

Digital Sovereignty, AI Sovereignty: New Dimensions of Geopolitical Competition in the Context of Deglobalization

UDC 323:327.172

DOI: <https://doi.org/10.15421/172662>**Radionova Iryna**Dr.Sc., Full Prof., <https://orcid.org/0000-0001-7134-3674>, radionova.irina@gmail.com*H.S. Skovoroda Kharkiv National Pedagogical University (Kharkiv, Ukraine)***Abstract.**

Relevance. Deglobalization processes have been found to be transforming the architecture of international relations and prompting a rethink of the nature of sovereignty in the context of digital transformation and the geopoliticalization of technology. The growing dependence of states on external digital platforms, infrastructures and algorithmic systems creates new strategic vulnerabilities and highlights the importance of digital and AI sovereignty in contemporary state policy.

The purpose. The study aims to define digital and AI sovereignty as new dimensions of geopolitical competition in the context of deglobalization.

Results. It has been established that technological sovereignty, digital sovereignty, AI sovereignty and data sovereignty form a hierarchically interconnected system of strategic state autonomy. The main models of digital sovereignty (rights-based model, market-oriented, centralisation and state-based) and their impact on regulatory fragmentation in the global digital space are characterised. It is found that AI sovereignty encompasses both “sovereignty over AI” and “sovereignty through AI”, acquiring technological, cultural, and value significance. The trend towards the fragmentation of the global digital order and the formation of a “resilient interdependence” paradigm is identified.

Conclusions. It has been established that digital and AI sovereignty operate as dynamic political and institutional constructs that shape contemporary geopolitical competition. Their role in balancing strategic autonomy with selective integration into global technological networks has been characterised. For Ukraine, it has been found that the development of sovereign digital infrastructure and national AI technologies is a key prerequisite for security, cyber resilience and long-term competitiveness amid technological turbulence.

Keywords: digital sovereignty, AI sovereignty, technological sovereignty, data sovereignty, deglobalization, geopolitical competition, global digital order, resilient interdependence

Цифровий суверенітет, ШІ-суверенітет: нові виміри геополітичної конкуренції в умовах деглобалізації

Радіонова Ірина*Харківський національний педагогічний університет імені Г.С. Сковороди (Харків, Україна)***Анотація**

Актуальність. Виявлено, що процеси деглобалізації трансформують архітектуру міжнародних відносин і зумовлюють переосмислення природи суверенітету в умовах цифрової трансформації та геополітизації технологій. З'ясовано, що зростання залежності держав від зовнішніх цифрових платформ, інфраструктур і алгоритмічних систем формує нові стратегічні вразливості, що актуалізує проблематику цифрового та ШІ-суверенітету як ключових вимірів сучасної державної політики.

Метою дослідження є визначення цифрового суверенітету та ШІ-суверенітету як нових вимірів геополітичної конкуренції в умовах деглобалізації.

Результати. Встановлено, що технологічний, цифровий суверенітет, ШІ-суверенітет і суверенітет даних формують ієрархічно взаємопов'язану систему стратегічної автономії держав. Охарактеризовано основні моделі цифрового суверенітету (модель, що базується на правах, ринково-орієнтовану, централізовану та державоцентричну) та їхній вплив на нормативну фрагментацію глобального цифрового простору. З'ясовано, що ШІ-суверенітет поєднує виміри «суверенітету над ШІ» та «суверенітету через ШІ», набуваючи не лише технологічного, а й культурно-ціннісного значення. Виявлено тенденцію фрагментації глобального цифрового порядку та формування парадигми «резильєнтної взаємозалежності».

Висновки. Встановлено, що цифровий і ШІ-суверенітет функціонують як динамічні політико-інституційні конструкції, які визначають конфігурацію сучасної геополітичної конкуренції. Охарактеризовано їхню роль як інструментів балансування між стратегічною автономією та вибірковою інтеграцією в глобальні технологічні мережі. З'ясовано, що для України розвиток суверенної цифрової інфраструктури та національних ШІ-технологій є ключовою передумовою безпеки, кіберстійкості та довгострокової конкурентоспроможності в умовах технологічної турбулентності.

Ключові слова: цифровий суверенітет, ШІ-суверенітет, технологічний суверенітет, суверенітет даних, деглобалізація, геополітична конкуренція, глобальний цифровий порядок, резильєнтна взаємозалежність

Вступ.

