Стойко Олена Михайлівна

Європейський підхід до розуміння цифрового суверенітету

УДК 327:004.056(477:061.1 ЄС)
DOI https://doi.org/10.24195/2414-9616.2025-6.13

Стойко Олена Михайлівна
доктор політичних наук, провідний науковий співробітник
Інституту держави і права імені В. М. Корецького Національної академії наук України
вул. Трьохсвятительська, 4, Київ, Україна
ORCID: 0000-0002-1021-5270

Розглянуто еволюцію розуміння цифрового суверенітету у нормативно-правових документах Євросоюзу та політичних деклараціях лідерів. Протягом останнього десятиліття ЄС прийняв низку регуляторних актів щодо використання цифрових технологій, однак питання утвердження свого суверенітету у цій сфері набуло актуальності з 2019 року. ЄС був одним із глобальних лідерів у правовому регулюванні інформаційно-комунікаційних технологій, прийнявши у 2016 році Загальний регламент про захист даних.Особливістю вузького підходу до цифрового суверенітету, характерного для цього етапу, є його розгляд у контексті інфраструктури та програмного забезпечення. Найбільшу увагу за вузького розуміння цифрового суверенітету ЄС приділяв захисту даних та приватності, кібербезпеці та підтримці конкурентоспроможності європейських технологічних компаній. Однак пандемія, російсько-українська війна виявила загрозливу залежність ЄС від зовнішніх акторів та вразливість, зокрема і в суспільно-політичних процесах. Прийняття Берлінської декларації (2025) стало важливою віхою у захисті демократії та європейських цінностей як важливої складової цифрового суверенітету у широкому його розумінні. Запропонований Єврокомісією Європейський щит демократії передбачає низку заходів у таких ключових напрямах як: 1) захист цілісності інформаційного простору; 2) зміцнення європейських інституцій, забезпечення чесних і вільних виборів та вільних і незалежних ЗМІ та 3) підвищення стійкості суспільства та залучення громадян. Особливу роль відведено громадянському суспільству, організації якого отримають фінансову, організаційну та інформаційну підтримку з боку ЄС.
Ключові слова: *цифровий суверенітет, цифровізація, демократія, медіаграмотність, кібербезпека, дані, штучний інтелект, ЄС, євроінтеграція, громадянське суспільство.*

Вступ. За останнє десятиліття цифровий або технологічний суверенітет став однією з провідних тем європейського політичного дискурсу, що зумовлено прагненням ЄС зменшити структурну залежність від іноземних технологій та забезпечити більший контроль над своєю цифровою інфраструктурою, критичними ресурсами, потоками даних та інноваційними екосистемами.

Цифрова політика була визначена одним із ключових політичних пріоритетів Європейської комісії на 2019–2024 роки [1] , а її голова У. фон дер Ляєн пообіцяла, що Європа має досягти «технологічного суверенітету» у критично важливих сферах [2].

У нещодавньому звіті Комісії про медіа суверенітет (2019) підкреслено, що конкуренція з боку глобальних технологічних гравців, які не завжди дотримуються європейських правил і фундаментальних цінностей і які ставлять привласнення та оцінку даних в центр своєї стратегії, становить серйозний політичний виклик для Європи [17]. У 2019 році Європейська Рада наголосила, що ЄС необхідно продовжувати розвивати конкурентоспроможну, безпечну, інклюзивну та етичну цифрову економіку з підключенням до мережі світового класу, та закликала приділяти особливу увагу питанням безпеки даних та штучного інтелекту (ШІ) [9]. У жовтні 2025 року депутати Європарламенту обговорили з представниками Ради та Єврокомісії шляхи просування та захисту цифрових правил ЄС і зменшення технологічної залежності від суб'єктів, що не входять до ЄС [15]. Особливу увагу було приділено обговоренню важливості побудови безпечної та автономної цифрової економіки та повного впровадження цифрових правил ЄС, зокрема законів про цифрові послуги та цифрові ринки, про штучний інтелект, про кіберстійкість, про дані, про мікросхеми та правила щодо криптоактивів.

Однак російсько-українська війна, посилення конкуренції у глобальному технологічному змаганні з дедалі очевиднішим відставанням ЄС від Китаю та США змушує Євросоюз перейти від вузького до широкого розуміння цифрового суверенітету. Тому **метою статті** є вивчення зміни у підході ЄС до утвердження свого цифрового суверенітету.

