

Цифровий суверенітет держави: наукова риторика та реальні зміни

УДК 321.011:004]:327:351.746.1(477:0
61.1ЄС)
DOI <https://doi.org/10.24195/2414-9616.2024-6.23>

Милосердна Ірина Михайлівна
кандидат політичних наук, доцент,
доцент кафедри політології
Одеського національного університету
імені І. І. Мечникова
вул. Всеволода Змієнка, 2, Одеса,
Україна
ORCID: 0000-0003-2083-9500

Стаття присвячена аналізу сутності феномена «цифровий суверенітет» держави, визначенню його основних аспектів розуміння, а також особливості його формування в ЄС в умовах сучасного цифрового ландшафту.

Встановлено, що цифровий суверенітет держави являє собою необхідність для неї розвивати або зберігати щодо ключових технологій власну автономію або ж мати якомога нижчий рівень структурної залежності. Зміст цифрового суверенітету розкривається через аналіз технологічного суверенітету, інформаційної безпеки, а також цифровий суверенітет особистості. Зазначено, що інформаційна безпека має на увазі комплекс заходів, спрямованих на захист інформації від несанкціонованого доступу, використання, розкриття, зміни або знищення та її забезпечення є критично важливим для цифрового суверенітету держави та її національної безпеки. У статті наголошується, що цифровий суверенітет має на увазі юридичне закріплення принципу суверенної рівності держав щодо інформаційно-комунікаційної технологій.

У статті розглядається нормативна база, а також досвід формування та розвитку цифрового суверенітету ЄС. Встановлено, що під час формування цифрового суверенітету ЄС основний наголос робить на індивідуальні права. Визначено три елементи цифрового суверенітету ЄС: активніша підтримка розвитку технологій у середині ЄС; зусилля з вироблення глобальних норм для регулювання даних і цифрового середовища; суворіші обмеження для учасників ринку ЄС, які не входять до ЄС. Серед основних проблем у подальшому формуванні та розвитку цифрового суверенітету ЄС виокремлено: значну роль приватних суб'єктів у суспільній цифровій сфері, втручання іноземних гравців, кризи правової держави в Європі, ризик неефективного цифрового управління та недостатній рівень цифрової грамотності. Також у статті наголошено, що цифровізація та впровадження новітніх ІКТ має бути спрямоване не лише на ухвалення ефективних рішень, досягнення найкращих результатів і підвищення стійкості, а й на розширення консультацій з громадянами та громадянським суспільством, а суверенна влада має бути підзвітною та відкритою для громадського осмислення та контролю, щоб справді демократизувати цифровий суверенітет.

Ключові слова: цифровий суверенітет, державний суверенітет, інформаційна безпека, інформаційний простір, ІКТ, цифровізація, ЄС, Україна.

Вступ. Цифрові технології кардинально змінюють як суспільство, так і людину, включно з тим, як ми діємо, спілкуємося і мислимо. Неминуче цей вплив поширюється і на політичні інститути, розширюючи їх зміст і певною мірою видозмінює. Це не оминає стороною і такий феномен як суверенітет держави, який в умовах цифровізації наповнюється новим значенням. Незважаючи на окремі правові аспекти та різночитання щодо обсягу поняття, але цифровий суверенітет уже став невід'ємною частиною політичної та академічної риторики, різноманітні трактування та підходи до цієї категорії знаходять відображення в офіційних документах держав та міжнародних організацій.

Метою статті є аналіз сутності цифрового суверенітету держави, особливості та досвід його формування в сучасній європейській практиці.

Методи дослідження. Методологічна основа дослідження базується на принципах об'єктивності, багатофакторності та системності. Основним методом є міждисциплінарний метод аналізу дискурсу, оскільки він дає змогу відповісти на такі запитання: якими є основні аспекти

змісту цифрового суверенітету; якими є основні елементи цифрового суверенітету ЄС; що виступає в якості основного акценту в формуванні інформаційної безпеки ЄС.

