавства про протидію олігархам та реформу судової системи, непрозорі процедури, широкі дискреційні повноваження органів влади та відсутність достатніх запобіжників можуть призводити до політично вмотивованих рішень, що підриває довіру до правових інститутів [32]. У цифровому вимірі це означає загрозу використання інструментів, створених начебто для кіберзахисту чи боротьби з дезінформацією, для тиску на опонентів або незалежні медіа. У такій ситуації саме цифрова сфера стає тестом на здатність держави зберігати верховенство права в умовах війни: одні й ті самі технології можуть або посилювати інституційні гарантії, або відтворювати наявні деформації вибіркового правозастосування.

У контексті цифровізації ці інституційні обмеження конкретизуються у низці взаємопов’язаних викликів, які безпосередньо стосуються верховенства права.

По-перше, це інституційна спроможність держави забезпечити законність у кіберпросторі. Звіти Служби спеціального зв’язку та захисту інформації і незалежні дослідження фіксують кратне зростання кількості кіберінцидентів і атак, спрямованих не лише проти державних ресурсів, а й проти критичної інфраструктури, бізнесу та громадського сектору [33; 34]. В таких умовах посилення повноважень спецслужб і розширення інструментів моніторингу є передбачуваною реакцією, однак із точки зору верховенства права створює ризики непропорційного втручання в приватність, таємницю кореспонденції й свободу вираження поглядів.

По-друге, цифрова трансформація судової системи – впровадження електронного суду, дистанційних засідань, електронного доказування – породжує ризики нерівного доступу до правосуддя та технологічної дискримінації. Українські дослідження впливу діджиталізації на правосуддя підкреслюють, що без якісної технічної підтримки, стандартизованих процедур, захисту від збоїв та кіберзагроз електронні інструменти можуть не лише не посилити, а й послабити

гарантії справедливого суду [35]. Це особливо відчутно в умовах воєнного стану, коли частина громадян змушена перебувати на тимчасово окупованих територіях або за кордоном, і доступ до цифрових сервісів стає ключовою передумовою реалізації їхніх прав [36].

По-третє, регулювання персональних даних та штучного інтелекту набуває в Україні подвійного виміру. З одного боку, законопроєкт № 8153 про захист персональних даних, підготовлений у тісній співпраці з Радою Європи та експертами ЄС, покликаний гармонізувати національне законодавство з GDPR, запровадити інститут уповноваженого органу з захисту даних, сучасні принципи прозорості та підзвітності, а також спеціальні вимоги до автоматизованої обробки даних [22]. З іншого боку, експертні обговорення вказують на ризики недостатньої інституційної спроможності майбутнього регулятора, складність впровадження високих стандартів приватності для малого й середнього бізнесу та потенційний конфлікт між вимогами національної безпеки й захистом прав людини [31]. Отже, саме в цій сфері особливо гостро постає питання, чи буде українська модель даних реально сумісною з європейськими стандартами верховенства права, чи залишиться переважно декларативною.

По-четверте, у сфері демократичних процедур і політичних прав цифрові інструменти поєднуються з безпрецедентними обмеженнями, спричиненими війною. Відтермінування виборів під час воєнного стану, обмеження свободи зібрань, заборона окремих політичних партій і медіа – усе це має конституційні підстави, але в довгостроковій перспективі породжує ризик «нормалізації» надзвичайних режимів. Громадські аналітичні центри наголошують, що проведення виборів під час повномасштабної війни суперечить Конституції та міжнародним стандартам, однак одночасно вимагають від держави чітких дорожніх карт повернення до повноцінного демократичного процесу після скасування воєнного стану [37]. У цифровому вимірі це означає необхідність такого дизайну систем електронного урядування і е-демократії, який би гарантував відновлення повноцінних виборчих процедур, політичної конкуренції та публічної підзвітності, а не фіксував надзвичайні обмеження як постійну модель управління.

У сукупності ці тенденції окреслюють не просто набір окремих технічних чи процедурних проблем, а системний ризик зміщення балансу між публічною владою та індивідуальною свободою в цифровому середовищі. Саме тому в інформаційну еру верховенство права має виступати не декларацією, а базовим критерієм допустимості будь-яких цифрових рішень держави — від кібербезпеки й е-правосуддя до регулювання персональних даних, штучного інтелекту та е-демократії. Інакше кажучи, питання полягає не лише в тому, які цифрові технології впроваджує держава, а насамперед у тому, чи підпорядковані ці технології вимогам правової визначеності, пропорційності та ефективного захисту прав людини.