Методи дослідження. Для досягнення цієї мети було використно системний підхід для розгляду цифрового суверенітету як частини ширшого феномена, що включає в себе безпеку, економіку, технологію, політику та геополітику, а також комплекс якісних методів дослідження, зокрема контент-аналіз для вивчення нормативно-правових документів Євросоюзу, що регулюють цифрову сферу, прогностичний метод для оцінки перспектив розвитку цифрового суверенітету в ЄС.

Результати. Можна виділи два розуміння цифрового суверенітету: вузьке і широке. У вузькому розумінні цифровий суверенітет обмежується такими технологіями, як наноелектроніка, фотоніка, робототехніка, 5G, високопродуктивні обчислення, великі дані, хмарні обчислення, штучний інтелект

та сферою економіки даних Інтернет речей (IoT). Найбільшу стурбованість ЄС викликають захист даних та приватності, а також кібербезпека.

Що стосується даних, то ЄС прийняв дуже суворі рамки щодо конфіденційності та захисту даних, в основі яких лежить Загальний регламент про захист даних (ЗРЗД, 2016), який набув чинності в 2016 році, і запровадив захисне «право на забуття» та право на перенесення даних, щоб посилити контроль осіб над своїми власними даними [5]. Крім того, Єврокомісія визначила стратегію щодо просування міжнародних стандартів захисту даних. ЄС вважається розробником стандартів у сфері конфіденційності та захисту даних, оскільки різні країни включили положення ЗРЗД до свого національного законодавства, а деякі транснаціональні корпорації вирішили прийняти ЗРЗД як свій глобальний стандарт діяльності [7].

У 2025 році була прийнята Стратегія Євросоюзу щодо даних [11], яка визначає три пріоритетні напрямки дій, що базуються на: розширенні доступу до даних для штучного інтелекту, щоб забезпечити європейським підприємствам доступ до високоякісних даних, необхідних для інновацій [3]; вдосконаленні правил щодо даних, щоб надати підприємствам правову визначеність та зменшити витрати на дотримання вимог; захисті суверенітету ЄС у сфері даних, щоб зміцнити позицію Союзу щодо міжнародних потоків даних.

У сфері кібербезпеки ще у 2019 році залежність від китайської інфраструктури 5G була визначена як критична слабкість ЄС, а також було підкреслено ризик того, що відсутність єдиного європейського кіберпростору робить спільноту вразливою перед зовнішнім впливом. Держави-члени ЄС опублікували звіт, в якому застерігають від надмірної залежності від одного постачальника обладнання, що збільшує ризик потенційного переривання поставок і створює загрозу безпеці [12].

Ще однією проблемою, яка викликає занепокоєння держав-членів ЄС, є відсутність контролю над даними, що генеруються на їхній території. Останнім часом європейські уряди почали відмовлятися від хмарних рішень, що пропонуються компаніями, які не є членами ЄС, і натомість впроваджувати хмарні рішення, розроблені в Європі.

Крім того, великі онлайн-платформи, які переважно базуються за межами ЄС, дедалі частіше розглядаються як такі, що домінують у цілих секторах економіки ЄС і позбавляють держави-члени ЄС їх суверенітету в таких сферах, як авторське право, захист даних, оподаткування або транспорт. Ця проблема поширилася на інші сфери, такі як електронна комерція та дезінформація в Інтернеті, де законодавство ЄС не в змозі протидіяти впливу іноземних високотехнологічних компаній.

У відповідь, починаючи з 2014 року, ЄС запровадив низку інструментів для боротьби з кібератаками. Одним з перших стала Директива про безпеку мереж та інформації (2016), яка покращила можливості та співробітництво держав-членів у сфері кібербезпеки і визначила для компаній заходи щодо запобігання та повідомлення про інциденти безпеки та кібератаки в ключових секторах (тобто енергетика, транспорт, банківська справа, інфраструктура фінансових ринків, охорона здоров'я, водопостачання та цифрова інфраструктура). Європейський закон про кібербезпеку (2019) [8] запроваджує (необов'язкову) загальноєвропейську систему сертифікації кібербезпеки для продуктів ІКТ, щоб забезпечити захист споживачів та підприємств від загроз кібербезпеки.

