

ЦИФРОВИЙ СУВЕРЕНІТЕТ ДЕРЖАВ: МІЖ ДЕМОКРАТІЄЮ І КОНТРОЛЕМ У ГЛОБАЛЬНОМУ ПРОСТОРИ

У тезах досліджується феномен цифрового суверенітету як нової форми реалізації державної влади в умовах глобальної цифровізації. Автор розкриває трансформацію поняття суверенітету у XXI столітті, зосереджуючи увагу на зміні балансу між державами та транснаціональними цифровими корпораціями, які дедалі частіше впливають на політичні процеси та суспільну комунікацію. Аналізуються різні моделі реалізації цифрового суверенітету – європейська регуляторна, китайська авторитарна та американська геоекономічна.

Особливу увагу приділено дилемі між цифровим контролем та цифровою демократією, використанню технологій для участі громадян у прийнятті рішень, а також загрозам, які постають унаслідок моніторингу, цензури й застосування штучного інтелекту. Автор стверджує, що міжнародне право наразі не здатне забезпечити ефективного регулювання цифрового простору, що створює виклики для глобальної етики, прав людини та міждержавної рівноваги. У висновку підкреслюється необхідність формування глобальних стандартів цифрової відповідальності, що забезпечували б баланс між суверенітетом, свободами і технологічним прогресом.

Ключові слова: цифровізація, цифрова демократія, глобальне врядування, цифрова нерівність, інтернет платформи.

У XXI столітті цифрові технології стали не лише каталізатором глибоких трансформацій соціально-економічного життя, але й фундаментальним чинником, що переосмислює і переналаштовує архітектуру сучасної системи міжнародних відносин. Процеси цифровізації охопили всі сфери людської діяльності – від економіки і освіти до оборони й дипломатії, – створюючи новий глобальний простір взаємодії, який дедалі більше виходить за межі фізичних територій і національних кордонів. У цьому контексті виникає якісно новий вимір – цифровий простір, що суттєво розширює уявлення про природу державного суверенітету у сучасному світі.

Традиційне розуміння суверенітету, сформоване в епоху Вестфальської системи, базувалося на домінуванні держави над певною фізичною територією, визначеними кордонами, природними ресурсами та населенням. Проте в умовах цифрової епохи ці параметри більше не є вичерпними. До них додається новий критично важливий компонент – здатність держави здійснювати ефективний контроль і управління у цифровому вимірі. Це включає кілька взаємопов'язаних елементів: регулювання потоків цифрової інформації; контроль над інфраструктурою зв'язку і передавання даних; забезпечення кібербезпеки; управління діяльністю глобальних цифрових платформ; а також формування і реалізацію національної політики у сфері захисту персональних даних громадян.

Сукупність цих завдань і механізмів отримала назву цифрового суверенітету. Це поняття означає прагнення держав до збереження та утвердження своєї автономії в цифровому просторі, захисту національних інтересів в умовах глобальної мережевої взаємозалежності, а також забезпечення інформаційної безпеки як складової національної безпеки загалом. Таким чином, цифровий суверенітет постає як нова парадигма державного суверенітету, що вимагає переосмислення усталених норм міжнародного права та інституційної взаємодії між державами.

Цифровий суверенітет можна визначити як сукупність прав і механізмів, за допомогою яких держава встановлює правила цифрової взаємодії в межах своєї юрисдикції, регулює збирання, обробку, зберігання й передачу даних, захищає критичну інформаційну інфраструктуру, а також формує політику щодо діяльності іноземних цифрових компаній на національному ринку. Цей концепт став відповіддю на безпрецедентне розширення влади приватних технологічних гігантів – таких як Google, Meta, Microsoft, TikTok – які дедалі частіше функціонують як некласичні глобальні актори міжнародних відносин.

Завдяки своїм технологічним ресурсам, алгоритмічному контролю над потоками інформації, доступу до величезних обсягів персональних даних користувачів, ці транснаціональні корпорації набули фактичного впливу на публічну сферу, що традиційно була прерогативою держави. У багатьох випадках саме цифрові платформи визначають умови інформаційного обігу, модерацію контенту, структуру комунікацій та навіть рамки політичного дискурсу. При цьому вони залишаються непідзвітними національним урядам, оскільки не

є суб'єктами міжнародного публічного права і можуть діяти згідно із власною корпоративною логікою, яка не завжди узгоджується з національними чи суспільними інтересами [3].