Можливості зміцнення верховенства права в умовах цифровізації: українська перспектива. Попри зазначені слабкі місця й ризики, українська правова система має значний потенціал використати цифрову трансформацію як вікно можливостей для зміцнення верховенства права. На цьому тлі, євроінтеграція та процес переговорів про вступ до ЄС створюють зовнішній «якір» реформ: у документах ЄС прямо наголошується, що консолідація верховенства права – одна з ключових передумов членства, а Україні рекомендується включити себе до загальноєвропейського «rule-of-law toolbox» – інструментарію моніторингу й підтримки реформ [38, підрозділ 2.2.2 “Rule of law”]. Це означає, що цифрові проєкти в сфері правосуддя, боротьби з корупцією, публічних закупівель чи управління фінансами можуть і повинні оцінюватися саме через призму верховенства права, а не лише ефективності чи економії ресурсів.

Водночас, специфічно український досвід цифровізації – насамперед платформи «Дія» – вже позиціонується на міжнародному рівні як успішний приклад цифрової держави в умовах війни, який поєднує доступність сервісів, зменшення бюрократії та прозорість процедур [39]. Наступним кроком має стати послідовне «вшивання» вимог верховенства права у дизайн цифрових сервісів, зокрема шляхом: - забезпечення можливості ефективного оскарження автоматизованих рішень; - чіткого розмежування повноважень органів, які опрацьовують дані; - прозорості алгоритмів і реєстрів, що впливають на права громадян; - запровадження реальних, а не декларативних механізмів судового й адміністративного контролю за цифровими платформами. Наступним етапом має стати розробка національної моделі регулювання штучного інтелекту, яка відкриває можливість від самого початку закласти ризик-орієнтований, людиноцентричний підхід, сумісний із AI Act. «Біла книга» з регулювання ШІ вже пропонує адаптацію європейських стандартів до українського контексту, зокрема у зв’язці з законопроєктом № 8153 щодо персональних даних [40]. Якщо ці підходи будуть імплементовані системно, Україна може не лише уникнути сценарію «цифрового авторитаризму», а й стати одним із регіональних лідерів із побудови правової моделі етичного й підзвітного використання ШІ.

Нарешті, розвиток цифрової інфраструктури правосуддя й адміністративних послуг створює можливість для підвищення правової культури й доступу до правової інформації. Дослідження гарантій прав людини в Україні на основі практики ЄСПЛ підкреслюють, що саме прозорість, публічність і доступність правової інформації є передумовами реального, а не декларативного верховенства права [41]. У цифрову добу це означає, що відкриті реєстри, електронні судові рішення, аналітика судової практики та публічні дані про діяльність органів влади стають не лише інструментом контролю, а й умовою належної якості правотворчості й правозастосування.

Отже, інформаційна ера висуває до національних правових систем вимогу не просто «оцифрувати» наявні інститути, а глибоко переосмислити їх крізь

призму верховенства права. На прикладі України видно, що цифрова трансформація й війна виступають одночасно каталізаторами й тестом для правової системи. Саме в цій подвійній перспективі з одного боку, цифровізація державного управління, інтеграція до європейського цифрового права, реформи у сфері захисту даних і кібербезпеки розширюють сферу дії верховенства права та створюють нові механізми його реалізації. З іншого – хронічні інституційні слабкості, корупція, ризики вибіркового правозастосування та надзвичайні повноваження у воєнний час загрожують відтворити старі деформації у нових – цифрових – формах.

Специфіка української правової системи в інформаційну еру полягає саме в цій діалектиці ризику й можливості. Якщо принцип верховенства права буде послідовно інтегрований у цифрове законодавство, інституційну архітектуру та дизайн цифрових сервісів (від персональних даних і ШІ до е-правосуддя й е-демократії), цифрова держава може стати інструментом консолідації правопорядку й довіри громадян. Якщо ж цього не станеться, цифровізація ризикує перетворитися на технократичну оболонку, що маскує збереження вибіркового правозастосування та дефіциту відповідальності.