В результаті ЄС почав утверджуватися як орган, що встановлює стандарти в галузі кібербезпеки, оскільки країни, що не входять до ЄС, а також приватні компанії, які ведуть бізнес або мають дочірні компанії в ЄС, оновили свої практики та політики в галузі кібербезпеки, щоб забезпечити відповідність цим новим і розширеним законодавчим вимогам.

Для посилення кібербезпеки ЄС необхідно вжити заходів у трьох напрямках:

1) переглянути систему сертифікації кібербезпеки ЄС, яка забезпечує гармонізований набір правил для захисту споживачів та підприємств в ЄС. Так впровадження обов'язкової, а не добровільної, системи сертифікації в масштабах ЄС стало б кроком вперед у забезпеченні справді безпечного середовища і сприяло б утвердженню ЄС як органу, що встановлює стандарти в галузі кібербезпеки;

2) покращити координацію у питаннях кібербезпеки. Хоча уже було оголошено про створення нового Спільного підрозділу з кібербезпеки для забезпечення посиленої співпраці між державами-членами, у звіті Європейської рахункової палати наголошується, що ЄС необхідно вжити додаткових заходів для усунення непослідовності у транспонуванні або прогалин у законодавстві ЄС (наприклад, обмежені та різноманітні правові рамки щодо обов'язків дбайливості; директиви ЄС з корпоративного права не містять конкретних вимог щодо розкриття інформації про кіберризики) [10]. Важливим кроком також стало прийняття пропозиції Єврокомісії щодо створення європейських центрів компетенції з кібербезпеки у галузі промисловості, технології та досліджень, перший з яких було відкрито 8 травня 2023 року у Бухаресті (Румунія).

3) удосконалення процедури закупівель в ЄС. Резолюція Європейського парламенту від 2019 року закликає зробити безпеку обов'язковим аспектом у всіх процедурах державних закупівель для відповідної інфраструктури як на рівні ЄС, так і на національному рівні. Держави-члени повинні розробити конкретні вимоги безпеки, які могли б застосовуватися в контексті державних закупівель, пов'язаних з мережами 5G, включаючи обов'язкові

вимоги щодо сертифікації кібербезпеки. У більш загальному плані можна було б розглянути можливість перегляду правил державних закупівель ЄС та положень про надання грантів з метою кращого врахування критичних аспектів цифрових технологій у чутливих секторах. Це означало б надання достатньої ваги міркуванням безпеки при оцінці тендерних пропозицій та більший акцент на диверсифікації постачальників ІКТ, а також на прозорості ланцюгів постачання мережевого обладнання.

На рівні ЄС було запропоновано або вже обговорюється низка ініціатив, спрямованих на прискорення процесу цифровізації та посилення стратегічної автономії Європи в цифровій сфері, які базуються на трьох основних елементах: 1) створенні системи управління даними; 2) сприянні створенню надійного середовища; 3) адаптації правил конкуренції та регулювання.

1. Контроль над неперсональними даними має вирішальне значення. ЄС може отримати вигоду від своїх великих промислових ресурсів даних. З цією метою надзвичайно важливим є створення безпечної загальноєвропейської системи обробки даних та сприяння інвестиціям у передові технології.

2. Для створення надійного цифрового середовища необхідно запровадити європейську хмарну та інформаційну інфраструктури для зміцнення суверенітету Європи в галузі даних і розв'язання проблеми домінування на ринку хмарних технологій і зберігання даних неєвропейських постачальників, що може мати негативні наслідки для безпеки та прав громадян ЄС. Відповідно до європейської стратегії у сфері даних, на рівні ЄС можуть бути запропоновані подальші заходи для сприяння впровадженню загальноєвропейської хмарної інфраструктури (наприклад, встановлення спільних стандартів хмарних технологій, еталонної архітектури та вимог до взаємодії).