Результати. У політичній науці склався консенсус, згідно з яким суверенітет почав відігравати визначальне значення у світовій політиці після 1648 р. із підписанням Вестфальського мирного договору, що закріпив підвалини Вестфальської політичної системи миру, яка зберігає своє значення й досі. Хоча дослідження суверенітету були пов'язані з Ж. Боденом, який визначав суверенітет як найвищу, абсолютну владу над громадянами та підданими, якою володіє монарх як представник Бога на Землі. Від самого початку категорія державного суверенітету була тісно пов'язана з контролем над певною територією.

Насамперед суверенітет означає незалежність конкретної держави стосовно інших держав, а також її верховну владу над усіма силами в межах національних кордонів. Таке саме тлумачення можна застосувати і до цифрового суверенітету, під яким у найширшому сенсі можна розуміти

незалежність держави у внутрішній і зовнішній політиці в цифровій сфері.

На думку Б. Ларсена «цифровий суверенітет означає здатність держави контролювати свою цифрову долю, він може охоплювати контроль над усім ланцюжком постачань ШІ, від даних до апаратного і програмного забезпечення» [17].

При дослідженні цифрового суверенітету теоретиками виокремлюються такі його основні напрями вивчення: як політична концепція, намагаючись оцінити його політичну корисність і нормативну бажаність [19; 20]; як політичну роль або функції цифрового суверенітету, прагнучи «зрозуміти, що суверенітет «робить» [5], тобто як цифровий суверенітет впливає на політику формування цифрової політики [6].

Слід зазначити, що дослідження цифрового суверенітету тісно пов'язані з аналізом технологічного суверенітету, а також безпеки, зокрема й інформаційної. Технологічний суверенітет передбачає забезпечення незалежності в наукових розробках, визначенні стандартів, безпеці фізичної інфраструктури зв'язку [8].

Формування цифрового суверенітету, необхідність контролю та незалежності в цифрових питаннях з'являється й з необхідності забезпечення безпеки. З появою глобальних мереж держави дедалі більше усвідомлюють свою вразливість, виражену в питаннях інфраструктурного контролю [15]. Після викриттів Е. Сноудена (2013 р.) акцент на державній автономії та безпеці став основним елементом дискурсів про цифровий суверенітет. Вимоги національного (або регіонального) цифрового суверенітету висувують актори, які наголошують на ризиках іноземного стеження і маніпуляцій, наводячи найрізноманітніші приклади – від дезінформації [23] до телекомунікаційної інфраструктури [24] і промислової [16].

Інформаційна безпека передбачає комплекс заходів, спрямованих на захист інформації від несанкціонованого доступу, використання, розкриття, зміни або знищення. Забезпечення інформаційної безпеки є критично важливим для держави, бізнесу та громадян, оскільки витік або втрата даних може призвести до серйозних наслідків, включно з фінансовими витратами, втратою репутації та навіть загрозами національній безпеці.

Цифрові технології транскордонні, але в політичній сфері світ розбитий на суверенні держави. Важливою умовою для розвитку діалогу з цифрової проблематики є взаємна повага і визнання його суб'єктів, насамперед суверенних держав. За цих умов суверенітет може виступити в ролі спільного знаменника, необхідного для подальшого розвитку міжнародного співробітництва у сфері забезпечення інформаційної безпеки за поваги до інтересів усіх держав.

Важливим стимулом для зміцнення цифрового суверенітету стала необхідність захисту критичної інформаційної інфраструктури від можливих атак. Цифровий суверенітет має на увазі контроль над зовнішнім виміром цифрової інфраструктури для захисту від інформаційного впливу та кібератак, наявність автономної програмно-апаратної бази в галузі цифрових технологій, розвинутого ІТ-сектору і платформних компаній.

У європейському науковому дискурсі також порушується питання про цифровий суверенітет особистості, під яким слід розуміти безпеку персональних даних і захист від негативного інформаційного впливу та дезінформації, а також захист від практики «наглядового капіталізму» з боку ІТ-гігантів, під яким розуміють збирання персональних даних та їхнє подальше використання з метою впливу на вподобання користувачів.

Отже, цифровий суверенітет можна інтерпретувати як необхідність для країни розвивати або зберігати щодо ключових технологій власну автономію або ж мати якомога нижчий рівень структурної залежності.

