МІЖНАРОДНІ ВІДНОСИНИ

INTERNATIONAL RELATIONS

EMPIRIO
SCIENTIFIC JOURNAL

EMPIRIO 3, № 2 (2026)

https://doi.org/10.18523/3041-1718.2026.3.2.29-39
УДК 327(4-672ЄС):004

Данило Непочатов
Аспірант,
спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»,
кафедра міжнародних відносин і політичної філософії,
Харківський національний економічний університет імені Семена Кузнеця, Україна
https://orcid.org/0009-0006-5819-5842
danylo.nepochatov@hneu.net

ЦИФРОВИЙ СУВЕРЕНІТЕТ ЯК ЗОВНІШНЬОПОЛІТИЧНИЙ ПРОЄКТ ЄС: РЕГУЛЯТОРНІ ІНСТРУМЕНТИ ТА КІБЕРДИПЛОМАТІЯ

У статті досліджено цифровий суверенітет Європейського Союзу як стратегічний проєкт, спрямований на подолання аутсайдерства у світі в умовах технологічної залежності від США та КНР. Виявлено прогалину в науковому дискурсі щодо системного зв'язку між внутрішнім регулюванням ЄС та його зовнішньополітичною активністю. Європейську цифрову незалежність розглянуто через призму трьох взаємопов'язаних вимірів: суверенітету даних (контроль над транскордонними потоками та юрисдикція), технологічної автономії (подолання інфраструктурної залежності) та нормативної ваги єдиного європейського ринку.

Наукова новизна дослідження полягає в обґрунтуванні двофазної трансмісійної моделі, яка пояснює механізм конвертації нормативної влади ЄС у геополітичний вплив. Перша фаза описує односторонній регуляторний експорт через Брюссельський ефект: ринкова вага ЄС змушує глобальних гравців імплементувати європейські стандарти (GDPR, AI Act). Друга фаза — багатостороння кібердипломатія — активується, коли ринкова логіка вичерпує свої можливості, дозволяючи ЄС використовувати регуляторні прецеденти (наприклад, рішення Суду ЄС у справі Schrems II) як дипломатичні аргументи на міжнародних майданчиках (G7, OEWG).

Доведено, що за умов дефіциту інфраструктурної потужності («поетичної влади») ЄС компенсує її нарощуванням «кібернетичної влади» — спроможності встановлювати правила гри.

Методологічною базою дослідження є системний підхід і метод кейс-стаді (аналіз бразильського LGPD та корпоративних політик Big Tech).

Зроблено висновок, що цифровий суверенітет ЄС є моделлю «регуляторної дипломатії за замовчуванням», завдяки якій Європейський Союз зберігає суб'єктність у глобальному технологічному протистоянні.

Ключові слова: цифровий суверенітет, кібердипломатія, Брюссельський ефект, Пекінський ефект, технологічна автономія, ЄС, штучний інтелект.

Постановка проблеми. Глобальне геополітичне суперництво між Сполученими Штатами і Китаєм набуває особливої гостроти в кіберпросторі та сфері цифрових технологій. Через надмірну політизацію та перманентну конкуренцію цей простір перетворився на те, що Лукас Келло охарактеризував як стан «немиру» — ситуацію, яка не сягає масштабів відкритої війни, але й однозначно не є миром[1]. В умовах такого жорсткого протистояння Європейський Союз виявився вразливим: через брак власних технологічних компаній у цифровому вимірі ЄС утворився «стратегічний вакуум»[2]. Оскільки цю порожнечу швидко заповнили американські Big Tech компанії, Євросоюз розпочав боротьбу за статус стратегічного актора в глобальному технологічному протистоянні.

Цей вакуум особливо відчутний в економічному і технологічному вимірах. Згідно з консенсусом провідних міжнародних інституцій, цифрові технології та потоки даних є фундаментальним драйвером економічного зростання у XXI столітті: за оцінкою ЮНКТАД, до 2033 року цифрова економіка разом із технологічним сектором досягне 5 трлн дол. США[3]. З огляду на те, що цифрові платформи та штучний інтелект формуватимуть левову частку доданої вартості глобального ВВП у наступному десятилітті, відставання ЄС у розбудові власної інфраструктури становить пряму загрозу його геополітичній суб'єктності. Показовою є оцінка Центру Белфера при Гарвардському університеті: у сфері критичних та новітніх технологій ЄС посідає лише третє місце (41,6 пункту), суттєво поступаючись США (84,1) та КНР (66,9)[4]. Залежність від зовнішніх постачальників є структурною, наприклад, на Amazon, Microsoft та Google припадає близько 70 % хмарного ринку ЄС, а загалом Союз залежить від третіх країн у понад 80 % своїх цифрових продуктів, послуг, інфраструктури та інтелектуальної власності[5].

Саме це технологічне відставання і є ключем до розуміння регуляторної стратегії ЄС. Італійський філософ Лучано Флоріді концептуалізував цю асиметрію через дихотомію двох форм цифрової влади. «Кібернетична влада» (*cybernetic power*) — це здатність регулювати, контролювати та встановлювати правила цифрового простору. «Поетична влада» (*poietic power*) — це здатність самостійно створювати цифрову інфраструктуру, платформи і технології[6]. США і КНР володіють обома формами влади одночасно, ЄС — лише першою.