3. Сприятливе регулятивне середовище передбачає оновлення та адаптацію політики ЄС у сфері конкуренції та нормативно-правову базу до цифрової ери. Наразі обговорюється перехід до більш захисних та обережних механізмів, включаючи нові правила щодо іноземної державної власності та практик великих технологічних компаній, що спотворюють конкуренцію. Також триває робота над розробкою нових інструментів ЄС для досягнення конвергенції механізмів перевірки інвестицій та оцінки поглинань високотехнологічних європейських компаній. Крім того, створення робочої групи ЄС з питань стратегічних галузей та технологій, завданням якої буде визначення стратегічно важливих галузей, для яких будуть запроваджені обмеження на іноземні інвестиції та винятки з державної допомоги та політики конкуренції, може забезпечити координацію між державами-членами та ЄС у цьому питанні.

З огляду на стрімкий технологічний розвиток необхідно адаптувати інструменти політики ЄС у сфері конкуренції та регулювання. У низці досліджень та звітів міститься заклик доповнити оцінку ex-post ex-ante правилами, які б краще регулювали поведінку великих цифрових платформ, що передбачає адаптацію перспективного підходу до регулювання цифрових ринків та забезпечення більшої відкритості, справедливості та передбачуваності екосистем онлайн-платформ та онлайн-діяльності. У довгостроковій перспективі розглядається можливість створення власних цифрових інструментів та рішень (наприклад, операційних систем та мобільних платформ), які дозволять уникнути технологічної залежності та сприяють створенню відкритих, але при цьому безпечних цифрових екосистем в ЄС. Крім того, в рамках конкуренції та регуляторної бази для досягнення більшої технологічної автономії бажаним видається перехід до більш захисних та обережних механізмів, включаючи нові правила щодо власності іноземних держав та практик великих технологічних компаній, що спричиняють спотворення ринку.

Широкомасштабне вторгнення російських військ в Україну, активізація гібридної війни щодо європейських держав, дедалі більше значення сучасних інформаційно-комунікаційних технологій та ШІ для суспільних процесів зумовило перехід до широкого розуміння Євросоюзом цифрового суверенітету, яке включає і політичну сферу. Знаковим у цьому сенсі стало підписання 18 листопада 2025 року в Берліні під час Саміту з питань європейського цифрового суверенітету Декларації про європейський цифровий суверенітет (так звана Берлінська декларація) [6]. Підписанти взяли на себе політичне зобов'язання забезпечити спільну основу для посилення цифрових можливостей Європи. Берлінська декларація є ще однією віхою в спробах Союзу та його держав-членів сформулювати узгоджене бачення свого цифрового майбутнього.

У ній під цифровим суверенітетом розуміється «забезпечення того, щоб Європа могла діяти незалежно та самостійно на основі міжнародного права, власних законів, цінностей та інтересів безпеки, одночасно розвиваючи міжнародне співробітництво зі своїми партнерами, які поділяють європейські цінності та принципи». Це означає здатність держав-членів регулювати свою цифрову інфраструктуру, дані та технології, а фізичних і юридичних осіб: діяти незалежно у цифровому світі, що дозволяє приймати автономні рішення щодо використання, управління та розвитку цифрових систем без надмірної залежності від зовнішніх суб'єктів з метою захисту європейських демократій та європейських цінностей. У ній викладено такі основні принципи:

– уникнення дублювання регуляторних актів та реалізація послідовної політики. При цьому цифровий суверенітет не слід помилково тлумачити як протекціонізм, а скоріше як спільний європейський

підхід, що зміцнює нашу здатність діяти вільно, залишаючись у співпраці з глобальними ринками та партнерами; як відкритість Європи для глобальних партнерів зі спільними цінностями;

− створення сприятливого інвестиційного клімату та справедливої нормативно-правової бази, яка сприятиме інноваціям та конкурентоспроможності, з урахуванням інтересів малого, середнього і великого бізнесу;

− забезпечення суверенітету даних: найбільш чутливі дані Європи повинні бути ефективно захищені від надмірного зовнішнього втручання або позаєвропейських законів;

− залучення довгострокових інвестицій у стратегічні галузі, такі як високопродуктивні обчислення, напівпровідники, комунікаційні мережі нового покоління, супутникова інфраструктура, квантові технології, кібербезпека, хмарні технології та штучний інтелект;

− політика відкритих рішень, якщо вони відповідають високим стандартам кібербезпеки та доповнюються надійними запатентованими технологіями, де це доречно;