У цьому сенсі український досвід має значення не лише для національної, а й для порівняльної теорії права: він демонструє, що в умовах війни та стрімкого технологічного розвитку верховенство права залишається ключовим критерієм легітимності будь-яких цифрових новацій і фактично визначає, чи стає цифрова держава інструментом посилення прав людини та підзвітності влади, чи лише відтворює структурну слабкість панування права в оновленій технічній формі.

Висновки. Інформаційна ера радикально змінює спосіб функціонування правових систем, а цифрова держава стає одним із ключових середовищ реалізації права. Порівняльний аналіз розвитку цифрового регулювання у провідних юрисдикціях – від національних відповідей на кіберзлочинність (CFAA, судова практика у справі Van Buren v. United States) до наднаціональних рамок Ради Європи й ЄС (Будапештська конвенція, GDPR, DSA, DMA, AI Act) – показує, що юридично успішні моделі цифрового врядування спираються не стільки на технічні рішення, скільки на послідовну інтеграцію принципу верховенства права. Саме він забезпечує передбачуваність і пропорційність регулювання, обмеження дискреції держави й великих платформ, а також реальні механізми підзвітності в умовах алгоритмічного прийняття рішень.

Український досвід підтверджує амбівалентність цифрової трансформації: з одного боку, євроінтеграційний курс, гармонізація законодавства із GDPR і Конвенцією 108+, розвиток системи кібербезпеки та екосистеми «Дія» розширюють простір дії верховенства права та створюють нові інструменти реалізації прав людини. З іншого боку, хронічні інституційні слабкості – низькі позиції в індексах верховенства права й сприйняття корупції, проблеми незалежності судової влади, виконання судових рішень і протидії олігархічному

впливу – обмежують здатність правової системи гарантувати реальну, а не декларативну дію правових стандартів. Воєнний стан додатково підсилює ризики вибіркового правозастосування, розширює повноваження органів безпеки та створює спокусу використовувати цифрові інструменти як засіб контролю, а не як ресурс прозорості й підзвітності.

У цьому контексті цифрова трансформація української держави постає одночасно як поле ризиків і як «вікно можливостей» для зміцнення верховенства права. Від того, наскільки послідовно принципи правової визначеності, рівності перед законом, пропорційності та ефективного судового захисту будуть «вшиті» в дизайн цифрових сервісів, архітектуру кібербезпеки, регулювання персональних даних, штучного інтелекту, е-правосуддя й е-демократії, залежить, чи стане цифрова держава інструментом консолідації правопорядку й довіри громадян, чи перетвориться на технократичну оболонку, що маскує збереження вибіркового правозастосування та дефіциту відповідальності. У цьому сенсі український досвід важливий не лише у національному вимірі, а й для порівняльного правознавства та загальної теорії права, оскільки наочно демонструє: в екстремальних умовах стрімкого технологічного розвитку саме верховенство права визначає, чи будуть цифрові інновації працювати на посилення прав людини й підзвітності влади або ж відтворюватимуть у цифровому середовищі вже наявні інституційні деформації верховенства права.

Література:

1. Ravšelj D., Umek L., Todorovski L., Aristovnik A. A Review of Digital Era Governance Research in the First Two Decades: A Bibliometric Study // Future Internet. – 2022. – Vol. 14, No. 5. – Art. 126. – DOI: 10.3390/fi14050126.

2. Ó Fathaigh R. Communication on Shaping Europe's Digital Future [Електронний ресурс] // IRIS. – 2020. – 2020-4:1/14. – European Audiovisual Observatory (Council of Europe). – Режим доступу: https://merlin.obs.coe.int/download/8841/pdf (дата звернення: 23.11.2025).

3. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [Електронний ресурс] // Official Journal of the European Union. – 2022. – L 265. – P. 1–66. – Режим доступу: https://eur-lex.europa.eu/eli/reg/2022/1925/oj (дата звернення: 23.11.2025).

4. European Commission. 2020 Rule of Law Report: The Rule of Law Situation in the European Union [Електронний ресурс]. – Brussels : European Commission, 2020. – 28 p. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0580 (дата звернення: 23.11.2025).

5. Council of Europe, European Commission for the Efficiency of Justice (CEPEJ). European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment [Електронний ресурс]. – Strasbourg : Council of Europe, 2018. – 21 p. – Режим доступу: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c (дата звернення: 23.11.2025).