Не маючи власних технологічних гігантів, підводних кабелів, що конкурують із американськими, чи виробничих потужностей, порівнянних із китайськими, Євросоюз обрав єдину доступну йому асиметричну відповідь: компенсувати дефіцит «поетичної влади» нарощуванням «кібернетичної». З цієї причини випливає справжній бум нормотворення 2018–2025 років та ухвалення документів: GDPR, DSA, DMA, AI Act, Chips Act. Така регуляторна активність є спробою вижити та відстояти суверенітет технологічно залежного актора, який не може перемогти в цих перегонах. До того ж за бажанням Євросоюзу бути світовим технологічним лідером криється глибша проблема — страх, що за умов тотальної інфраструктурної залежності від США та КНР він втратить саму здатність розвивати технології за власними правилами, які передбачають повагу до прав людини та верховенства права. Якщо цифрова інфраструктура Євросоюзу залишатиметься переважно американською чи китайською, правила користування нею визначатимуть Вашингтон або Пекін, а не Брюссель. Такий сценарій може призвести до системної загрози демократичній суб'єктності ЄС, тому нормотворча активність 2018–2025 років є спробою закріпити демократичні стандарти в цифровому просторі.

---

1 Lucas Kello, *Striking Back: The End of Peace in Cyberspace – And How to Restore It* (Yale University Press, 2022), https://doi.org/10.2307/j.ctv2v55b54.

2 Tobias Liebetrau, "Cyber Conflict Short of War: A European Strategic Vacuum," *European Security* 31, no. 4 (2022): 497–516, https://doi.org/10.1080/09662839.2022.2031991.

3 United Nations Conference on Trade and Development, *Digital Economy Report* (2024), https://unctad.org/system/files/official-document/der2024_en.pdf.

4 "Critical and Emerging Technologies Index T," with The Belfer Center for Science and International Affairs, June 5, 2025, https://www.belfercenter.org/critical-emerging-tech-index.

5 Vaida Gineikyte-Kanclere et al., *European Software and Cyber Dependencies* (2025).

6 Luciano Floridi, "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU," *Philosophy & Technology* 33, no. 3 (2020): 369–78, https://doi.org/10.1007/s13347-020-00423-6.

Окрім конкуренції із КНР та США, ЄС також занепокоєний низкою безпекових подій у кіберпросторі: кібернападом Росії на Естонію у 2007 році; справою Едварда Сноудена, яка підважила довіру до спроможності США забезпечити технологічну співпрацю відповідно до цінностей Євросоюзу; пандемією COVID-19, яка оголила вразливість ланцюгів постачання технологій; та повномасштабним вторгненням Росії в Україну, що остаточно надало питанням кіберстійкості безпекового виміру.

Світові компанії та країни не можуть нехтувати новим європейським законодавством у техносфері, адже ВВП на душу населення в ЄС (43 тис. дол. США) за населення 448 млн робить його одним із найпривабливіших ринків у світі — і саме ця ринкова вага перетворює внутрішнє законодавство на зовнішньополітичний інструмент. Коли транснаціональні корпорації змушені адаптуватися до європейських норм, щоб зберегти доступ до цього ринку, треті країни копіюють регламенти ЄС як еталонну модель, а країни G7 визначили стандарти AI Act основою міжнародного Кодексу поведінки з розвитку ШІ, що прямо свідчить, що регуляторна архітектура виконує функцію кібердипломатії. Саме так ЄС намагається утриматись у світі технодомінування США та Китаю: не через симетричну конкуренцію в інфраструктурних перегонах, яку він програє, а через встановлення нормативних правил, які відповідають його цінностям і поширюються далеко за межі його кордонів.

Водночас системний зв'язок між цією внутрішньою регуляторною архітектурою та кібердипломатичною діяльністю ЄС на міжнародних майданчиках залишається концептуально недоопрацьованим, зокрема механізм двофазної трансмісії, за якої внутрішнє нормотворення спочатку формує регуляторний експорт, а потім активує кібердипломатичну діяльність саме там, де ринкова логіка вичерпує свої можливості. Ізольоване дослідження цих двох вимірів призводить до нерозуміння кібердипломатичної стратегії ЄС та недостатнього усвідомлення ролі Брюссельського ефекту.

Аналіз останніх досліджень і публікацій. За останні кілька років багато дослідників звертались до проблематики цифрового суверенітету та кібердипломатії. Її можна поділити на три взаємопов'язані напрями.

Перший напрям — концептуальне осмислення цифрового суверенітету як проблеми контролю над даними, інфраструктурою та технологічними ланцюгами. Зокрема, Ю. Полє та Т. Тіль розглядають цифровий суверенітет не лише як техніко-правову категорію, а й як політично навантажене поняття, що по-різному інтерпретується в демократичних та авторитарних моделях цифрового врядування[7]. Їхній підхід важливий для цієї статті, оскільки дає змогу показати ціннісний розрив між європейським розумінням цифрового суверенітету, заснованим на верховенстві права та правах людини, і авторитарними моделями, які тяжіють до державного контролю над інформаційним простором. У межах цього ж напряму Л. Флоріді акцентує увагу на технологічній залежності ЄС і розмежовує різні форми цифрової влади, вказуючи на дефіцит інфраструктурних потужностей Євросоюзу[8]. Це дає змогу розглядати цифровий суверенітет і як нормативний та правовий проєкт, і як питання матеріальної спроможності контролювати критичні цифрові ресурси.