Також цифровий суверенітет має на увазі юридичне закріплення принципу суверенної рівності держав щодо інформаційно-комунікаційного середовища (ІКТ) у міжнародних документах із метою його формалізації не тільки як міжнародно-правової норми, а й як норми права.

Демократичні країни почали схвалювати цифровий суверенітет, зокрема в Європі. Так, у 2017 р. Е. Макрон висловився за «суверенну Європу», яка «керуватиме, а не братиме участь» у цифровій трансформації, «просуваючи свою модель у рамках глобалізації, модель, що поєднує інновації та регулювання» [18].

ЄС робить акцент на суверенітеті окремих людей і наголошує на таких фундаментальних цінностях, як людська гідність, свобода, демократія, рівність, верховенство закону та повага до прав людини [9; 14]. ЄС прагне бути лідером у створенні глобальних норм і стандартів у сфері регулювання та стандартизації цифрових технологій. Ключову роль у цьому відіграє високий стандарт захисту даних, що міститься в Загальному регламенті щодо захисту даних, який наразі поєднується з політикою, спрямованою на розвиток спільного ринку даних у Європі для стимулювання інновацій [13]. GDPR покликаний уніфікувати порядок захисту персональних даних в Інтернеті за допомогою правил і норм, а також загрози застосування штрафних санкцій. За умовами GDPR, будь-яка організація, незалежно від її місцезнаходження, повинна дотримуватися низки правил управління даними, якщо вона хоче торгувати з клієнтами в країнах ЄС. Ці правила дозволяють окремим громадянам краще контролювати те, як можуть бути використані їхні дані. Крім того, вони встановлюють потен-

ційні штрафи в розмірі майже 25 мільйонів доларів за витік даних [11].

ЄС, у міру розвитку свого цифрового ландшафту, нарощує свої зусилля з розширення власних технологічних можливостей і встановлення норм глобального управління. Під керівництвом голови Європейської комісії Урсули фон дер Ляєн ідея «цифрового суверенітету» стала центральним, керівним принципом діяльності Європи у сфері цифрових і технологічних технологій.

Згідно з доповіддю «Європейський союз і пошук цифрового суверенітету: будівництво «фортеці Європа» чи підготовка до нового світу?» (2020 р.) модель цифрового суверенітету ЄС включає три елементи: а) активніша підтримка розвитку технологій усередині ЄС, у вигляді ресурсів і політики для розвитку власних можливостей ЄС у сфері нових технологій, а також для ширшої цифровізації європейської економіки; б) зусилля з вироблення глобальних норм для регулювання даних і цифрового середовища; в) суворіші обмеження для учасників ринку ЄС, які не входять до ЄС. Так, з виходом і поступовим ухваленням ключових законодавчих пропозицій, а також нових національних правил у деяких країнах-членах ЄС, намітилася закономірність: ресурси і нормативні акти спрямовані на підтримку «європеїзації» ключових технологій і активів (включно з даними). Версія цифрового суверенітету ЄС не дає урядам привілейованого доступу до технологій і даних і не посилює контроль режиму над цифровою економікою. Радше, на думку політиків ЄС, він покликаний захистити інтереси приватних осіб і компаній у ЄС. Щонайменше, влада ЄС на одному ринку здатна впливати на встановлення стандартів у всьому світі, і ЄС продемонстрував готовність змусити інших прийняти стандарти ЄС або відмовитися від доступу на свій ринок. У короткостроковій перспективі такий підхід зробив ЄС світовим лідером у сфері цифрового регулювання [7].

Концепцію цифрового суверенітету Європи визначено в документі «Цифровий суверенітет для Європи» (2020 р.), згідно з яким «цифровий суверенітет означає для Європи здатність діяти незалежно в цифровому світі» із особливий акцентом на контролі європейців над своїми даними, суверенітет у сфері даних [23]. Необхідність такого контролю викликана тим, що невелика кількість великих технологічних компаній контролює величезні обсяги даних про своїх користувачів. За оцінками, 92 % усіх даних у західному світі зберігається на серверах, що належать США [11]. Це охоплює всі види діяльності в Інтернеті та в мережі, починаючи з даних регіональних і національних урядів і закінчуючи соціальними мережами. За такої кількості користувачів і такого обсягу інформації їхня політика і дії можуть мати значний вплив. Прикладом тому може слугувати Twitter, який заборонив

доступ до своєї платформи кільком відомим користувачам.