− створення спільних європейських активів у сфері штучного інтелекту, даних, хмарних потужностей та космічної інфраструктури, зокрема через державно-приватні партнерства та рішення з відкритим кодом;

− проактивна позиція ЄС на міжнародній арені для створення динамічної глобальної цифрової екосистеми. Співпраця в таких сферах, як безпечна та надійна цифрова інфраструктура, нові технології, стійкість ланцюгів постачання, сировина, кібербезпека, потоки даних, цифрові стандарти та цифрові навички, має вирішальне значення для зміцнення європейської економічної стійкості та забезпечення її значущості в глобальному цифровому порядку;

− посилення системи управління: замість створення нових чи дублюючих структур слід зосередитися на оптимізації та інтеграції чинних, забезпечуючи ясність і ефективність. Управління повинно зміцнювати довіру, зменшувати фрагментацію та забезпечувати прозорий механізм колективного прийняття рішень, виходити з принципу інклюзивності;

− розвиток людського капіталу: інвестиції в освіту та дослідження, цифрові навички та цифрову грамотність громадян необхідно для розширення можливостей європейської робочої сили, громадян, державних адміністрацій та підприємств. Медіа- та інформаційна грамотність є необхідною для підвищення рівня знань про цифрове середовище та навчання безпечній навігації в ньому, і її необхідно розвивати через навчання протягом усього життя, щоб забезпечити нашу стійкість та конкурентоспроможність;

− захист демократії.

Акцент на розвитку людського капіталу і захисті демократичних механізмів є відображенням широкого розуміння ЄС цифрового суверенітету й у цьому напрямі було зроблено низку важливих кроків. По-перше, це прийняття Плану дій щодо європейської демократії (2020) [14], який мав за мету сприяти проведенню вільних і чесних виборів та активній демократичній участі; підтримувати вільні та незалежні засоби масової інформації; та протидіяти дезінформації.

По-друге, це пакет заходів «Про захист демократії» (2023) [13], який був прийнятий напередодні виборів до Європарламенту 2024 року задля забезпечення прозорості представництва іноземних інтересів в ЄС. Для запровадження узгодженого підходу до усунення перешкод на внутрішньому ринку та оснащення ЄС інструментами прозорості, які дозволять йому захищати демократію, залишатися відкритим суспільством та захищати основні права, зокрема свободу вираження поглядів та доступ до інформації, була запропонована Директива про гармонізацію вимог щодо прозорості представництва інтересів, що здійснюється від імені третіх країн [16]. Вона має на меті забезпечити загальний високий рівень прозорості та демократичної підзвітності в усьому ЄС щодо лобістських кампаній, що надаються як послуга, а також подібних заходів, що здійснюються суб'єктами від імені уряду третьої країни, які намагаються вплинути на розробку, формулювання або впровадження державної політики чи законодавства, або на процеси прийняття державних рішень.

По-третє, це впровадження Європейського щита демократії. У середині листопада 2025 року Єврокомісія представила Європейський щит демократії, що містить низку заходів для зміцнення, захисту та просування сильних і стійких демократій у всьому ЄС [4]. Ця програма передбачає низку заходів за трьома основними напрямками: 1) захист цілісності інформаційного простору; 2) зміцнення європейських інституцій, забезпечення чесних і вільних виборів та вільних і незалежних ЗМІ та 3) підвищення стійкості суспільства та залучення громадян.

В її рамках планується створення нового Європейського центру демократичної стійкості, який об'єднає досвід і ресурси ЄС та держав-членів для посилення колективної спроможності передбачати, виявляти та реагувати на загрози і зміцнювати демократичну стійкість. Центр має стати платформою для сприяння обміну інформацією та підтримки розбудови спроможності протистояти новим спільним загрозам, зокрема іноземним маніпуляціям інформацією та втручанням і дезінформації. У рамках Центру буде створено платформу для зацікавлених сторін, щоб сприяти діалогу з перевіреними зацікавленими сторонами, такими як організації громадянського суспільства

(ОГС), дослідники та науковці, перевіряльники фактів та медіапровайдери.