Другий напрям досліджень пов'язаний із нормативною владою Європейського Союзу та екстратериторіальним впливом його правових стандартів. Центральною для цього напряму є концепція Брюссельського ефекту, розроблена А. Бредфорд. Дослідниця показує, що ЄС здатен поширювати власні стандарти за межі своєї території не стільки через класичний примус, скільки через регуляторну вагу єдиного ринку, доступ до якого залишається критично важливим для транснаціональних компаній. У цій логіці внутрішні норми ЄС можуть набувати глобального значення, оскільки компанії адаптують свої практики до європейських правил, навіть якщо вони працюють поза межами Союзу[9]. Водночас М. Ері та Т. Штрайнц, аналізуючи Пекінський ефект, пропонують альтернативну оптику для розуміння цифрового впливу КНР, що ґрунтується

[7] Julia Pohle et al., "Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices," *Policy & Internet* 16, no. 4 (2024): 666–71, https://doi.org/10.1002/poi3.437.

[8] Floridi, "The Fight for Digital Sovereignty."

[9] Anu Bradford, "The Brussels Effect," in *The Brussels Effect*, 1st ed., by Anu Bradford (New York: Oxford University Press, 2012), 25–66, https://doi.org/10.1093/oso/9780190088583.003.0003.

на інфраструктурному експорті, цифровому шовковому шляху та просуванні китайської моделі транснаціонального управління даними[10]. Порівняння підходів Бредфорд, Ері та Штрайнца дає змогу чіткіше побачити, що цифровий суверенітет є інструментом глобальної конкуренції різних моделей цифрового порядку.

Третій напрям досліджень розкриває геополітичний вимір цифрової взаємозалежності та значення мережевих структур у сучасній міжнародній політиці. Г. Фаррелл та А. Ньюман у концепції озброєної взаємозалежності показують, що держави та інтеграційні об'єднання, які контролюють ключові вузли глобальних економічних та інформаційних мереж, здатні використовувати ці позиції для політичного впливу[11]. Для аналізу цифрового суверенітету ЄС ця концепція важлива, оскільки дає змогу пояснити, як регуляторні, ринкові та інфраструктурні переваги можуть перетворюватися на зовнішньополітичний ресурс. За такого розгляду ЄС постає як суб'єкт, що використовує власний ринок, правові стандарти та інституційну спроможність як вузлові точки впливу в глобальному цифровому середовищі.

Водночас залишається важлива аналітична прогалина, адже наявні дослідження не дають цілісного пояснення того, як саме внутрішня регуляторна архітектура ЄС трансформується в зовнішньополітичний вплив через кібердипломатію. Саме тому в цій статті увагу зосереджено на зв'язку між внутрішнім цифровим нормотворенням ЄС, регуляторним експортом і багатосторонньою кібердипломатією як взаємопов'язаними елементами цифрового суверенітету.

Методологічною основою дослідження є системний підхід, який дає змогу розглядати цифровий суверенітет ЄС як інтегрований зовнішньополітичний проєкт. Нормативно-правовий та документальний аналіз застосовано для реконструкції першої фази трансмісійної моделі через вивчення базових регуляторних актів ЄС (GDPR, DSA, DMA, AI Act, Chips Act) та їхньої здатності формувати глобальні стандарти. Порівняльний метод використано для концептуального розмежування європейської демократичної моделі відкритого цифрового суверенітету та китайського технонаціоналізму (Пекінський ефект), що дає змогу визначити межі Брюссельського ефекту. Саме там, де він вичерпує свої можливості, активується кібердипломатичний вимір. Для практичної верифікації другої фази трансмісійної моделі залучено метод кейс-стаді: оцінювання наслідків рішення Суду ЄС у справі *Schrems II* та його конвертації в дипломатичний аргумент у межах OEWG, імплементації європейських норм транснаціональними корпораціями (Facebook, Microsoft) та екстратериторіального впливу на законодавство третіх країн (бразильський LGPD).

Мета статті — дослідити цифровий суверенітет як інтегрований зовнішньополітичний проєкт ЄС, що реалізується через два взаємозумовлені виміри: внутрішню регуляторну архітектуру та кібердипломатичну діяльність на міжнародній арені. Автор вважає, що внутрішнє регулювання ЄС цифрової та технологічної сфер стає вагомою дипломатичною стратегією, яка із застосуванням кібердипломатії дає змогу досягти геополітичних цілей на зовнішній арені.

Виклад основного матеріалу дослідження. Першою політичною відповіддю на описаний у постановці проблеми стратегічний вакуум стала промова Еммануеля Макрона в Сорбонні у вересні 2017 року: він уперше проголосив цифровий суверенітет одним із ключів майбутнього Європи[12]. Логічним продовженням цієї політичної візії стала інституційна переорієнтація Європейської комісії: у вересні 2020 року президентка Урсула фон дер Ляєн перетворила концепт цифрового суверенітету на офіційну стратегічну мету десятиліття, акцентувавши на необхідності розбудувати європейську хмарну інфраструктуру, стати лідером у просуванні етичних підходів функціонування штучного інтелекту та створити умови для безпечної цифрової ідентичності

[10] Matthew S. Erie and Thomas Streinz, *The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance*, 2021, https://www.nyujilp.org/wp-content/uploads/2022/02/NYUJILP_Vol54.1_Erie_Streinz_1-91.pdf.

[11] Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security* 44, no. 1 (2019): 42–79, https://doi.org/10.1162/isec_a_00351.