Сучасна геополітична динаміка дедалі більше формується під впливом процесів деглобалізації, яку можна визначити як рух у напрямі менш інтегрованого світу, де пріоритет надається потужним національним державам, локальним рішенням та посиленому прикордонному контролю на противагу глобальним інституціям і вільним потокам (Kornprobst & Wallace, 2025). Цей тренд, що характеризується розривом глобальних ланцюгів постачання, технологічним протистоянням і національним протекціонізмом, змушує держави кардинально переосмислювати підходи до власної безпеки, економічної незалежності та, що особливо важливо, суверенітету.

В умовах цифрової трансформації залежність від іноземної технологічної інфраструктури та платформ постає не лише економічною проблемою, а й стратегічною вразливістю, що загрожує національній безпеці. Виникає потреба у створенні «цифрових кордонів» для захисту суспільно значущих цінностей, критично важливих інформаційних потоків і даних громадян.

Аналіз попередніх досліджень та публікацій. Вітчизняні дослідники розглядають цифровий суверенітет у контексті національної безпеки. Ю.І. Калюжна фокусує увагу на з'ясуванні еволюції політики цифрового суверенітету ЄС, ініціативах Міністерства цифрової трансформації України, поглибленні демократичного партнерства між ЄС та Україною (Калюжна, 2025). Досвід формування та розвитку цифрового суверенітету ЄС також досліджується Милосердною І.М. (2024). Ю.П. Калайда висвітлює кращі практики зарубіжного досвіду у сфері забезпечення цифрового суверенітету, окреслює загрози діяльності соціальних мереж та онлайн-платформ у контексті цифрового суверенітету, деталізує шляхи удосконалення вітчизняного законодавства щодо посилення цифрового суверенітету (Калайда, 2021).

Метою дослідження є визначення цифрового суверенітету та ШІ-суверенітету як нових вимірів геополітичної конкуренції в умовах деглобалізації.

Результати дослідження.

Загострення геополітичної конкуренції у цифровій сфері активізувало академічні та політичні дискусії навколо понять технологічного (technological sovereignty) та цифрового суверенітету (digital sovereignty), які потребують концептуального уточнення. Технологічний суверенітет є ширшим поняттям і охоплює прагнення держави до стратегічної автономії у критично важливих для сучасного розвитку технологіях. Йдеться про здатність до власних наукових досліджень і розробок (R&D), внутрішнього виробництва ключових компонентів та формування незалежної технологічної політики, яка дозволяє забезпечувати базові внутрішні сервіси без зовнішньої залежності. Цифровий суверенітет

часто розглядається як складова або інструмент технологічного суверенітету. Його основними характеристиками є контроль над цифровою сферою на фізичному рівні (ресурси, інфраструктура, пристрої), на рівні коду (стандарти, правила, дизайн) і на рівні інформації (контент, дані) (Falkner et al., 2023). Цифровий суверенітет визначається як здатність держави самостійно контролювати та керувати власною цифровою інфраструктурою, хмарними сервісами, платформами й даними відповідно до національного законодавства та ціннісних орієнтирів. Це передбачає юрисдикцію в кіберпросторі, захист цифрових прав, регулювання діяльності платформ, посилення режимів кібербезпеки та впровадження обмежень щодо діяльності іноземних технологічних компаній (Fleming, 2025).

Зростання значення ШІ для сучасної геополітичної конкуренції зумовлює виокремлення поняття суверенного ШІ або ШІ-суверенітету (sovereign AI). У вітчизняному дискурсі також використовується термін AI-суверенітет (Мінцифри розвиватиме інфраструктуру для впровадження ШІ, 2025). ШІ-суверенітет передбачає прагнення держави до контролю над технологіями ШІ та пов'язаними з ними даними на всіх етапах – від розробки й навчання до впровадження. На практиці він охоплює дві взаємопов'язані складові. Перша – суверенітет над ШІ, тобто стратегічне прагнення розвивати й контролювати власну обчислювальну інфраструктуру, технології та дані як передумову незалежної цифрової політики. Друга – суверенітет через ШІ, коли ШІ-інструменти стають засобом посилення державного суверенітету в традиційних сферах: безпеці, економіці, державному управлінні та захисті культурної ідентичності (Turbovov, 2025).