У зв'язку з цим, ініціативою ЄС, яка спрямована на розв'язання цієї проблеми, є проєкт «European Cloud Initiative Gaia-X», оголошений спільно Німеччиною та Францією з метою створення безпечної європейської хмари для обміну даними, яка б забезпечувала збереження контролю за власниками даних [12]. Основним акцентом у створенні безпечної хмари є розширення можливостей квантових обчислень, оскільки наявні методи шифрування можуть застаріти, якщо з'являться квантові комп'ютери. Існує загроза, відома як «зберігай сьогодні, а атакуй потім», коли організації можуть перехоплювати і зберігати повідомлення зараз, маючи намір розшифрувати їх, щойно з'являться квантові комп'ютери. Щоб протистояти цій загрозі, необхідно заздалегідь розробити рішення для захисту даних, які можна активувати в міру необхідності.

Також, у відповідь на зростаючий вплив Китаю, що реалізується через «Цифровий шовковий шлях» і багатосторонні форуми, ЄС тепер наполягає на скоординованому підході «команди Європи» до просування своєї моделі управління даними, в тому числі, зокрема, через стратегію «Глобальні ворота» і центр «Цифри для розвитку» [14]. Замість того, щоб продовжувати покладатися виключно на ринкові механізми для сприяння поширенню регулювання в стилі GDPR, ЄС дедалі частіше пропонує технічну підтримку країнам Глобального Півдня, зацікавленим у розвитку регулювання захисту даних. Ця послуга дедалі частіше пропонується в рамках ширшої підтримки країн у розробленні їхньої цифрової політики та національних стратегій цифрової трансформації [7].

Серед проблем, з якими стикається європейський цифровий суверенітет і які необхідно розв'язати для збереження спроможності здійснювати свої суверенні повноваження є: значна роль приватних суб'єктів у суспільній цифровій сфері, втручання іноземних гравців, криза правової держави в Європі, ризик неефективного цифрового управління і недостатній рівень цифрової грамотності.

Особливе місце серед цих проблем посідає цифрова грамотність, оскільки для ефективного здійснення цифрового суверенітету, необхідно розуміти, що таке цифрові технології, як вони функціонують, якими є їх можливості та обмеження і як вони впливають на суспільство. Це справедливо для регулюючих органів національного-регіонального-міжнародного рівнів, які розробляють політику в галузі цифрових технологій, але також важливо і для громадян, які повинні мати змогу висловлювати свою поінформовану думку в рамках демократичного процесу щодо того, яким вони бачать цифрове майбутнє для сус-

пільства. У цьому разі ми маємо говорити про підвищення рівня цифрової грамотності населення, володіння ними цифровими навичками (навички роботи з інформацією та даними, навички спілкування та співпраці, навички створення цифрового контенту, навички безпеки та навички розв'язання проблем). Громадяни повинні вміти використовувати технології та цифрові медіа безпечно, відповідально, критично й ефективно, щоб повноцінно брати участь у демократії, особливо в міру того, як дедалі більше функцій переходить в цифрову сферу.

Що ж стосується інформаційної безпеки в ЄС, то основний акцент спрямовано на захисті персональних даних і цифрових прав громадян. Нормативним актом в ЄС, спрямованим на забезпечення інформаційної безпеки, є друга директива про мережі та інформаційні системи (NIS2), яка передбачає розроблення національних стратегій кібербезпеки державам-членам, можливості реагування на інциденти і механізми співпраці для підвищення стійкості основних служб і постачальників цифрових послуг [10].

Держави ЄС повинні перенести її положення в національне законодавство і призначити компетентні органи для нагляду за її виконанням. Країни також повинні створити механізми співпраці, такі як групи реагування на інциденти комп'ютерної безпеки (CSIRTs), для полегшення обміну інформацією та координації реагування на інциденти.