[12] Emmanuel Macron, "Initiative pour l'Europe – Discours d'Emmanuel Macron pour une Europe souveraine, unie, démocratique," elysee.fr, September 26, 2017, https://www.elysee.fr/emmanuel-macron/2017/09/26/initiative-pour-l-europe-discours-d-emmanuel-macron-pour-une-europe-souveraine-unie-democratique.

для всіх[13]. Згодом цей підхід операціоналізували в програмі «Цифровий компас», перевівши політичні заяви в площину конкретних інфраструктурних та нормативних індикаторів.

З аналізу нормативної бази 2018–2025 років пропонуємо виокремити три відмінних, хоча й взаємопов'язаних виміри розуміння цифрового суверенітету Євросоюзом, кожен із яких формує окремий шар регуляторної архітектури і слугує вхідним ресурсом для трансмісійної моделі.

Перший вимір — це суверенітет даних, який полягає у встановленні юрисдикції над персональними та промисловими даними, які генеруються на території ЄС, незалежно від місця їхньої фізичної обробки чи зберігання. Ключовим інструментом реалізації цієї стратегії є Загальний регламент про захист даних (*General Data Protection Regulation, GDPR*), зокрема його глава V, яка жорстко регламентує умови транскордонної передачі інформації[14]. Поворотним моментом у практичній площині стало рішення Суду ЄС у справі *Schrems II* (2020), яке скасувало механізм спеціальної правової бази, яка дозволяла американським компаніям отримувати та обробляти персональні дані мешканців Європейського Союзу — «Щит конфіденційності ЄС–США» — через несумісність американського законодавства про стеження з основоположними правами громадян ЄС. Це змусило Вашингтон реформувати власне законодавство та у 2023 році ухвалити новий рамковий договір «Механізм конфіденційності даних між ЄС та США», що продемонструвало спроможність Євросоюзу в односторонньому порядку блокувати трансатлантичні цифрові потоки, фактично нав'язуючи власні правові стандарти глобальним технологічним гравцям[15].

Другий вимір — це технологічна автономія, яка передбачає зменшення стратегічної залежності від позаєвропейських постачальників у критичних секторах. Як показує Л. Флоріді, дефіцит «поетичної влади» ЄС та структурна залежність від третіх країн змушує нарощувати «кібернетичну владу», яка проявляється в документах та програмах[16]: закон, спрямований на розвиток власної індустрії напівпровідників (Chips Act); ініціатива зі створення об'єднаної інфраструктури даних та хмарних обчислень (GAIA-X); розвиток ініціативи зі створення суперкомп'ютерів (EuroHPC); заходи з розвитку інфраструктури для телекомунікаційних мереж 5G. Регуляторну архітектуру технологічної автономності доповнюють регламент ЄС із посилення кібербезпеки (Cybersecurity Act) та AI Act, який став першим у світі комплексним регулюванням ШІ за принципом ризик-орієнтованого підходу, перетворивши ЄС на глобального першого кодифікатора в цій сфері.

Третій вимір — це нормативна вага єдиного ринку ЄС. Здатність Євросоюзу диктувати глобальні правила гри зумовлена тим, що цей економічний простір є надто привабливим, аби світові компанії його ігнорували. Оскільки розробляти окремий цифровий продукт для Європи та окремий для решти світу фінансово невигідно, транснаціональні корпорації застосовують європейські стандарти глобально. Яскравим прикладом цього є дія законів про цифрові послуги (DSA) та цифрові ринки (DMA). Встановлюючи жорсткі вимоги до прозорості алгоритмів, модерації контенту та обмеження монополій великих платформ, ці документи змушують технологічних гігантів змінювати саму архітектуру своїх продуктів. Отже, внутрішні європейські обмеження для компаній автоматично перетворюються на нову глобальну норму. Американська дослідниця Ану Бредфорд називає це явище Брюссельським ефектом: регулювання ЄС набуває екстратериторіального характеру[17]. Водночас нормативна потужність ЄС стикається із серйозним викликом — Пекінським ефектом. На відміну від регуляторного впливу Брюсселя, що діє через ринкову логіку, модель КНР ґрунтується на інфраструктурному експорті в межах програми «Цифровий шлях». Будуючи фізичні мережі та дата-центри по всьому світу, Китай де-факто впроваджує

---

[13] Ursula von der Leyen, "State of the Union 2020 – European Commission," 2020, https://commission.europa.eu/strategy-and-policy/state-union/state-union-2020_en.

[14] 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) (Text with EEA Relevance), 119 OJ L (2016), http://data.europa.eu/eli/reg/2016/679/oj.

[15] Hendrik Mildebrath, "The CJEU Judgment in the *Schrems II* Case," 2020, https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.

[16] Floridi, "The Fight for Digital Sovereignty."

[17] Bradford, "The Brussels Effect."

власну модель цифрового врядування, що тяжіє до державного контролю та авторитарних практик[18]. Така експансія перетворює конкуренцію цифрових стандартів із суто економічного процесу на арену геополітичного та ціннісного протистояння двох принципово різних моделей врядування. Саме як відповідь на цей виклик концепт цифрового суверенітету ЄС зазнав суттєвої еволюції. Якщо на початку 2020 року Єврокомісія розглядала його як прагматичний інструмент досягнення технологічної автономії, то Європейська декларація про цифрові права та принципи закріпила оновлену візію відкритого цифрового суверенітету, що перевело концепт із питання технологічної незалежності у стратегічний проєкт захисту демократичних цінностей і верховенства права в глобальному кіберпросторі як ціннісної альтернативи китайській моделі[19].