У результаті виникає асиметрія між публічною владою (державою) та приватною цифровою владою (технологічними корпораціями), що ставить під сумнів ефективність держав у захисті цифрових прав своїх громадян, гарантуванні інформаційної безпеки та збереженні політичного суверенітету у віртуальному просторі. Держава, яка втрачає контроль над цифровою інфраструктурою, автоматично послаблює свої позиції як повноцінний суб'єкт міжнародних відносин. Тому цифровий суверенітет дедалі більше розглядається не лише як технічна або економічна категорія, а як політична доктрина, що інтегрує в собі безпековий, юридичний, культурний та етичний виміри.

Крім того, дискусії щодо цифрового суверенітету торкаються глобальних нормативних дилем: чи має держава право обмежувати діяльність іноземних платформ, посиляючись на національні інтереси, і чи не порушує це глобальні принципи відкритості Інтернету? Такі питання стають особливо актуальними в умовах геополітичної напруги та зростання кіберзагроз, коли держави починають розглядати інформаційний простір як поле стратегічного протистояння.

Різні країни реалізують цифровий суверенітет по-різному. ЄС демонструє регуляторний підхід, зосереджений на захисті цифрових прав громадян і контролі за діяльністю платформ. Визначальним етапом стала імплементація «Загального регламенту про захист персональних даних» (GDPR), який надає громадянам право контролювати обробку своїх даних, а також зобов'язує компанії до прозорості та відповідальності. У цьому ж напрямку працюють нові регламенти ЄС: «Digital Services Act» та «Digital Markets Act», що встановлюють правила для цифрових гігантів і сприяють прозорості алгоритмів. Китай реалізує іншу модель, а саме інфраструктурно-авторитарну. Тут держава не лише регламентує, а й активно володіє основними платформами, блокує доступ до іноземних ресурсів і розвиває власні аналоги, такі наприклад як: WeChat, Weibo, Baidu. Створення «Великого китайського фаєрволу», система соціального рейтингу, масове спостереження за онлайн-активністю громадян усе це свідчить про глибоке проникнення держави в цифрове життя суспільства. У США цифровий суверенітет реалізується через підтримку глобального домінування національних технологічних компаній і встановлення міжнародних стандартів. Тут підхід ґрунтується не на ізоляції, а на поширенні впливу через ринки, інновації та геополітичну інтеграцію. Саме Сполучені Штати найбільше впливають на розвиток цифрових стандартів, інфраструктури, розробку штучного інтелекту й систем комунікації. З іншого боку, американські компанії регулярно критикуються за монополізацію, експлуатацію персональних даних, втручання у внутрішні справи інших держав [2; 1; 3].

Важливо підкреслити, що цифровий суверенітет не завжди є синонімом безпеки і прогресу. У багатьох країнах його використання супроводжується придушенням свободи слова, обмеженням доступу до інформації, поширенням онлайн-цензури та масовим наглядом. Так виникає явище цифрового авторитаризму, а саме поєднання новітніх технологій з авторитарними практиками управління, що дозволяє не лише контролювати населення, а й моделювати політичну поведінку через інформаційні маніпуляції. Такі процеси становлять серйозну загрозу для цифрової демократії, тобто, концепції, яка передбачає відкритість, підзвітність, електронну участь громадян у врядуванні, прозорість алгоритмів та доступ до публічної інформації.

У сучасну епоху цифрових трансформацій демократія набуває нових форм та механізмів реалізації, адаптуючись до змін у способах комунікації, доступу до інформації та організації громадянської участі. Цифрова демократія – це концепт, що позначає використання інформаційно-комунікаційних технологій (ІКТ) для посилення демократичних процесів, розширення участі громадян у політичному житті та забезпечення прозорості й підзвітності влади. Вона не замінює традиційні форми демократії, але значною мірою доповнює та модернізує їх, відкриваючи нові канали для взаємодії між державою і суспільством.

Реалізація цифрової демократії відбувається через набір інструментів, що забезпечують активну участь громадян у процесах прийняття рішень, контролі за владою та формуванні публічної політики. До таких інструментів належать: електронне голосування, яке дозволяє здійснювати виборчі процедури дистанційно та оперативно, підвищуючи доступність для широких верств населення; електронні петиції, що надають змогу громадянам формулювати колективні запити та ініціативи до органів влади; онлайн-дискусії та форуми, де громадяни можуть висловлювати свої погляди щодо поточних питань, брати участь у консультаціях і дебатах; краудсорсинг рішень, який передбачає колективне вироблення політичних чи управлінських рішень шляхом залучення громадськості до аналізу проблем та формулювання рішень; платформи прозорого врядування (open government), що забезпечують доступ до відкритих даних, державних бюджетів, рішень та процедур.

Використання таких технологій не лише розширює канали політичної участі, а й зміцнює соціальну залученість, оскільки громадяни мають змогу безпосередньо впливати на процеси управління. Це, у свою чергу, посилює довіру до інституцій, підвищує ефективність зворотного зв'язку між владою та суспільством і створює умови для більш відповідального й відкритого врядування [1].