Україна також обрала курс на входження до загальносвітового інформаційного простору, побудову інформаційного суспільства, розвиток електронної демократії [4]. Тому проблема формування цифрового суверенітету, як і інформаційної безпеки, зокрема, є однією з пріоритетних і для України. Так, ще в Законі України «Про Національну програму інформатизації» від 4 лютого 1998 року № 74/98-ВР під поняттям «інформаційний суверенітет держави» розуміється здатність держави контролювати та регулювати потоки інформації з-за меж держави з метою дотримання законів України, прав і свобод громадян, гарантування національної безпеки держави» (даний закон втратив чинність 01.03.2023 на підставі 2807-ІХ) [3].

Останнє десятиліття демонструє значні зміни у формуванні в державі автономної цифрової інфраструктури, відбувається створення як твердої. На думку К.В. Єфремової, як й інші країни, Україна зіштовхується з величезним впливом технологічних корпорацій, які забезпечують роботу та доступ до всесвітньої цифрової інфраструктури [2].

Як зазначає Д.В. Дубов, серед основних викликів у подальшому формуванні цифрового суверенітету в Україні є: вкрай складні військово-політичні та економічні умови; спроможності держави ефективно конкурувати на міжнародних цифрових ринках, передусім – через власні ІТ-корпорації;

зовнішня політика України щодо майбутнього кіберпростору (Україна бере участь у роботі Міжнародного союзу електрозв'язку, взаємодіє з ICANN однак досі ми не маємо чіткої та послідовної позиції держави щодо того, яким Україні бачиться «майбутнє інтернету»); розвиток військової складової цифрового суверенітету; неоднозначне питання щодо системи нормативно-правових документів, що впливають на формування інформаційного/цифрового суверенітету [1].

Результати. Таким чином, в умовах стрімких темпів цифровізації політичної сфери, цифровий суверенітет став актуальною проблемою для держав, оскільки традиційні механізми суверенітету тепер глибоко переплетені з цифровими технологіями, що ставить під сумнів здатність держав здійснювати контроль у межах власних кордонів.

Суть цифрового суверенітету полягає в необхідності контролю над цифровими технологіями на фізичному рівні (ресурси, інфраструктура, пристрої), на рівні коду (стандарты, правила, дизайн) та на інформаційному рівні (контент, дані).

Слід розуміти, що найближчими роками концепція цифрового суверенітету набуде ще більшої політичної значущості з огляду на широке впровадження інформаційно-комунікаційних технологій, штучного інтелекту. Однак, необхідно розуміти, що цифровізація має використовуватися як засіб досягнення більшого добробуту, сприяти ухваленню більш ефективних рішень, досягненню кращих результатів і підвищенню стійкості виробництва та споживання. Всебічний перегляд GDPR, діалог з громадянським суспільством, а також навчання цифровим навичкам можуть сприяти поліпшенням, необхідним для того, щоб дані європейських громадян опинилися в їхніх власних руках. Суверенна влада має бути підзвітна і відкрита для суспільного осмислення і контролю, щоб дійсно демократизувати цифровий суверенітет.

Кожна держава має своє унікальне соціальне, економічне та політичне середовище і технологічні можливості, які згодом визначають її внутрішні пріоритети та цифрову зовнішню політику. Таким чином, не можна говорити про «універсальний» підхід до цифрового суверенітету. Так, наприклад, для європейського цифрового суверенітету базовими складовими є: безпека, інновації, регулювання та цінності, а також відкритість. Центральним елементом цифрового суверенітету європейців є їхній контроль над своїми даними.

ЛІТЕРАТУРА:

1. Дубов Д.В. «Цифровий суверенітет» у сучасному світі: виклики та можливості для України. *Вісник Національної академії керівних кадрів культури і мистецтв*. 2015. № 1. С. 205–209. URL: <https://journals.uran.ua/visnyknakkkim/article/download/138366/135286>

2. Єфремова К.В. Забезпечення цифрового суверенітету держави в умовах індустрії 4.0. *Конституційні засади розвитку інноваційного суспільства* : зб. наук. пр. за матеріалами інтернет-конференції (м. Харків, 25 червня 2021 року) / за ред. А. В. Стріжкової. Харків : НДІ ПЗІР НАПрН України, 2021. С. 25–30. URL : <https://openarchive.nure.ua/server/api/core/bitstreams/f981db39-23a5-470f-bf25-e1af2f3701dc/content>.