6. United States. Computer Fraud and Abuse Act: Public Law 99-474. Title 18, United States Code, Section 1030, as amended [Електронний ресурс]. – Washington, D.C. : U.S. Government Printing Office, 1986. – Режим доступу: https://www.law.cornell.edu/uscode/text/18/1030 (дата звернення: 23.11.2025).

7. Kerr O. S. Vagueness Challenges to the Computer Fraud and Abuse Act // Minnesota Law Review. – 2010. – Vol. 94, No. 5. – P. 1561–1607. – Режим доступу: https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1507&context=mlr (дата звернення: 23.11.2025).

8. Van Buren v. United States. 593 U.S. 374 (2021) : Opinion of the Supreme Court of the United States, June 3, 2021 [Електронний ресурс]. – Washington, D.C. : Supreme Court of the United States, 2021. – 54 p. – Режим доступу: https://www.supremecourt.gov/opinions/20pdf/19-783_k53l.pdf (дата звернення: 23.11.2025).

9. Clough J. A. A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation // Monash University Law Review. – 2014. – Vol. 40, No. 3. – P. 698–736. – Режим доступу: https://ssrn.com/abstract=2615789 (дата звернення: 23.11.2025).

10. Cybercrime Programme Office (C-PROC), Council of Europe. The Budapest Convention on Cybercrime: Benefits and Impact in Practice [Електронний ресурс]. – Strasbourg : Council of Europe, 2020. – Режим доступу: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac (дата звернення: 23.11.2025).

11. European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // Official Journal of the European Union. – 2016. – L 119. – P. 1–88.

12. Bradford A. The Brussels Effect: How the European Union Rules the World. – Oxford : Oxford University Press, 2020. – Chapter 5: Digital Economy. – P. 131–170. – DOI: 10.1093/oso/9780190088583.003.0006.

13. Кунер К. Б., Бейґрейв Л. А., Доксі К., Дречслер Л., Тозоні Л. (ред.) The EU General Data Protection Regulation: A Commentary / Update of Selected Articles. – Oxford : Oxford University Press, 2021. – 332 с. – DOI: 10.2139/ssrn.3839645.

14. All-Party Parliamentary Group on the Rule of Law. Data Processing and the Rule of Law: Briefing [Електронний ресурс]. – London : The Bingham Centre for the Rule of Law, 13.05.2019. – 12 p. – Режим доступу: https://www.biicl.org/documents/2101_data_processing_appg_briefing_-_may_2019_002.pdf (дата звернення: 23.11.2025).

15. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [Електронний ресурс] // Official Journal of the European Union. – 2022. – L 277. – P. 1–102. – Режим доступу: https://eur-lex.europa.eu/eli/reg/2022/2065/oj (дата звернення: 23.11.2025).

16. De Gregorio G. What is Digital Constitutionalism? A view from Europe [Електронний ресурс] // Heinrich-Böll-Stiftung. – 30 March 2022. – Режим доступу: https://il.boell.org/en/2023/03/30/what-digital-constitutionalism-view-europe (дата звернення: 23.11.2025)..

17. European Parliament. EU AI Act: First Regulation on Artificial Intelligence [Електронний ресурс]. – 2023. – Режим доступу: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (дата звернення: 23.11.2025).

18. The Wall Street Journal. EU AI Act Passes: World's First Comprehensive Legislation on Artificial Intelligence [Електронний ресурс]. – 2024. – Режим доступу: https://www.wsj.com/tech/ai/ai-act-passes-european-union-law-regulation-e04ec251 (дата звернення: 23.11.2025).

19. European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [Електронний ресурс] // Official Journal of the European Union. – 2024. – L 1689. – Режим доступу: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (дата звернення: 23.11.2025).

20. CERIDAP. The EU and the AI Act: Was it Worthwhile to Be the First? [Електронний ресурс]. – 2024. – Режим доступу: https://ceridap.eu/the-eu-and-the-ai-act-was-it-worthwhile-to-be-the-first (дата звернення: 23.11.2025).

21. Верховна Рада України. Проєкт Закону про захист персональних даних : № 8153 від 25.10.2022 р. [Електронний ресурс]. – Офіційний вебсайт Верховної Ради України. – Режим доступу: https://itd.rada.gov.ua/billinfo/Bills/Card/40707 (дата звернення: 23.11.2025).