Проведений аналіз трьох вимірів — суверенітету даних, технологічної автономії та нормативної ваги ринку — дає змогу перейти до центрального питання дослідження: як ця внутрішня регуляторна архітектура трансформується в зовнішньополітичний вплив? Кожен із трьох вимірів формує окремий шар нормативного тиску, однак сукупно вони живлять єдину двофазну трансмісійну модель (див. рисунок). На нашу думку, цей процес реалізується через два послідовні та взаємозумовлені механізми — односторонній регуляторний експорт (Брюссельський ефект) та багатосторонню кібердипломатію. Причому каузальний зв'язок між ними асиметричний: другий механізм активується саме там, де перший натикається на структурне обмеження, перетворюючи регуляторні прецеденти на дипломатичні аргументи.

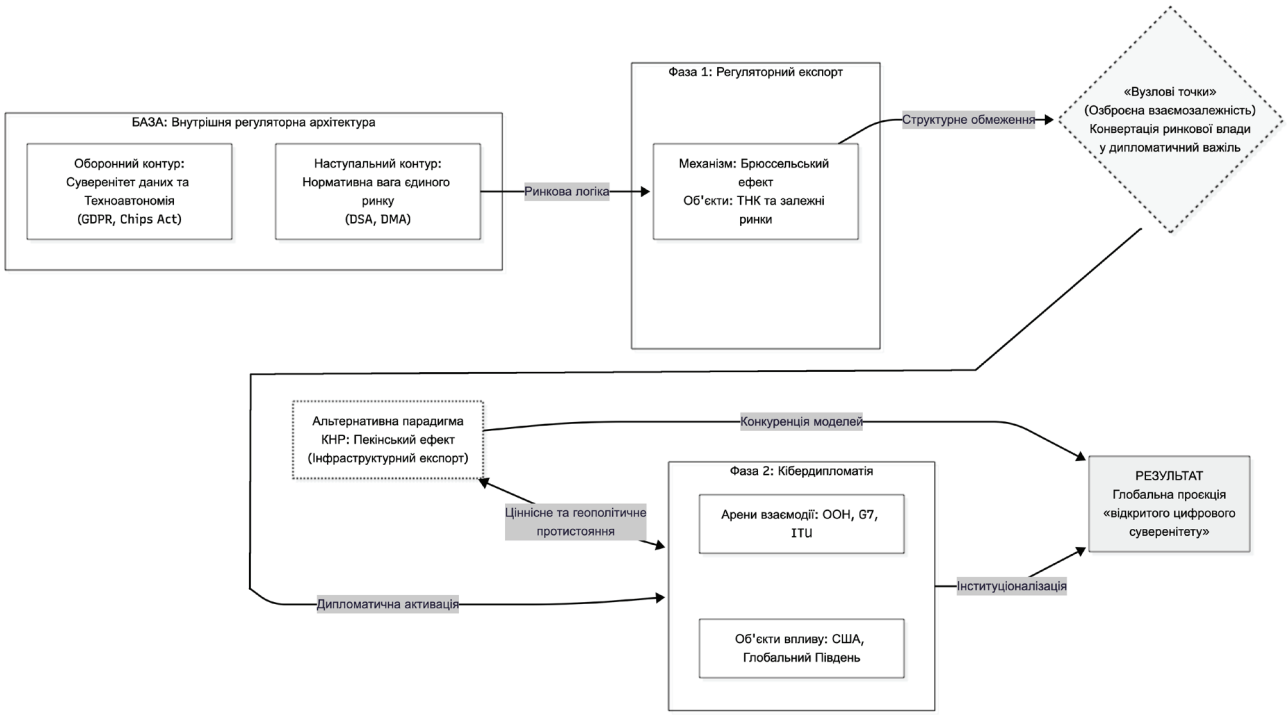

Рисунок. Двофазна трансмісійна модель цифрового суверенітету ЄС як зовнішньополітичного проєкту

Першим механізмом трансмісії є Брюссельський ефект, який Ану Бредфорд визначає як здатність ЄС односторонньо формувати глобальні стандарти без укладання міжнародних угод чи застосування класичних дипломатичних важелів. Цей механізм працює через ринкову логіку: транснаціональні корпорації, що прагнуть зберегти доступ до єдиного ринку, добровільно імплементують європейські стандарти в глобальному масштабі, оскільки підтримувати дві паралельні системи економічно нераціонально[17]. Показовим прикладом є GDPR: після набуття ним

[18] Erie and Streinz, *The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance*.
[19] Digital Compass 2030 (2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0067.

чинності у 2018 році понад 120 країн реформували або ухвалили нове законодавство про захист персональних даних, орієнтуючись на європейський регламент як еталонну модель. Аналогічно AI Act вже на етапі розроблення спонукав Microsoft, Google та OpenAI адаптувати корпоративні політики до європейської ризик-орієнтованої класифікації, фактично перетворюючи ЄС на першого кодифікатора, чиї стандарти визначають рамку дискусії задовго до появи альтернативних регуляторних моделей[20].

Найбільш показовим кейсом цього механізму є Бразилія: у серпні 2018 року ця країна ухвалила закон Lei Geral de Proteção de Dados (LGPD), який набрав чинності у 2020 році. Закон практично відтворює архітектуру GDPR — принцип мінімізації даних, право на доступ та видалення, вимоги щодо призначення відповідального за захист даних і механізм транскордонних передач. Науковці визначають LGPD як «бразильський GDPR»: щоб не втратити доступу до європейського ринку, бразильські компанії повинні відповідати вимогам GDPR, що й стало основним мотивом ухвалення LGPD[21]. Аналогічну логіку демонструють транснаціональні технологічні корпорації: ще до набуття GDPR чинності Facebook та Microsoft публічно оголосили про глобальне впровадження його вимог для всіх своїх користувачів незалежно від юрисдикції[22, 23].