3. Закон України «Про Національну програму інформатизації» від 04.02.1998. URL : <https://zakon.rada.gov.ua/laws/show/74/98-вр/ed19980204#Text>

4. Милосердна І.М., Краснопольська Т.М. Процес цифровізації політики: межі пізнання та особливості трансформації. *Актуальні проблеми політики*. 2022. Вип. 70. С. 106–113. URL : http://app.nuoua.od.ua/archive/70_2022/17.pdf

5. Barrinha A., Christou G. Speaking sovereignty: The EU in the cyber domain. *European Security*. 2022. 31(3) P. 356–376. URL : <https://doi.org/10.1080/09662839.2022.2102895>

6. Bellanova R., Carrapico H., Duez, D. Digital sovereignty and European security integration: An introduction. *European Security*, 2022. 31(3). P. 337–355. URL : <https://doi.org/10.1080/09662839.2022.2101887>

7. Burwell F., Propp K. The European Union and the search for digital sovereignty: Building «Fortress Europe» or preparing for a new world?» 2020. June 22. URL : <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-european-union-and-the-search-for-digital-sovereignty/>

8. Crespi F., Caravella S., Menghini M., Salvatori Ch. European Technological Sovereignty: An Emerging Framework for Policy Strategy. *Intereconomics*. 2021. V. 56. №6. P. 348–354. URL : <https://www.intereconomics.eu/contents/year/2021/number/6/article/european-technological-sovereignty-an-emerging-framework-for-policy-strategy.html>

9. Declaration on European Digital Rights and Principles. Brussels: European Commission. 2022. URL : <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles>

10. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/172, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) URL : <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

11. Fleming Sean What is digital sovereignty and why is Europe so interested in it? 2021. March. URL : <https://www.weforum.org/stories/2021/03/europe-digital-sovereignty/>

12. GAIA-X: a European Initiative for increased digital sovereignty. URL : <https://gaia-x.eu/what-is-gaia-x/>

13. General Data Protection Regulation (GDPR). 2018. URL : <https://gdpr-info.eu/>,\

14. Global Gateway overview. 2021. URL : https://international-partnerships.ec.europa.eu/policies/global-gateway/global-gateway-overview_en

15. Hansen L. Nissenbaum H. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*. 2009. 53(4). P. 1155–1175. URL : <https://doi.org/10.1111/j.1468-2478.2009.00572.x>

16. Hobbs C. Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry. *European Council on Foreign Relations*. 2020. URL : https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/

17. Larsen Benjamin Cedric The Geopolitics of AI and the Rise of Digital Sovereignty'. Brookings, 2022, 8 December. URL : <https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/>

18. Macron E. President macron gives speech on new initiative for Europe. 2017, September 26. URL : [https://www.elysee.fr/en/emmanuel-macron/2017/09/26/president-macron-gives-speech-on-new-initiative-for-europe\(open in a new window\)](https://www.elysee.fr/en/emmanuel-macron/2017/09/26/president-macron-gives-speech-on-new-initiative-for-europe(open in a new window))

19. Mueller M. Against sovereignty in cyberspace. *International Studies Review*, 2020. 22(4). P. 779–801. URL : <https://doi.org/10.1093/isr/viz044>

20. Obendiek, A. Take Back Control? Digital Sovereignty and a Vision for Europe. Jacques Delors Centre Policy Papers. 2021. 15 p. URL : <https://doi.org/10.48462/opus4-3934>

21. Pohle J., Thiel T. Digital sovereignty. Internet Policy Review. 2020. Vol.9. Issue 4. URL : <https://policyreview.info/concepts/digital-sovereignty>

22. Smuha, Nathalie A., Digital Sovereignty in the European Union: Five Challenges from a Normative Perspective (July 07, 2024). Published in Barrett, G., Müller-Graff, PC., Rageade, JP., Vadász, V. (eds), *European Sovereignty: The Legal Dimension* (Springer, 2024)., URL : <https://ssrn.com/abstract=4501591>

23. Tambiama M. Digital sovereignty for Europe. EPRS: European Parliamentary Research Service. 2020. URL : [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf)