Постає питання меж і можливостей цифрового суверенітету. Спроба класифікувати типи національного цифрового суверенітету реалізується через виокремлення чотирьох моделей: моделі, що базується на правах (rights-based model), ринково-орієнтованої моделі (market-oriented model), моделі централізації (centralisation model) та державної моделі (state-based model) (Fratini et al., 2024). Кожна з цих моделей відрізняється за пріоритетами, методами регулювання та співвідношенням ролей держави, ринку й прав громадян, а також має різну управлінську ефективність щодо реагування на виклики й ризики, зумовлені технологічним прогресом, геополітичними змінами та еволюцією суспільних норм. Кожна з них має свої переваги та недоліки. Розглянемо їх детальніше.

Модель, що базується на правах, забезпечує відносний баланс між правами й ризиками, однак може бути недостатньо гнучкою. ЄС є прикладом застосування такої моделі. Основними сферами формування цифрової політики ЄС є політика у сфері ШІ, хмарних технологій, конкуренції, авторського

права, регулювання цифрових фінансів, промислова політика, регулювання інтернет-контенту та встановлення цифрових стандартів. У межах цієї моделі пріоритет надається правам громадян і поєднанню вільного обігу даних із суворим захистом приватності. Європейський регламент GDPR (General Data Protection Regulation) та AI Act є спробами встановлення глобальних стандартів, що базуються на певних цінностях, фактично експортуючи регуляторний вплив ЄС. Модель передбачає обмеження влади платформ (штрафи, контентна відповідальність) і розвиток власної інфраструктури (проєкт GAIA-X) для зменшення залежності від іноземних технологічних корпорацій.

Ринково-орієнтована модель стимулює інновації, проте є слабшою у сфері захисту прав громадян і протидії монополіям. Основним прикладом її застосування є США, які автори називають «архетиповим» випадком. До цієї моделі також тяжіють Велика Британія, Японія та Австралія. Її пріоритетами є економічне зростання, інновації та активне просування власних цифрових продуктів, норм і стандартів на міжнародній арені. Захист прав часто поступається економічним інтересам, а наголос робиться на саморегулюванні бізнесу. Державне втручання мінімальне й здебільшого спрямоване на підтримку національних технологічних компаній. Водночас принцип невтручання поступається логіці національної безпеки: якщо діяльність іноземних компаній або використання іноземних технологій оцінюються як загроза, вони можуть бути обмежені чи заборонені (наприклад, TikTok або Huawei у США).

Модель централізації передбачає державний контроль над цифровим простором і можливе обмеження прав громадян. Досягнення національної безпеки забезпечується шляхом витіснення іноземних платформ, підтримки національних аналогів, цензури, фільтрації контенту, обмеження доступу до інтернету, локалізації даних тощо. Очевидним є прагнення відтворити фізичні кордони у цифровому просторі. Прикладами реалізації цієї моделі є Росія, Іран, Білорусь, В'єтнам і Бангладеш.

Державна модель реалізується в КНР. Їй притаманне органічне зростання цифрової сфери у тісному симбіозі з державним апаратом і досягнення цифрової самодостатності. Цифровізація постає інструментом державотворення, економічного зростання та геополітичного впливу. Чітко визначено ідеологічну й політичну роль КПК у формуванні цифрового середовища. Питання національної безпеки розглядаються крізь призму глобального лідерства. Розвиток власних технологій є основою цифрового суверенітету, тому значні державні інвестиції спрямовуються на пріоритетні технології, розвиток ШІ та захист кіберпростору.

Жодна з чотирьох моделей не демонструє оптимального балансу між всебічним регулюванням

цифрових технологій і достатнім рівнем підтримки інновацій та реагування на соціальні й економічні зміни. Автори пропонують модель «надійного управління» (robust governance) як оптимальну для реагування на турбулентність цифрової епохи – технологічні зрушення та геополітичні трансформації (Fratini et al., 2024). Вона поєднує переваги перелічених моделей і мінімізує їхні ризики, однак постає питання можливості її практичної реалізації.

Реалізація будь-якої з моделей є тривалим, комплексним і ресурсомістким процесом. Ілюстрацією цього може слугувати проєкт Програми дій Європейської комісії, спрямованої на досягнення цифрового суверенітету, очікувана вартість якого становить близько 3,6 трильйона євро. Водночас такий стратегічний курс, що передбачає обмеження або відмову від використання американських технологій, потребує формування складної мережі стратегічних альянсів і партнерств.