Однак Брюссельський ефект має структурне обмеження: він є ефективним щодо приватних корпорацій та окремих держав, які не можуть протистояти через економічне відставання від ЄС. Деякі держави здатні активно протиставляти альтернативну нормативну парадигму, і саме тут ринкова логіка вичерпує свої можливості. У таких випадках Євросоюз переходить від пасивного регулювання до активного примусу, що концептуально описується теорією озброєної взаємозалежності Фаррелла та Ньюмана. Ця теорія доводить, що контроль над ключовими вузлами (*chokepoints*) глобальних мереж дає непропорційну геополітичну владу[24]. Для ЄС такими вузловими точками стали власні юридичні регламенти. Блокуючи передачу даних у юрисдикції з нижчими стандартами безпеки, ЄС використовує правові норми як зброю для стримування альтернативних нормативних парадигм. У цифровому контексті такими вузловими точками ЄС є сертифікаційні схеми ENISA, які де-факто визначають технічні вимоги для постачальників обладнання з третіх країн; транскордонний механізм GDPR, який надає Євросоюзу спроможність в односторонньому порядку блокувати цифрові потоки з юрисдикціями, що не забезпечують адекватного рівня захисту. Саме ці регуляторні вузлові точки стають входом до другої фази.

Другим механізмом трансмісії є кібердипломатія, яка активізується там, де Брюссельський ефект не може діяти безпосередньо, тобто у відносинах із суверенними державами, які протиставляють альтернативні парадигми. Ключовим документом, що інституціоналізував кібердипломатію як повноцінний стратегічний напрям зовнішньої політики ЄС, стала Стратегія кібербезпеки для цифрового десятиліття 2020 року[25]. На відміну від попередньої Стратегії 2013 року, яка зосереджувалася переважно на технічних аспектах захисту мереж, оновлена вперше об'єднала регуляторну стійкість, оперативну спроможність та зовнішню кібердипломатію в єдину рамку. Інструментом перемикання між двома фазами слугує Cyber Diplomacy Toolbox — набір дипломатичних заходів, що дає змогу конвертувати регуляторні прецеденти фази 1 (автоматичного

---

[20] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA Relevance) (2024), http://data.europa.eu/eli/reg/2024/1689/oj.

[21] Richie Koch, "What Is the LGPD? Brazil's Version of the GDPR," *GDPR.Eu*, July 31, 2019, https://gdpr.eu/gdpr-vs-lgpd/.

[22] Andrew Tarantola, "Can Facebook Really Apply the EU's Data-Privacy Rules Worldwide?," Engadget, April 12, 2018, https://www.engadget.com/2018-04-12-facebook-eu-gdpr.html.

[23] Julie Brill, "Microsoft's Commitment to GDPR, Privacy and Putting Customers in Control of Their Own Data," *Microsoft On the Issues*, May 21, 2018, https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/.

[24] Farrell and Newman, "Weaponized Interdependence."

[25] "The EU's Cybersecurity Strategy for the Digital Decade | Shaping Europe's Digital Future," accessed April 15, 2026, https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

експорту стандартів через ринок) у потужні дипломатичні аргументи на міжнародних майданчиках фази 2, де ЄС взаємодіє вже не з бізнесом, а з іншими суверенними державами[26].

Конкретний зв'язок між регуляторним і дипломатичним вимірами простежується в тому, що рішення Суду ЄС у справі *Schrems II* змусило США видати Виконавчий указ 14086, який змінив правила функціонування розвідувального апарату Штатів[27]. Цей прецедент Брюссель використовує в межах майданчика OEWG як доказ ефективності чинних правових рамок: ЄС аргументує, що належна імплементація наявних норм дієвіша за створення нових міжнародних договорів, які пропонують альтернативні центри сили. Отже, суто юридичний акт фази 1 стає інструментом ідеологічної боротьби за модель глобального кіберврядування у фазі 2. По-друге, AI Act забезпечив Євросоюзу право першого голосу на ключових багатосторонніх майданчиках. Наприклад, у Хіросімському процесі зі штучного інтелекту, ініційованому в межах саміту G7 у 2023 році, ЄС визначав порядок денний дискусій ще до появи будь-якої альтернативної регуляторної моделі, а окремі його положення стали частиною нового кодексу поведінки G7[28]. По-третє, сертифікаційні схеми ENISA стають технічним стандартом для глобальних постачальників, що підсилює позицію ЄС у суперечках про технічну стандартизацію в межах Міжнародного союзу електрозв'язку (ITU), де КНР активно просуває власні стандарти через компанії на кшталт Huawei[29].

Висновки

У процесі дослідження проаналізовано цифровий суверенітет як інтегрований зовнішньополітичний проєкт Європейського Союзу та обґрунтовано системний зв'язок між внутрішньою регуляторною архітектурою ЄС і його кібердипломатичною діяльністю на міжнародній арені, що дає змогу зробити такі висновки.