24. Voelsen D. 5G, Huawei und die Sicherheit unserer Kommunikationsnetze – Handlungsoptionen für die deutsche Politik. SWP-Aktuell. 2019. №. 5. 2019. URL : <https://doi.org/10.18449/2019A05>

REFERENCES:

1. Dubov D.V. (2015) «Cyfrovij suverenitet» u suchasnomu sviti: vyklyky ta mozhlyvosti dlya Ukrainy. *Visnyk Nacionalnoyi akademiyi kerivnyx kadrov kultury i mystecztv*. № 1. S. 205–209. Retrieved from: <https://journals.uran.ua/visnyknakkim/article/download/138366/135286> [in Ukrainian]

2. Yefremova K.V. (2021) Zabezpechennya cyfrovogo suverenitetu derzhavy v umovax industriyi 4.0. *Konstytucijni zasady rozvytku innovacijnogo suspilstva* : zb. nauk. pr. za materialamy internet-konferenciyi (m. Xarkiv, 25 chervnya 2021 roku) / za red. A. V. Strizhkovoyi. Xarkiv : NDI PZIR NAPrN Ukrainy. S. 25–30. Retrieved from: <https://openarchive.nure.ua/server/api/core/bitstreams/f981db39-23a5-470f-bf25-e1af2f3701dc/content> [in Ukrainian]

3. Закон Ukrainy «Pro Nacionalnu programu informatyzaciyi» vid 04.02.1998. *Ofitsiyni sait Verkhovnoi Rady Ukrainy* [Official website of the Verkhovna Rada of Ukraine]. Retrieved from: <https://zakon.rada.gov.ua/laws/show/74/98-вр/ed19980204#Text> [in Ukrainian]

4. Myloserdna I.M., Krasnopol'ska T.M. (2022) Proces cyfrovizaciyi polityci: mezhi piznannya ta osob-

lyvosti transformaciyi. *Aktualni problemy polityky*. Vyp.70. S. 106–113. Retrieved from: http://app.nuoua.od.ua/archive/70_2022/17.pdf [in Ukrainian]

5. Barrinha A., Christou G. (2022) Speaking sovereignty: The EU in the cyber domain. *European Security*. 31(3) P. 356–376. Retrieved from: <https://doi.org/10.1080/09662839.2022.2102895> [in English]

6. Bellanova R., Carrapico H., Duez, D. (2022) Digital sovereignty and European security integration: An introduction. *European Security*. 31(3). P. 337–355. Retrieved from: <https://doi.org/10.1080/09662839.2022.2101887> [in English]

7. Burwell F., Propp K. (2020) The European Union and the search for digital sovereignty: Building «Fortress Europe» or preparing for a new world?» June 22. Retrieved from: <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-european-union-and-the-search-for-digital-sovereignty/> [in English]

8. Crespi F., Caravella S., Menghini M., Salvatori Ch. (2021) European Technological Sovereignty: An Emerging Framework for Policy Strategy. *Intereconomics*. V. 56. №6. P. 348–354. Retrieved from: <https://www.intereconomics.eu/contents/year/2021/number/6/article/european-technological-sovereignty-an-emerging-framework-for-policy-strategy.html>. [in English]

9. Declaration on European Digital Rights and Principles (2022) Brussels: European Commission. Retrieved from: <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles> [in English]

10. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Retrieved from: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> [in English]

11. Fleming Sean (2021) What is digital sovereignty and why is Europe so interested in it? March. URL : <https://www.weforum.org/stories/2021/03/europe-digital-sovereignty/> [in English]

12. GAIA-X: a European Initiative for increased digital sovereignty. Retrieved from: <https://gaia-x.eu/what-is-gaia-x/> [in English]

13. General Data Protection Regulation (GDPR). 2018. Retrieved from: <https://gdpr-info.eu/>, [in English]

14. Global Gateway overview. 2021. Retrieved from: https://international-partnerships.ec.europa.eu/policies/global-gateway/global-gateway-overview_en [in English]

15. Hansen L. Nissenbaum H. (2009) Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*. 53(4). P. 1155–1175. Retrieved from: <https://doi.org/10.1111/j.1468-2478.2009.00572.x> [in English]