22. Council of Europe Office in Ukraine. Protection of Ukrainians 'Personal Data Is on Time – an Expert Discussion of the Opinion Provided by the Council of Europe on the Draft Law No. 8153 of 25.10.2022 on "Personal Data Protection" [Електронний ресурс]. – News & Events, 14.06.2023. – Режим доступу: https://www.coe.int/en/web/kyiv/-/protection-of-ukrainians-personal-data-is-on-time-an-expert-discussion-of-the-opinion-provided-by-the-council-of-europe-on-the-draft-law-no.-8153-of-25.10.2022-on-personal-data-protection- (дата звернення: 23.11.2025).

23. Державна служба спеціального зв'язку та захисту інформації України. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році [Електронний ресурс]. – 08.01.2024. – Київ. – Режим доступу: https://scpc.gov.ua/uk/articles/334 (дата звернення: 23.11.2025).

24. Кабінет Міністрів України. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : розпорядження від 07 берез. 2025 р. № 204-р. – Київ : КМУ, 2025. – 15 с.

25. Harvard Kennedy School. Ukraine's Digital Transformation: Innovation for Resilience [Електронний ресурс]. – 01.04.2025. – Режим доступу: https://www.hks.harvard.edu/centers/cid/voices/ukraines-digital-transformation-innovation-resilience (дата звернення: 23.11.2025).

26. Time Magazine. Diia recognized in TIME's Best Inventions 2024 for its significant impact and bold innovations, in the "Apps & Software" category — including online marriage and digital passport equivalency. *Digital State UA*, [Електронний ресурс]. – 14.03.2025. – Режим доступу: https://digitalstate.gov.ua/news/govtech/diia-among-times-2024-best-inventions (дата звернення: 23.11.2025).

27. World Justice Project. Ukraine Ranks 88 out of 142 in the World Justice Project Rule of Law Index [Електронний ресурс]. – Washington, DC : World Justice Project, 2024. – 4 p. – Режим доступу: https://worldjusticeproject.org/sites/default/files/documents/Ukraine_2.pdf (дата звернення: 23.11.2025).

28. Transparency International Ukraine. The 2023 Corruption Perceptions Index in the World [Електронний ресурс]. – Berlin ; Kyiv : Transparency International, 2024. – Режим доступу: https://cpi.ti-ukraine.org/2023/en/ (дата звернення: 23.11.2025).

29.European Commission. Commission Staff Working Document: Ukraine 2023 Report. Accompanying the document Communication on EU Enlargement Policy. SWD(2023) 699 final [Електронний ресурс]. – Brussels : European Commission, 2023. – Режим доступу: https://enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_699%20Ukraine%20report.pdf (дата звернення: 23.11.2025).

30. Shadow Report on Chapter 23 "Justice and Fundamental Rights" of the European Commission's 2023 Report on Ukraine [Електронний ресурс]. – 2024. – Режим доступу: https://www.pravojustice.eu/storage/app/uploads/public/66d/f14/496/66df14496ba65213093673.pdf (дата звернення: 23.11.2025).

31. Луценко В. Р. Правове забезпечення цифрової трансформації в Україні // Вісник Ужгородського національного університету. Серія: Право. – 2024. DOI: https://doi.org/10.24144/2307-3322.2024.81.1.9

32. European Commission for Democracy through Law (Venice Commission). Opinion on the Law "On the Prevention of Threats to National Security, Associated with the Excessive Influence of Persons Having Significant Economic or Political Weight in Public Life (Oligarchs)" of Ukraine. CDL-AD(2023)018 [Електронний ресурс]. – Venice : Council of Europe, 2023. – Режим доступу: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2023)018-e (дата звернення: 23.11.2025).

33. Davydiuk O., Potii O. National Cybersecurity Governance: Ukraine [Електронний ресурс] // National Cybersecurity Governance in Non-NATO Member States. – Tallinn : NATO Cooperative Cyber Defence Centre of Excellence, 2024. – Режим доступу: https://ccdcoe.org/uploads/2024/08/National-Cybersecurity-Governance_Ukraine_Davydiuk_Potii_2024.pdf (дата звернення: 23.11.2025).

34. Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році. [Електронний ресурс]. – Kyiv: SSSCIP, 2024. – Режим доступу: https://scpc.gov.ua/uk/articles/334 (дата звернення: 23.11.2025).