Окремої уваги заслуговує сфера ШІ, розвиток якої потребує значних інвестицій. Американські технологічні компанії концентрують у своїй структурі провідних дослідників з усього світу та щорічно спрямовують мільярди доларів на дослідження й розробки. Показовим прикладом є те, що лише на інфраструктуру для ШІ компанія Meta витратила понад 30 мільярдів доларів у 2024 році. Для досягнення паритету з технологічними можливостями великих американських корпорацій у сфері хмарних обчислень і ШІ Європейському Союзу, за оцінками, необхідно інвестувати щонайменше 500 мільярдів євро протягом наступного десятиліття (Lundblad, 2025).

Питання цифрового суверенітету набувають особливого значення в контексті країн із економіками, що розвиваються, зокрема Індії. Тут подібні стратегічні заходи часто інтерпретуються як відповідь на явища, які визначаються термінами «цифровий імперіалізм» або «цифровий колоніалізм». Ці поняття описують домінування західних, передусім американських, технологічних корпорацій у країнах Глобального Півдня, що, на думку низки дослідників, призводить до нових форм гегемонії та економічної експлуатації (Pohle, Thiel, 2020). Водночас такі ініціативи викликають скептицизм з боку деяких західних держав, де їх часто трактують як прояв «цифрового протекціонізму» – навмисного створення бар'єрів для вільної цифрової торгівлі.

Підкреслимо, що для лідера цифрового розвитку – США – характерним є активне просування власних цифрових продуктів, норм і стандартів на міжнародній арені, що, своєю чергою, спричиняє проблематизацію концепту цифрового суверенітету. Деякі дослідники трактують цифровий суверенітет як синонім обмежувальної політики (Pohle, Thiel, 2020). У такій інтерпретації широкий спектр заходів – від цензури та фільтрації контенту до вимог щодо локалізації

даних і спеціальних режимів інтелектуальної власності, спрямованих на протидію дезінформації або захист приватності, – може розглядатися як потенційно протекціоністський. Отже, дискурс навколо цифрового суверенітету, технологічного суперництва та протекціонізму відображає глибші політико-економічні розбіжності між різними акторами глобальної цифрової екосистеми.

У цьому контексті захист культурної ідентичності постає ключовою складовою концепції суверенного ШІ, набуваючи особливої значущості. Йдеться вже не лише про технологічну автономію, а й про розвиток та імплементацію ШІ, який інтегрує національні цінності, правові норми, мовну специфіку та культурну спадщину, виходячи за межі технічних стандартів, домінуючих у глобалізованих моделях. Показовим прикладом реалізації такого підходу є ініціатива LatAmGPT, спрямована на створення першої великої мовної моделі для Латинської Америки, що враховує лінгвістичні діалекти, культурні аліюзи та історичні контексти регіону, які переважно ігноруються в англомовних тренувальних даних. Цей випадок демонструє, що концепція суверенного ШІ може трансцендувати технократичні завдання та перетворюватися на інструмент культурного відродження (Лакомов, 2025). Подібне розширення цілей цифрового суверенітету – від економічного й технологічного захисту до культурного самовизначення – додатково ускладнює аналіз співвідношення між відкритістю та протекціонізмом у міжнародній цифровій політиці.

Порівняльний аналіз підходів США, КНР та ЄС до цифрового суверенітету засвідчує їхній системний вплив на трансформацію глобального цифрового порядку в умовах деглобалізації та посилення нормативно-ціннісної поляризації. Геополітизація технологій, що проявляється у стратегічному значенні вибору цифрової інфраструктури, стандартів зв'язку та архітектур ШІ, зумовлює переосмислення технологічних рішень як елементів зовнішньополітичної та безпекової стратегії держав. Інституційна та регуляторна дивергенція між провідними акторами спричиняє багатовимірну фрагментацію глобального цифрового простору, в межах якої універсалістська модель глобального управління поступається конкуренції альтернативних нормативних режимів – ліберального (США), ціннісно-регуляторного (ЄС) та державоцентричного (КНР). У цьому контексті концепція цифрового суверенітету еволюціонує від нормативного ідеалу автономії до парадигми «резильєнтної взаємозалежності» (resilient interdependence) (Brunet, 2026), що передбачає поєднання стратегічної самодостатності з вибірковою інтеграцією в глобальні технологічні ланцюги. Відтак цифровий і ШІ-суверенітет постають не як статичні категорії, а як динамічні політико-економічні конструкції, що потребують формування

диференційованих державних стратегій, спрямованих на мінімізацію асиметричних залежностей і водночас на інституціоналізацію контрольованих форм міжнародної кооперації.