По-перше, цифровий суверенітет ЄС реалізується через три взаємопов'язані виміри — суверенітет даних, технологічну автономію та нормативну вагу єдиного ринку, кожен із яких формує окремий шар регуляторної архітектури, що слугує вхідним ресурсом двофазної трансмісійної моделі. Ці виміри не є рівнозначними: якщо суверенітет даних і технологічна автономія відображають переважно оборонну логіку зменшення залежності, то нормативна вага ринку є наступальним інструментом, який перетворює внутрішнє законодавство на зовнішньополітичний важіль.

По-друге, зв'язок між внутрішнім регулюванням і зовнішньополітичним впливом реалізується через двофазну трансмісійну модель із каузальною асиметрією між фазами. Брюссельський ефект як перший механізм діє через ринкову логіку і є ефективним щодо транснаціональних корпорацій та економічно залежних держав, однак структурно неспроможний впливати на суверенні держави, які протиставляють альтернативні парадигми цифрового управління. Саме це обмеження активує другий механізм — кібердипломатію, яка конвертує регуляторні прецеденти першої фази в дипломатичні аргументи на міжнародних майданчиках. Принципово важливим є те, що ЄС здійснює цей вплив не лише через традиційні інструменти, наприклад, переговори, атрибуцію кіберзлочинів та санкції, а й через регуляторну дипломатію за замовчуванням: коли GDPR змушує Вашингтон видати Виконавчий указ 14086, а AI Act визначає порядок денний Хіросімського процесу G7, ЄС здійснює кібердипломатичний вплив структурно через вузлові точки взаємозалежності, контроль над якими дає непропорційну геополітичну вагу.

По-третє, описана стратегія функціонує в умовах зростаючої геополітичної конкуренції з Пекінським ефектом — альтернативною моделлю нормативного експорту КНР, яка поширюється через фізичну розбудову цифрової інфраструктури в межах програми «Цифровий шлях». Ця

[26] "The EU Cyber Diplomacy Toolbox: An In-Depth Analysis of Cyber Diplomacy," accessed May 4, 2026, https://www.cyber-diplomacy-toolbox.com/.

[27] "Executive Order 14086 – Policy and Procedures," *United States Department of State*, n.d., accessed May 7, 2026, https://www.state.gov/executive-order-14086-policy-and-procedures/.

[28] "Hiroshima AI Process," accessed April 15, 2026, https://www.soumu.go.jp/hiroshimaaiprocess/en/index.html.

[29] *The Geopolitics of Technology Charting the EU's Path in a Competitive World*, with European Parliament (European Parliament, 2024), https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762384/EPRS_BRI(2024)762384_EN.pdf.

конкуренція є асиметричною: там, де ЄС встановлює правила через ринок, КНР будує мережі через інфраструктуру. Протистояння між відкритим цифровим суверенітетом ЄС, заснованим на верховенстві права і захисті фундаментальних прав, та китайською моделлю технонаціоналізму відображає глибший ціннісний розлом у глобальному кіберпросторі.

Перспективи подальших досліджень полягають в емпіричному вимірюванні ефективності кібердипломатичних інструментів ЄС, зокрема впливу санкційного механізму Cyber Diplomacy Toolbox на зниження частоти та інтенсивності зловмисних кібероперацій проти держав-членів. Окремим перспективним напрямом є дослідження тристороннього геополітичного протистояння Брюсселя, Пекіна та Вашингтона в цифровій і технологічній сферах, а також місця України в цьому змаганні. Запропонований у статті аналітичний інструментарій двофазної трансмісійної моделі може бути застосований для оцінювання спроможності України формувати власний цифровий суверенітет і порівняння вітчизняної регуляторної бази кіберпростору з європейською.

Bibliography

Belfer Center for Science and International Affairs. “Critical and Emerging Technologies Index T.” With The Belfer Center for Science and International Affairs. June 5, 2025. https://www.belfercenter.org/critical-emerging-tech-index.

Bradford, Anu. “The Brussels Effect.” In *The Brussels Effect*, 1st ed., by Anu Bradford, 25–66. Oxford University Press, 2012. https://doi.org/10.1093/oso/9780190088583.003.0003.

Brill, Julie. “Microsoft’s Commitment to GDPR, Privacy and Putting Customers in Control of Their Own Data.” *Microsoft On the Issues*, May 21, 2018. https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/.

Digital Compass 2030 (2020). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0067.

Erie, Matthew S., and Thomas Streinz. *The Beijing Effect: China’s “Digital Silk Road” as Transnational Data Governance*. 2021. https://www.nyujilp.org/wp-content/uploads/2022/02/NYUJILP_Vol54.1_Erie_Streinz_1-91.pdf.

European Commission. “The EU’s Cybersecurity Strategy for the Digital Decade | Shaping Europe’s Digital Future.” Accessed April 15, 2026. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

Farrell, Henry, and Abraham L. Newman. “Weaponized Interdependence: How Global Economic Networks Shape State Coercion.” *International Security* 44, no. 1 (2019): 42–79. https://doi.org/10.1162/isec_a_00351.

Floridi, Luciano. “The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU.” *Philosophy & Technology* 33, no. 3 (2020): 369–78. https://doi.org/10.1007/s13347-020-00423-6.

Gineikyte-Kanclere, Vaida, Militsa Eggert, Goda Skiotyte, and Visionary Analytics. *European Software and Cyber Dependencies*. 2025.

“Hiroshima AI Process.” Accessed April 15, 2026. https://www.soumu.go.jp/hiroshimaaiprocess/en/index.html.

Kello, Lucas. *Striking Back: The End of Peace in Cyberspace – And How to Restore It*. Yale University Press, 2022. https://doi.org/10.2307/j.ctv2v55b54.