35. Кривцун Д. Гармонізація законодавства України з європейським правом у сфері цифрової трансформації судів // Слово Національної школи суддів України. – 2023. – № 3 (44). – С. 46–50. DOI 10.37566/2707-6849-2023-3(44)-4

36. Яновська О. Digital Technologies in the Judiciary Under Martial Law in Ukraine [Електронний ресурс] / Oleksandra Yanovska // Supreme Court of Ukraine. – 09.10.2025. – Режим доступу: https://court.gov.ua/eng/supreme/pres-centr/news/1894732/ (дата звернення: 23.11.2025).

37. Юридична довідка про неможливість проведення виборів в умовах воєнного стану [Електронний ресурс] // Громадянська мережа ОПОРА. – 10.10.2023. – Режим доступу: https://oporaua.org/vybory/yuridichna-dovidka-pro-nemozhlivist-provedennya-viboriv-v-umovah-voyennogo-stanu-24947 (дата звернення: 23.11.2025).

38. Darvas Z., Dabrowski M., Grabbe H., Léry Moffat L., Sapir A., Zachmann G. Ukraine's Path to European Union Membership and Its Long-term Implications [Електронний ресурс] : Policy Brief. – Brussels : Bruegel, 07.03.2024. – Режим доступу: https://www.bruegel.org/policy-brief/ukraines-path-european-union-membership-and-its-long-term-implications?utm_source=chatgpt.com (дата звернення: 23.11.2025).

39. Мануілова К. В., Норчук Ю. Правові засади цифровізації державного управління в Україні: виклики та перспективи // Legal Horizons. – 2025. – Т. 25, № 2. – С. 24–34. – [Електронний ресурс]. – Режим доступу: https://legalhorizons.com.ua/lh/article/view/204/140 (дата звернення: 23.11.2025).

40. Міністерство цифрової трансформації України. Біла книга з регулювання ШІ в Україні: бачення Мінцифри : версія для консультацій [Електронний ресурс]. – Київ : Міністерство цифрової трансформації України, 2024. – Режим доступу: https://repository.ldufk.edu.ua/handle/34606048/39053 (дата звернення: 23.11.2025).

41. Кучук А., Кобко Є., Радчук А., Книшов В., Волошанівська Т. Забезпечення прав людини в Україні на основі практики Європейського суду з прав людини // Соціально-правові студії. – 2025. – Т. 8, № 2. – С. 324–338. – DOI: 10.32518/sals2.2025.324. – Режим доступу: https://sls-journal.com.ua/uk/journals/tom-8-2-2025/zabezpechennya-prav-lyudini-v-ukrayini-na-osnovi-praktiki-yevropeyskogo-sudu-z-prav-lyudini (дата звернення: 23.11.2025).

References:

1. Ravšelj, D., Umek, L., Todorovski, L., & Aristovnik, A. A Review of Digital Era Governance Research in the First Two Decades: A Bibliometric Study. *Future Internet*, 2022, Vol. 14, No. 5, Art. 126. DOI: 10.3390/fi14050126.

2. Ó Fathaigh, R. Communication on Shaping Europe's Digital Future. *IRIS*, 2020, 2020-4:1/14. European Audiovisual Observatory (Council of Europe). Retrieved from https://merlin.obs.coe.int/download/8841/pdf.

3. European Union. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). *Official Journal of the European Union*, 2022, L 265, pp. 1–66. Retrieved from https://eur-lex.europa.eu/eli/reg/2022/1925/oj.

4. European Commission. 2020 Rule of Law Report: The Rule of Law Situation in the European Union. Brussels: European Commission, 2020. 28 p. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0580.

5. Council of Europe, European Commission for the Efficiency of Justice (CEPEJ). European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment. Strasbourg: Council of Europe, 2018. 21 p. Retrieved from https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c.

6. United States. Computer Fraud and Abuse Act: Public Law 99-474. Title 18, United States Code, Section 1030, as amended. Washington, D.C.: U.S. Government Printing Office, 1986. Retrieved from https://www.law.cornell.edu/uscode/text/18/1030.

7. Kerr, O. S. Vagueness Challenges to the Computer Fraud and Abuse Act. *Minnesota Law Review*, 2010, Vol. 94, No. 5, pp. 1561–1607. Retrieved from https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1507&context=mlr.

8. Van Buren v. United States. 593 U.S. 374 (2021): Opinion of the Supreme Court of the United States, June 3, 2021. Washington, D.C.: Supreme Court of the United States, 2021. 54 p. Retrieved from https://www.supremecourt.gov/opinions/20pdf/19-783_k53l.pdf.