Зауважимо, що в Україні у відповідь на геополітичні виклики реалізується проєкт «AI Factory». Міністерство цифрової трансформації України створює суверенну фабрику штучного інтелекту – AI Factory. Проєкт передбачає розбудову сучасної національної цифрової інфраструктури для запуску державних ШІ-сервісів. Власна інфраструктура розглядається як основа цифрового суверенітету України, суверенітету ШІ та захисту даних. AI Factory спрямована на досягнення технологічної незалежності держави, забезпечення повного контролю над даними та захист критично важливої інформації. Проєкт включає технологічне обладнання, програмне забезпечення, суверенні дата-центри, а також програми підготовки технічних фахівців, які створюватимуть і впроваджуватимуть ШІ-продукти для державного управління та оборонної сфери (Мінцифри розвиватиме інфраструктуру для впровадження ШІ, 2025).

В інформаційних матеріалах про AI Factory особлива увага приділяється захисту даних. Із розвитком ШІ захист персональних даних громадян стає дедалі актуальнішим завданням для держав. У цьому контексті формується окреме поняття суверенітету даних (data sovereignty), яке охоплює контроль над обробкою, зберіганням і переміщенням даних, а також регулювання транскордонних потоків інформації. Значення даних зросло настільки, що концепт суверенітету даних набуває самостійного теоретичного статусу. Зокрема, він був окремо актуалізований на першому European Summit on Digital Sovereignty (Берлін/Мюнхен, 17 листопада 2025 р.) (Focus on digital sovereignty in Europe, 2025). Створення суверенної та безпечної інфраструктури даних Gaia-X покликане захистити дані громадян ЄС від зовнішньої юрисдикції. Водночас вільний потік даних є необхідною умовою функціонування інноваційної економіки. Відповіддю на це внутрішнє напруження стала концепція «вільного потоку даних із довірою» (Data Free Flow with Trust, DFFT), запропонована Японією у 2019 році на Всесвітньому економічному форумі в Давосі та надалі розвинена в низці міжнародних документів. Сьогодні експертна спільнота DFFT у межах Організації економічного співробітництва та розвитку (OECD) шляхом поінформованого діалогу сприяє виробленню політичних відповідей на виклики транскордонного руху даних, ідентифікації тенденцій і формуванню нових напрямів політики у сфері даних (Moving forward on data free flow with trust, 2023).

Висновки.

Цифровий суверенітет і ШІ-суверенітет у контексті деглобалізації набувають статусу

структурних чинників трансформації міжнародних відносин і дедалі більше визначають логіку сучасної геополітичної конкуренції. Вони виходять за межі техніко-економічних параметрів і постають як комплексні політико-інституційні конструкції, що поєднують виміри безпеки, економічної спроможності, нормативного впливу та культурної репрезентації.

Технологічний суверенітет, цифровий суверенітет, суверенний ШІ та суверенітет даних формують ієрархічно взаємопов'язану систему, в межах якої ключовою характеристикою є напруга між прагненням до стратегічної автономії та об'єктивною необхідністю глобальної взаємозалежності. Конкуренція між моделями цифрового суверенітету США, ЄС і КНР зумовлює регуляторну дивергенцію та фрагментацію глобального цифрового простору, що супроводжується геополітизацією технологій і формуванням альтернативних нормативних режимів управління цифровими процесами.

У такій конфігурації цифровий суверенітет доцільно інтерпретувати не як ізоляціоністську практику, а як динамічний процес балансування між стратегічною самодостатністю та вибірковою інтеграцією в глобальні технологічні мережі. Парадигма «резильєнтної взаємозалежності»

дозволяє концептуалізувати цифровий суверенітет як здатність держави мінімізувати критичні залежності, зберігаючи доступ до інноваційних ресурсів і транснаціональних потоків даних.