16. Hobbs C. (2020) Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry. *European Council on Foreign Relations*. Retrieved from: https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/ [in English]

17. Larsen Benjamin Cedric (2022) The Geopolitics of AI and the Rise of Digital Sovereignty'. Brookings, 8 December. Retrieved from: <https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/> [in English]

18. Macron E. (2017) President Macron gives speech on new initiative for Europe. September 26. Retrieved from: <https://www.elysee.fr/en/emmanuel-macron/2017/09/26/president-macron-gives-speech-on-new-initiative-for-europe> [in English]

19. Mueller M. (2020) Against sovereignty in cyberspace. *International Studies Review*. 22(4). P. 779–801. Retrieved from: <https://doi.org/10.1093/isr/viz044> [in English]

20. Obendiek A. (2021) Take Back Control? Digital Sovereignty and a Vision for Europe. Jacques Delors Centre Policy Papers. 15 p. Retrieved from: <https://doi.org/10.48462/opus4-3934> [in English]

21. Pohle J., Thiel T. (2020) Digital sovereignty. *Internet Policy Review*. Vol.9. Issue 4. Retrieved from: <https://policyreview.info/concepts/digital-sovereignty> [in English]

22. Smuha Nathalie A. (2024) Digital Sovereignty in the European Union: Five Challenges from a Normative Perspective (July 07, 2024). Published in Barrett, G., Müller-Graff, PC., Rageade, JP., Vadász, V. (eds), *European Sovereignty: The Legal Dimension* (Springer,). Retrieved from: <https://ssrn.com/abstract=4501591> [in English]

23. Tambiama M. (2020) Digital sovereignty for Europe. EPRS: European Parliamentary Research Service. Retrieved from: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf) [in English]

24. Voelsen D. (2019) 5G, Huawei und die Sicherheit unserer Kommunikationsnetze – Handlungsoptionen für die deutsche Politik. SWP-Aktuell. №. 5. 2019. Retrieved from: <https://doi.org/10.18449/2019A05> [in German]

Digital sovereignty of the state: scientific rhetoric and real changes

Myloserdna Iryna Mykhailivna

Candidate of Political Sciences,
Associate Professor,
Associate Professor at the Department
of Political Science
Odesa I. I. Mechnikov National University
Vsevolod Zmienko str., 2, Odesa, Ukraine
ORCID: 0000-0003-2083-9500

The article is devoted to analysing the essence of the phenomenon of “digital sovereignty” of the state, defining its main aspects of understanding, as well as the peculiarities of its formation in the EU under the conditions of the modern digital landscape.

It is established that the digital sovereignty of a state represents the need for it to develop or maintain its own autonomy with regard to key technologies or to have the lowest possible level of structural dependence. The content of digital sovereignty is analysed through the analysis of technological sovereignty, information security, and the digital sovereignty of the individual. It is noted that information security implies a set of measures aimed at protecting information from unauthorised access, use, disclosure, alteration or destruction, and its provision is critical to the digital sovereignty of the state and its national security. The article notes that digital sovereignty implies the legal enshrinement of the principle of sovereign equality of states with regard to information and communication technologies.

The article considers the regulatory framework, as well as the experience of formation and development of digital sovereignty of the EU. It is established that in the formation of the EU digital sovereignty the main emphasis is placed on individual rights. Three elements of EU digital sovereignty are identified: more active support for technology development within the EU; efforts to develop global norms to regulate data and the digital environment; and stricter restrictions for non-EU EU market players. Among the main challenges in further shaping and developing the EU's digital sovereignty are highlighted: the significant role of private actors in the public digital sphere, the interference of foreign players, the crisis of the rule of law in Europe, the risk of ineffective digital governance and the insufficient level of digital literacy. The article also points out that digitalisation and adoption of the latest ICTs should not only aim at effective decision-making, better outcomes and increased sustainability, but also at greater consultation with citizens and civil society, and sovereign power should be accountable and open to public reflection and scrutiny in order to truly democratise digital sovereignty.

Key words: digital sovereignty, state sovereignty, information security, information space, ICT, digitalisation, EU, Ukraine.