Koch, Richie. “What Is the LGPD? Brazil’s Version of the GDPR.” *GDPR.Eu*, July 31, 2019. https://gdpr.eu/gdpr-vs-lgpd/.

Liebetrau, Tobias. “Cyber Conflict Short of War: A European Strategic Vacuum.” *European Security* 31, no. 4 (2022): 497–516. https://doi.org/10.1080/09662839.2022.2031991.

Macron, Emmanuel. “Initiative pour l’Europe – Discours d’Emmanuel Macron pour une Europe souveraine, unie, démocratique.” elysee.fr, September 26, 2017. https://www.elysee.fr/emmanuel-macron/2017/09/26/initiative-pour-l-europe-discours-d-emmanuel-macron-pour-une-europe-souveraine-unie-democratique.

Mildebrath, Hendrik. “The CJEU Judgment in the *Schrems II* Case.” 2020. https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.

Pohle, Julia, Riccardo Nanni, and Mauro Santaniello. “Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices.” *Policy & Internet* 16, no. 4 (2024): 666–71. https://doi.org/10.1002/poi3.437.

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) (Text with EEA Relevance), 119 OJ L (2016). http://data.europa.eu/eli/reg/2016/679/oj.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA Relevance) (2024). http://data.europa.eu/eli/reg/2024/1689/oj.

Tarantola, Andrew. "Can Facebook Really Apply the EU's Data-Privacy Rules Worldwide?" Engadget, April 12, 2018. https://www.engadget.com/2018-04-12-facebook-eu-gdpr.html.

"The EU Cyber Diplomacy Toolbox: An In-Depth Analysis of Cyber Diplomacy." Accessed May 4, 2026. https://www.cyber-diplomacy-toolbox.com/.

The Geopolitics of Technology Charting the EU's Path in a Competitive World. With European Parliament. European Parliament, 2024. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762384/EPRS_BRI(2024)762384_EN.pdf.

United Nations Conference on Trade and Development. *Digital Economy Report*. 2024. https://unctad.org/system/files/official-document/der2024_en.pdf.

United States Department of State. "Executive Order 14086 – Policy and Procedures." n. d. Accessed May 7, 2026. https://www.state.gov/executive-order-14086-policy-and-procedures/.

Von der Leyen, Ursula. "State of the Union 2020 – European Commission." 2020. https://commission.europa.eu/strategy-and-policy/state-union/state-union-2020_en.

Danylo Nepochatov
PhD Student,
Specialty 291 "International Relations, Public Communications and Regional Studies",
Department of International Relations and Political Philosophy,
Simon Kuznets Kharkiv National University of Economics, Ukraine
https://orcid.org/0009-0006-5819-5842
danylo.nepochatov@hneu.net

DIGITAL SOVEREIGNTY AS AN EU FOREIGN POLICY PROJECT: REGULATORY INSTRUMENTS AND CYBER DIPLOMACY

Abstract

The global technological rivalry between the United States and China has confronted the European Union with a structural dilemma: lacking its own technology giants, microelectronics manufacturing capacity, and cloud infrastructure comparable to that of the United States or China, Europe's digital sphere has produced what may be termed a "digital vacuum." This article examines EU digital sovereignty as a strategic project aimed at overcoming this outsider status amid deep technological dependence on external suppliers.

A gap in the scholarly discourse has been identified: existing research treats the EU's internal regulatory architecture and its external cyber diplomacy as separate phenomena, without explaining the systemic mechanism connecting them. To address this gap, the article distinguishes three spheres of EU digital sovereignty — data sovereignty, technological autonomy, and the normative weight of the single market — each of which forms a distinct layer of the regulatory architecture. These layers serve as the conceptual foundation for the central theoretical contribution of the work.

The scientific novelty lies in the substantiation of a two-phase transmission model that explains the mechanism by which the EU's normative power is converted into geopolitical influence. The first phase describes unilateral regulatory export through the "Brussels Effect": the EU's market weight compels transnational corporations and third countries to implement European standards globally. The second

phase — multilateral cyber diplomacy — is activated where market logic exhausts its possibilities, namely in relations with sovereign states that advance alternative paradigms. In this phase, regulatory precedents from the first phase are converted into diplomatic arguments: the *Schrems II* ruling prompted the United States to adopt Executive Order 14086, while the European AI Act set the agenda of the G7 Hiroshima Process before any alternative model had emerged.

It is demonstrated that, faced with a deficit of infrastructural capacity — or so-called "poietic power" — the EU compensates by expanding its "cybernetic power": the ability to establish the rules of the digital space. This strategy unfolds amid growing competition with Beijing and Washington, both of which are actively building physical infrastructure for the development of emerging technologies. The methodological basis of the study comprises a systemic approach, normative-legal analysis, and the case study method (the Brazilian LGPD, the corporate policies of Facebook and Microsoft, and the *Schrems II* ruling). The conclusion is drawn that EU digital sovereignty represents a model of "regulatory diplomacy by default" — one that allows the Union to preserve its geopolitical weight not through symmetrical infrastructural competition, but through the establishment of normative rules that extend far beyond its borders.

Keywords: digital sovereignty, cyber diplomacy, Brussels Effect, Beijing Effect, technological autonomy, EU, artificial intelligence.

Подано / Submitted: 30.03.2026
Схвалено до публікації / Accepted: 04.05.2026
Оприлюднено / Published: 29.05.2026