Як зазначає Л. Флоріді, розвиток цифрових технологій сприяє перетворенню громадян із пасивних спостерігачів на активних учасників інформаційного суспільства, що веде до формування нової етики цифрової взаємодії та відповідальності [4]. У цьому сенсі цифрова демократія – це не лише про інструменти, а й про зміну політичної культури, розширення горизонтів участі та переосмислення самого поняття «громадянства» в цифрову епоху.

Особливо загрозово виглядає тенденція до використання штучного інтелекту для прогнозування і контролю поведінки громадян, персоналізованого політичного таргетингу, фільтрації контенту на основі політичної лояльності. Подібні дії руйнують не лише принципи вільної комунікації, а й підривають саму сутність демократичної участі, зменшуючи роль індивіда до об'єкта маніпуляцій. У глобальному вимірі цифровий суверенітет перетворюється на поле геополітичного протистояння. Світ дедалі більше поляризується між відкритими цифровими системами й закритими інфраструктурами контролю. Формуються блоки союзників, які підтримують спільні технологічні стандарти, створюють союзи кібербезпеки, розробляють єдині протоколи шифрування, співпрацюють у сфері штучного інтелекту. При цьому питання прозорості, дотримання прав людини, недопущення монополій залишаються відкритими [5; 6].

Стрімкий розвиток цифрових технологій, трансформація форм комунікації та зростаюча роль цифрових платформ у політичному, соціальному й економічному житті висунули нові виклики перед системою міжнародного права, яка історично формувалася в умовах фізичної територіальності, чітких державних кордонів і суверенітетів. На відміну від традиційних сфер регулювання, таких як торгівля, безпека чи навколишнє середовище, цифровий простір є динамічним, безмежним і високотехнологічним середовищем, де юрисдикція однієї держави може легко перетинатися з інтересами іншої, а головними гравцями дедалі частіше виступають не держави, а приватні транснаціональні корпорації.

Попри зростаючу залежність держав від цифрової інфраструктури, міжнародне право поки що не повною мірою адаптувалося до нових реалій. Спроби виробити універсальні, зобов'язуючі норми цифрового врядування залишаються фрагментарними, обмеженими за масштабом і здебільшого мають рекомендаційний характер. Так, наприклад, ЮНЕСКО у 2023 році опублікувала «Guidelines for the Governance of Digital Platforms», в яких висловлено заклик до: забезпечення прозорості алгоритмів, що визначають інформаційні потоки та видимість контенту; захисту прав користувачів, включно з правом на приватність, свободу вираження поглядів та доступ до інформації; протидії дезінформації, яка підриває демократичні процеси та соціальну довіру [7].

Ці настанови становлять важливий крок у формуванні етичних і політичних орієнтирів для цифрової політики, однак, не маючи обов'язкової юридичної сили, вони не створюють дієвого механізму відповідальності для держав і, тим паче, для приватних платформ.

Унаслідок цього виникає вакуум нормативного регулювання, у якому одночасно функціонують наддержавні компанії та авторитарні уряди, які часто використовують цифровий простір для досягнення власних стратегічних цілей – зокрема, маніпуляції громадською думкою, цензури, стеження або кібернападів. Відсутність єдиного міжнародного договору чи конвенції, що охоплювала б питання цифрових прав, цифрового суверенітету, відповідальності платформ, кібербезпеки та штучного інтелекту, ускладнює координацію між країнами і створює простір для зловживань.

Крім того, спроби досягти міжнародного консенсусу щодо регулювання цифрової сфери часто натрапляють на конфлікт між ціннісними моделями: ліберальна демократична традиція (захист прав людини, вільний обіг інформації) вступає в суперечність із авторитарною практикою цифрового контролю. Так, переговори у межах ООН чи форуму IGF (Internet Governance Forum) часто залишаються декларативними, оскільки бракує політичної волі для ухвалення зобов'язуючих рішень.

Таким чином, у сфері міжнародного права наразі спостерігається нормативна невизначеність, яка суттєво стримує розвиток глобальної цифрової етики та унеможливує формування узгоджених стандартів відповідальності в цифровому середовищі. Відсутність ефективного регулювання не лише обмежує потенціал міждержавної співпраці, але й поглиблює глобальну нерівність – як у доступі до цифрових ресурсів, так і у здатності захищати національні інтереси в умовах цифрової взаємозалежності. Менш потужні держави, які не мають власної цифрової інфраструктури або впливу на діяльність транснаціональних платформ, опиняються у вразливому становищі, позбавлені реальних інструментів впливу на інформаційну політику, захист персональних даних чи реагування на цифрові загрози.