Для України цифровий і ШІ-суверенітет набувають особливого значення в умовах в умовах повномасштабної війни, гібридних загроз і трансформації глобального технологічного середовища. Контроль над національною цифровою інфраструктурою, даними та алгоритмічними системами постає передумовою забезпечення кіберстійкості, обороноздатності та інформаційної безпеки. Розвиток власних ШІ-технологій і суверенної цифрової інфраструктури сприяє зменшенню вразливості до зовнішнього тиску, підвищенню інституційної автономії та формуванню спроможності держави до стратегічного управління в умовах технологічної невизначеності.

Отже, цифровий і ШІ-суверенітет постають як багатовимірні політико-економічні конструкції, що визначають конфігурацію майбутнього глобального цифрового порядку. Здатність держав, зокрема України, інтегрувати технологічну автономію з міжнародною кооперацією стає ключовою умовою їхньої безпеки, стійкості та конкурентоспроможності в цифрову епоху.

БІБЛІОГРАФІЧНІ ПОСИЛАННЯ

- Калайда, Ю. П. (2021). Забезпечення цифрового суверенітету в умовах геополітичного протистояння: кращі практики зарубіжного досвіду. *Інформація і право*. № 2 (37). [https://doi.org/10.37750/2616-6798.2021.2\(37\).238363](https://doi.org/10.37750/2616-6798.2021.2(37).238363)
- Калужна, Ю. І. (2025). Цифровий суверенітет як фактор національної безпеки ЄС та України. *Національні інтереси України*. № 6/11. 1094 - 1124. https://www.researchgate.net/publication/393363261_Cifrovij_suverenitet_ak_faktor_nacionalnoi_bezpeki_ES_ta_Ukraini
- Лакомов, В. (2025). Суверенний штучний інтелект: між свободою і пам'яттю. *Фонд "Демократичні ініціативи імені Ілька Кучеріва"*. 14 листопада. <https://dif.org.ua/article/suverenniy-shtuchnij-intelekt-mizh-svobodoju-i-pamyattju>
- Милосердна, І. М. (2024). Цифровий суверенітет держави: наукова риторика та реальні зміни. *Науковий журнал "Політикус"*. Вип. 6. 154 - 160. http://politicus.od.ua/6_2024/25.pdf
- Мінцифри розвиватиме інфраструктуру для впровадження ШІ у державні сервіси - працюємо над AI Factory (2025). *Урядовий портал*. 7 серпня. <https://www.kmu.gov.ua/news/mintsyfyry-rozvyvaytyme-infrastrukturu-dlia-vprovadzhenia-shi-u-derzhavni-servisy-pratsuiemo-nad-ai-factory>
- Brunet, K. (2026). Why the race for tech sovereignty is a balancing act. *World Economic Forum*. 13 Jan. <https://www.weforum.org/stories/2026/01/race-for-tech-sovereignty-is-a-balancing-act/>
- Falkner G., Heidebrecht S., Obendiek A., & Seidl T. (2024). Digital sovereignty - Rhetoric and reality. *Journal of European Public Policy*. Vol. 31. 2099 - 2120. <https://doi.org/10.1080/13501763.2024.2358984>
- Fleming S. (2025). What is digital sovereignty and how countries approaching it? *World Economic Forum*. 10 Jan. <https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/>
- Focus on digital sovereignty in Europe: Gaia-X as a central topic at the 2025 Digital Summit. (2025). *Press Releases*. November 17. <https://gaia-x.eu/focus-on-digital-sovereignty-in-europe-gaia-x-as-a-central-topic-at-the-2025-digital-summit/>
- Fratini, S., Hine, E., Novelli, C. et al. (2024). Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models. *DISO*. 3, 59. <https://doi.org/10.1007/s44206-024-00146-7>
- Kornprobst, M., & Wallace, J. (2025). What is deglobalization? *Chatham House*. 8 January. <https://www.chathamhouse.org/2021/10/what-deglobalization>
- Lundblad, N. (2025). Digital Sovereignty: Can Europe Afford IT? *The Center for European Policy Analysis*. October 29. <https://cepa.org/article/digital-sovereignty-can-europe-afford-it/>
- Moving forward on data free flow with trust: New evidence and analysis of business experiences (2023). *OECD Digital Economy Papers*. No. 353, OECD Publishing, Paris. <https://doi.org/10.1787/1afab147-en>
- Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*. Vol. 9. Issue 4. <https://policyreview.info/concepts/digital-sovereignty>
- Turobov, A. (2025). What does AI sovereignty for the UK involve? *Bennett School of Public Policy*. Cambridge. 16 oct. <https://www.bennettschool.cam.ac.uk/blog/what-does-ai-sovereignty-for-the-uk-involve>