9. Clough, J. A. A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation. *Monash University Law Review*, 2014, Vol. 40, No. 3, pp. 698–736. Retrieved from https://ssrn.com/abstract=2615789.

10. Cybercrime Programme Office (C-PROC), Council of Europe. The Budapest Convention on Cybercrime: Benefits and Impact in Practice. Strasbourg: Council of Europe, 2020. Retrieved from https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac.

11. European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, 2016, L 119, pp. 1–88.

12. Bradford, A. *The Brussels Effect: How the European Union Rules the World*. Oxford: Oxford University Press, 2020. Chapter 5: Digital Economy, pp. 131–170. DOI: 10.1093/oso/9780190088583.003.0006.

13. Kuner, C. B., Bygrave, L. A., Docksey, C., Drechsler, L., & Tosoni, L. (eds.). *The EU General Data Protection Regulation: A Commentary / Update of Selected Articles*. Oxford: Oxford University Press, 2021. 332 p. DOI: 10.2139/ssrn.3839645.

14. All-Party Parliamentary Group on the Rule of Law. Data Processing and the Rule of Law: Briefing. London: The Bingham Centre for the Rule of Law, 2019. 12 p. Retrieved from https://www.biicl.org/documents/2101_data_processing_appg_briefing_-_may_2019_002.pdf.

15. European Union. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union*, 2022, L 277, pp. 1–102. Retrieved from https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

16. De Gregorio, G. What is Digital Constitutionalism? A View from Europe. *Heinrich-Böll-Stiftung*, March 30, 2022. Retrieved from https://il.boell.org/en/2023/03/30/what-digital-constitutionalism-view-europe.

17. European Parliament. EU AI Act: First Regulation on Artificial Intelligence. 2023. Retrieved from https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

18. The Wall Street Journal. EU AI Act Passes: World's First Comprehensive Legislation on Artificial Intelligence. 2024. Retrieved from https://www.wsj.com/tech/ai/ai-act-passes-european-union-law-regulation-e04ec251.

19. European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*, 2024, L 1689. Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

20. CERIDAP. The EU and the AI Act: Was it Worthwhile to Be the First? 2024. Retrieved from https://ceridap.eu/the-eu-and-the-ai-act-was-it-worthwhile-to-be-the-first.

21. Verkhovna Rada of Ukraine. Draft Law on Personal Data Protection No. 8153 dated October 25, 2022. Official website of the Verkhovna Rada of Ukraine. Retrieved from https://itd.rada.gov.ua/billinfo/Bills/Card/40707.

22. Council of Europe Office in Ukraine. Protection of Ukrainians' Personal Data Is on Time: An Expert Discussion of the Opinion Provided by the Council of Europe on the Draft Law No. 8153 of October 25, 2022 on "Personal Data Protection". *News & Events*, June 14, 2023. Retrieved from https://www.coe.int/en/web/kyiv/-/protection-of-ukrainians-personal-data-is-on-time-an-expert-discussion-of-the-opinion-provided-by-the-council-of-europe-on-the-draft-law-no.-8153-of-25.10.2022-on-personal-data-protection-.

23. State Service of Special Communications and Information Protection of Ukraine. Statistical report on the results of operation of the Vulnerability Detection and Response System to cyber incidents and cyberattacks in 2023. Kyiv, January 8, 2024. Retrieved from https://scpc.gov.ua/uk/articles/334.

24. Cabinet of Ministers of Ukraine. On approval of the action plan for 2025 for the implementation of the Cybersecurity Strategy of Ukraine: Order No. 204-r dated March 7, 2025. Kyiv: Cabinet of Ministers of Ukraine, 2025. 15 p.

25. Harvard Kennedy School. Ukraine's Digital Transformation: Innovation for Resilience. April 1, 2025. Retrieved from https://www.hks.harvard.edu/centers/cid/voices/ukraines-digital-transformation-innovation-resilience.

26. Time Magazine. Diia recognized in TIME's Best Inventions 2024 for its significant impact and bold innovations in the "Apps & Software" category, including online marriage and digital passport equivalency. *Digital State UA*, March 14, 2025. Retrieved from https://digitalstate.gov.ua/news/govtech/diia-among-times-2024-best-inventions.