У цьому контексті цифровий суверенітет постає як амбівалентне явище, що водночас відкриває нові можливості для захисту національного суверенітету та культурної ідентичності, але й створює ризики для основ демократичного ладу. Його надмірна або непрозора реалізація може спричинити цензуру, масове спостереження, обмеження свободи слова, а також використання цифрових інструментів для політичного контролю, особливо в авторитарних або напівавторитарних режимах. З іншого боку, виважена і збалансована реалізація цифрового суверенітету може стати основою для побудови цифрової демократії, де держава виступає гарантом цифрових прав, а не обмежувачем свобод.

Ключовим викликом сучасності є пошук балансу між легітимним державним регулюванням цифрового простору та забезпеченням фундаментальних цифрових прав людини – таких як: свобода вираження поглядів, право на приватність і захист персональних даних, право на участь у цифрових процесах, доступ до безпечної та достовірної інформації.

Без цього балансу цифровий простір ризикує стати або ареною хаотичної комерціалізації, або інструментом цифрового авторитаризму. У зв'язку з цим міжнародне співтовариство має усвідомити нагальну потребу в розробці глобальних нормативних механізмів цифрової відповідальності, які б поєднували: принципи державного суверенітету; універсальні стандарти прав людини; етичні засади

цифрового врядування; механізми міждержавного діалогу з питань цифрової безпеки, прозорості, штучного інтелекту та управління даними.

Лише в рамках спільних зусиль – з урахуванням культурного розмаїття, правової рівності держав і прав людини як універсальної основи – можливо створити справедливую, безпечну і відкриту цифрову екосистему, що буде служити як демократичним суспільствам, так і глобальному миру.

References

1. Coleman, S., & Shane, P. M. (2012). Connecting democracy: Online consultation and the flow of political communication. *European Journal of Communication* 28(4):477-480. <https://doi.org/10.1177/0267323113485777c>.
2. Creemers, R. (2017). Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century. *Journal of Contemporary China*, 26(103), 85–100. <https://doi.org/10.1080/10670564.2016.1206281>.
3. De Nardis, L. (2020). *The Internet in everything: Freedom and security in a world with no off switch*. Yale University Press.
4. Floridi, L. (2020). *The logic of information: A theory of philosophy as conceptual design*. Oxford University Press.
5. Freedom House. (2023). *Freedom on the Net 2023: The Repressive Power of Artificial Intelligence*. <https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence>
6. MacKinnon, R. (2012). *Consent of the networked: The worldwide struggle for Internet freedom*. Basic Books. ISBN 10: 0465024424.
7. UNESCO. (2023). *Guidelines for the governance of digital platforms*. <https://www.unesco.org/en/internet-trust/guidelines>.

DOI 10.34132/mspc2025.01.07.11

Pavlo Petrov

STATE DIGITAL SOVEREIGNTY: BETWEEN DEMOCRACY AND CONTROL IN THE GLOBAL SPACE

The paper explores the phenomenon of digital sovereignty as a new form of state power realization in the context of global digitalization. The author analyzes the transformation of the concept of sovereignty in the 21st century, focusing on the shifting balance between states and transnational digital corporations, which increasingly influence political processes and public communication. Various models of digital sovereignty implementation are examined – the European regulatory model, the Chinese authoritarian model, and the American geoeconomic model.

Special attention is paid to the dilemma between digital control and digital democracy, the use of technologies for citizen participation in decision-making, and the threats posed by surveillance, censorship, and the use of artificial intelligence. The author argues that international law currently fails to provide effective regulation of the digital space, which generates significant challenges for global ethics, human rights, and interstate balance. In conclusion, the paper emphasizes the need to develop global standards of digital responsibility that would ensure a balance between sovereignty, freedoms, and technological progress.

Keywords: digitalization, digital democracy, global governance, digital inequality, internet platforms.

Відомості про автора / Information about the Author

Павло Петров, канд. політ. наук, доц., доцент кафедри міжнародних відносин, факультету суспільних наук і міжнародних відносин Дніпровського національного університету імені Олеся Гончара, м. Дніпро, Україна, E-mail: ppgdmo@gmsil.com, orcid: <https://orcid.org/0000-0001-9124-1763>.

Pavlo Petrov, PhD in Political Science, Associate Professor, Department of International Relations, Faculty of Social Sciences and International Relations, Oles Honchar Dnipro National University, Dnipro, Ukraine. E-mail: ppgdmo@gmsil.com, orcid: <https://orcid.org/0000-0001-9124-1763>.

© П. Петров
27.05.2025.

Стаття отримана редакцією