1. Захист цілісності інформаційного простору є передумовою для реалізації громадянами своїх прав та участі у демократичному процесі. Комісія продовжить співпрацю з підписантами Кодексу поведінки щодо дезінформації та підготує протокол щодо інцидентів та кризових ситуацій у рамках Закону про цифрові послуги, щоб сприяти координації між відповідними органами та забезпечити швидке реагування на масштабні та потенційно транснаціональні інформаційні операції.

2. Зміцнення європейських інституцій, забезпечення чесних та вільних виборів, а також сприяння діяльності вільних і незалежних ЗМІ передбачає інтенсифікацію зусиль в рамках Європейської мережі співпраці з питань виборів шляхом налагодження систематичного обміну інформацією з ключових тем, що стосуються цілісності виборчих процесів. Планується створення незалежної Європейської мережі фактівчекерів для протидії поширенню дезінформації усіма офіційними мовами ЄС, а Європейська обсерваторія цифрових медіа розробить нові підходи для здійснення незалежного моніторингу та аналізу для оцінки ситуації у ході виборчої кампанії або в кризових ситуаціях. Для підтримки незалежної журналістики Єврокомісія планує виділити додаткове фінансування для медіа для посилення стійкості ЗМІ. У ході перегляду Директиви про аудіовізуальні медіапослуги Комісія планує посилити роль медіапослуг та удосконалить правила розміщення реклами для сприяння сталому розвитку медіа в ЄС. Також буде переглянуто Рекомендації Комісії щодо безпеки журналістів та посилено заходи для підтримки системи боротьби з неправомірними судовими позовами проти участі громадськості.

3. Підвищення стійкості суспільства та залучення громадян передбачає насамперед підвищення медіаграмотності та цифрової грамотності для всіх вікових груп, щоб допомогти їм розпізнавати та протидіяти маніпулюванню інформацією. Також планується низка заходів для активізації залучення громадян до демократичних процесів, зокрема шляхом широкого впровадження консультацій. Для підвищення раціональності процесу прийняття політичних рішень Єврокомісія розробить Рекомендації щодо підтримки наукових даних у процесі формування політики.

У рамках Європейського щита демократії також запропоновано Стратегію ЄС щодо громадянського суспільства, спрямовану на посилення залучення, захисту та підтримки організацій громадянського суспільства (ОГС). Оскільки громадянське суспільство відіграє важливу роль у демократичних процесах, сприяючи розробці політики, надаючи соціальні та громадські послуги, підвищуючи обізнаність про важливі соціальні питання та представляючи різні групи, то Єврокомісія прагне до посилення взаємодії з ОГС, що буде здійснюватися по трьох напрямах:

1) створення нової платформи громадянського суспільства для подальшого сприяння діалогу щодо захисту та просування цінностей ЄС.

2) створення онлайн-центру знань про громадянський простір для полегшення доступу до активних проєктів та інструментів, включаючи доступні заходи захисту;

3) збільшення фінансування (орієнтовно втричі – до 3,6 млрд євро у наступному бюджеті ЄС) та полегшення доступу до фінансових інструментів ОГС.

Висновки. Дедалі більше проникнення сучасних цифрових технологій у всі сфери суспільного життя та посилення глобальної гонки за технологічне лідерство між різними політичними режимами зумовило необхідність появи цифрового суверенітету. Євросоюз поступово відмовляється від вузького його розуміння, насамперед технологічного виміру – комунікаційна інфраструктура, дані, ШІ, до ширшого – політичного (захист демократичних інституцій) та людського (розвиток людського капіталу, медіаграмотність). Україна як кандидат на членство в Євросоюзі повинна враховувати таке широке розуміння цифрового суверенітету, зміцнення якого є особливо нагальним з огляду на російсько-українську війну.

ЛІТЕРАТУРА:

1. A Europe fit for the digital age: Empowering people with a new generation of technologies. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en

2. A Union that strives for more: My agenda for Europe. URL: https://commission.europa.eu/document/download/063d44e9-04ed-4033-acf9-639ecb187e87_en?filename=political-guidelines-next-commission_en.pdf

3. Communication From The Commission To The European Parliament And The Council Data Union Strategy Unlocking Data For AI. COM/2025/835 final. URL: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM%3A2025%3A835%3AFIN

4. Communication on the European Democracy Shield. URL: https://commission.europa.eu/document/2539eb53-9485-4199-bfdc-97166893ff45_en General publications12 November 2025