REFERENCES

- Brunet, K. (2026). Why the race for tech sovereignty is a balancing act. *World Economic Forum*. 13 Jan. <https://www.weforum.org/stories/2026/01/race-for-tech-sovereignty-is-a-balancing-act/>
- Falkner, G., Heidebrecht, S., Obendiek, A., & Seidl, T. (2024). Digital sovereignty - Rhetoric and reality. *Journal of European Public Policy*. Vol. 31. 2099 - 2120. <https://doi.org/10.1080/13501763.2024.2358984>
- Fleming S. (2025). What is digital sovereignty and how countries approaching it? *World Economic Forum*. 10 Jan. <https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/>
- Focus on digital sovereignty in Europe: Gaia-X as a central topic at the 2025 Digital Summit. (2025). *Press Releases*. November 17. <https://gaia-x.eu/focus-on-digital-sovereignty-in-europe-gaia-x-as-a-central-topic-at-the-2025-digital-summit/>
- Fratini, S., Hine, E., Novelli, C. *et al.* (2024). Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models. *DISO*. 3, 59. <https://doi.org/10.1007/s44206-024-00146-7>
- Kalayda, Y. P. (2021). Ensuring Digital Sovereignty in the Context of Geopolitical Confrontation: Best Practices of Foreign Experience. *Information and Law*, No. 2 (37). [https://doi.org/10.37750/2616-6798.2021.2\(37\).238363](https://doi.org/10.37750/2616-6798.2021.2(37).238363)
- Kaliuzhna, Y. I. (2025). Digital Sovereignty as a Factor of National Security for the EU and Ukraine. *National Interests of Ukraine*, No. 6/11, pp. 1094–1124. [https://doi.org/10.52058/3041-1793-2025-6\(11\)](https://doi.org/10.52058/3041-1793-2025-6(11))
- Kornprobst, M., & Wallace, J. (2025). What is deglobalization? *Chatham House*. 8 January. <https://www.chathamhouse.org/2021/10/what-deglobalization>
- Lakomov, V. (2025). Sovereign Artificial Intelligence: Between Freedom and Memory. Ilko Kucheriv Democratic Initiatives Foundation, November 14. Retrieved from <https://dif.org.ua/article/suverennyi-shtuchnyi-intelekt-mizh-svobodoyu-i-pamyattyu>
- Lundblad N. (2025). Digital Sovereignty: Can Europe Afford IT? *The Center for European Policy Analysis*. October 29. <https://cepa.org/article/digital-sovereignty-can-europe-afford-it/>
- Moving forward on data free flow with trust: New evidence and analysis of business experiences (2023). *OECD Digital Economy Papers*. No. 353, OECD Publishing, Paris. <https://doi.org/10.1787/1afab147-en>.
- Myloserdna, I. M. (2024). Digital Sovereignty of the State: Scientific Rhetoric and Real Changes. *Politicus Scientific Journal*, Issue 6, pp. 154–160. <https://doi.org/10.24195/2414-9616.2024-6.23>
- Pohle J., Thiel T. (2020). Digital sovereignty. *Internet Policy Review*. Vol. 9. Issue 4. <https://doi.org/10.14763/2020.4.1532>
- The Ministry of Digital Transformation Will Develop Infrastructure for the Implementation of AI in Public Services – We Are Working on the AI Factory (2025). *Government Portal*, August 7. <https://www.kmu.gov.ua/news/mintsyfry-rozvyvatyme-infrastrukturu-dlia-vprovadzhennia-shi-u-derzhavni-servisy-pratsiuemo-nad-ai-factory>
- Turobov A. (2025). What does AI sovereignty for the UK involve? *Bennett School of Public Policy*. Cambridge. 16 oct. <https://www.bennettschool.cam.ac.uk/blog/what-does-ai-sovereignty-for-the-uk-involve>