27. World Justice Project. Ukraine Ranks 88 out of 142 in the World Justice Project Rule of Law Index. Washington, DC: World Justice Project, 2024. 4 p. Retrieved from https://worldjusticeproject.org/sites/default/files/documents/Ukraine_2.pdf.

28. Transparency International Ukraine. The 2023 Corruption Perceptions Index in the World. Berlin; Kyiv: Transparency International, 2024. Retrieved from https://cpi.ti-ukraine.org/2023/en/.

29. European Commission. Commission Staff Working Document: Ukraine 2023 Report. Accompanying the document *Communication on EU Enlargement Policy*. SWD(2023) 699 final. Brussels: European Commission, 2023. Retrieved from https://enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_699%20Ukraine%20report.pdf.

30. Shadow Report on Chapter 23 "Justice and Fundamental Rights" of the European Commission's 2023 Report on Ukraine. 2024. Retrieved from https://www.pravojustice.eu/storage/app/uploads/public/66d/f14/496/66df14496ba65213093673.pdf.

31. Lutsenko, V. R. Legal support of digital transformation in Ukraine. *Visnyk of Uzhhorod National University. Series: Law*, 2024. DOI: 10.24144/2307-3322.2024.81.1.9 [in Ukrainian].

32. European Commission for Democracy through Law (Venice Commission). Opinion on the Law "On the Prevention of Threats to National Security, Associated with the Excessive Influence of Persons Having Significant Economic or Political Weight in Public Life (Oligarchs)" of Ukraine. CDL-AD(2023)018. Venice: Council of Europe, 2023. Retrieved from https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2023)018-e.

33. Davydiuk, O., & Potii, O. National Cybersecurity Governance: Ukraine. In *National Cybersecurity Governance in Non-NATO Member States*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2024. Retrieved from https://ccdcoe.org/uploads/2024/08/National-Cybersecurity-Governance_Ukraine_Davydiuk_Potii_2024.pdf.

34. State Cyber Protection Center of the State Service of Special Communications and Information Protection of Ukraine. Statistical report on the results of operation of the Vulnerability Detection and Response System to cyber incidents and cyberattacks in 2023. Kyiv: SSSCIP, 2024. Retrieved from https://scpc.gov.ua/uk/articles/334.

35. Kryvtsun, D. Harmonization of Ukrainian legislation with European law in the field of digital transformation of courts. *Slovo of the National School of Judges of Ukraine*, 2023, No. 3 (44), pp. 46–50. DOI: 10.37566/2707-6849-2023-3(44)-4 [in Ukrainian].

36. Yanovska, O. Digital Technologies in the Judiciary Under Martial Law in Ukraine. *Supreme Court of Ukraine*, October 9, 2025. Retrieved from https://court.gov.ua/eng/supreme/pres-centr/news/1894732/.

37. OPORA Civic Network. Legal opinion on the impossibility of holding elections under martial law. October 10, 2023. Retrieved from https://oporaua.org/vybory/yuridichna-dovidka-pro-nemozhlivist-provedennya-viboriv-v-umovah-voyennogo-stanu-24947.

38. Darvas, Z., Dabrowski, M., Grabbe, H., Léry Moffat, L., Sapir, A., & Zachmann, G. Ukraine's Path to European Union Membership and Its Long-term Implications: Policy Brief. Brussels: Bruegel, March 7, 2024. Retrieved from https://www.bruegel.org/policy-brief/ukraines-path-european-union-membership-and-its-long-term-implications.

39. Manuilova, K. V., & Norchuk, Yu. Legal foundations of digitalization of public administration in Ukraine: Challenges and prospects. *Legal Horizons*, 2025, Vol. 25, No. 2, pp. 24–34. Retrieved from https://legalhorizons.com.ua/lh/article/view/204/140 [in Ukrainian].

40. Ministry of Digital Transformation of Ukraine. White Paper on AI Regulation in Ukraine: Vision of the Ministry of Digital Transformation (consultation version). Kyiv: Ministry of Digital Transformation of Ukraine, 2024. Retrieved from https://repository.ldufk.edu.ua/handle/34606048/39053.

41. Kuchuk, A., Kobko, Ye., Radchuk, A., Knyshov, V., & Voloshanivska, T. Ensuring human rights in Ukraine based on the case law of the European Court of Human Rights. *Socio-Legal Studies*, 2025, Vol. 8, No. 2, pp. 324–338. DOI: 10.32518/sals2.2025.324 [in Ukrainian].