5. Data protection. Rules for the protection of personal data inside and outside the EU. URL: https://commission.europa.eu/law/law-topic/data-protection_en

6. Declaration for European Digital Sovereignty. https://cdn.table.media/assets/europe/declaration-for-european-digital-sovereignty_final.pdf

7. Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers, 2017. URL: https://ec.europa.eu/commission/presscorner/detail/en/memo_17_15

8. EU Cybersecurity Act. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) № 526/2013 (Cybersecurity Act) (Text with EEA relevance). PE/86/2018/REV/1. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj

9. European Council meeting (21 and 22 March 2019) – Conclusions. URL: https://data.consilium.europa.eu/doc/document/ST-1-2019-INIT/en/pdf

10. European Court of Auditors Report Review № 02/2019: Challenges to effective EU cybersecurity policy (Briefing Paper) 2019. URL: https://www.eca.europa.eu/en/publications?did=49416

11. European Data Union Strategy. URL: https://digital-strategy.ec.europa.eu/en/policies/data-union

12. Member States publish a report on EU coordinated risk assessment of 5G networks security (2019). URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6049

13. On Defence of Democracy. Communication From the Commission to the European Parliament, the Council, the European Economic And Social Committee And the Committee Of the Regions. Strasbourg, 12.12.2023. COM(2023) 630 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023DC0630

14. On the European democracy action plan. Communication From the Commission to the European Parliament, the Council, the European Economic And Social Committee And the Committee Of the Regions. Brussels, 3.12.2020. COM(2020) 790 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790

15. Promoting and protecting digital sovereignty in the EU. URL: https://www.europarl.europa.eu/news/en/agenda/plenary-news/2025-10-06/3/promoting-and-protecting-digital-sovereignty-in-the-eu

16. Proposal for a Directive Of the European Parliament And Of the Council establishing harmonised requirements in the internal market on transparency of interest representation carried out on behalf of third countries and amending Directive (EU) 2019/1937. COM/2023/637 final. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52023PC0637

17. Towards European media sovereignty: An Industrial Media Strategy to leverage Data, Algorithms and Artificial Intelligence. URL: https://commission.europa.eu/document/download/8edef798-23c6-421b-a5a8-23dfa89ce4a4_en?filename=guillaume_klossa_special_report-european_media_sovereignty-executive_summary.pdf

The European approach to understanding digital sovereignty

Stoiko Olena Mykhailivna

Doctor of Political Science, Leading Research Fellow
V. M. Koretsky Institute of State and Law of the National Academy of Sciences of Ukraine
Trokhsviatytelska str., 4, Kyiv, Ukraine
ORCID: 0000-0002-1021-5270

The evolution of the understanding of digital sovereignty in EU regulatory documents and political declarations by leaders is considered. Over the past decade, the EU has adopted a number of regulatory acts on the use of digital technologies, but the issue of asserting its sovereignty in this area has become relevant since 2019. The EU has been one of the global leaders in the legal regulation of information and communication technologies, adopting the General Data Protection Regulation in 2016. A distinctive feature of the narrow approach to digital sovereignty of this stage is its consideration in the context of infrastructure and software. The EU's narrow understanding of digital sovereignty focused on data protection and privacy, cybersecurity, and supporting the competitiveness of European technology companies. However, the pandemic and the Russian-Ukrainian war revealed the EU's threatening dependence on external actors and its vulnerability, particularly in socio-political processes. The adoption of the Berlin Declaration (2025) was an important milestone in the protection of democracy and European values as an important component of digital sovereignty in its broadest sense. The European Democracy Shield proposed by the European Commission provides for a series of measures in key areas such as: 1) protecting the integrity of the information space; 2) strengthening European institutions, ensuring fair and free elections and free and independent media; and 3) increasing the resilience of society and engaging citizens. A special role is assigned to civil society, whose organisations will receive financial, organisational and informational support from the EU.

Key words: *digital sovereignty, digitalisation, democracy, media literacy, cybersecurity, data, artificial intelligence, EU, European integration, civil society.*

Дата першого надходження рукопису до видання: 18.11.2025
Дата прийнятого до друку рукопису після рецензування: 12.12.2025
Дата публікації: 30.12.2025