Розділ 1

ПОЛІТИЧНІ ІНСТИТУТИ ТА ПРОЦЕСИ

УДК 321.011:004]: 327:351.746.1
DOI: 10.33663/1563-3349-2025-98-282

О. М. СТОЙКО

КОНЦЕПЦІЯ ЦИФРОВОГО СУВЕРЕНІТЕТУ: ПЕРЕДУМОВИ ФОРМУВАННЯ ТА СФЕРИ РЕАЛІЗАЦІЇ

Розглянуто еволюцію поняття «суверенітет» та його особливості в епоху цифровізації. Виділено та проаналізовані основні чинники, що сприяли появі концепції цифрового суверенітету, зокрема комерціалізація цифрової сфери, зростання загроз внутрішній безпеці, боротьба за технологічне лідерство у сфері ШІ та мілітаризація глобальної політики.

Обґрунтовано, що першочерговими сферами, в яких має реалізуватися цифровий суверенітет держави, є інфраструктура, економічна автономія, локалізація даних та автономія користувачів. Відзначено, що забезпечення автономії та безпеки користувачів породжує дилеми у забезпеченні прав і свобод людини.

Ключові слова: *цифровий суверенітет, цифровізація, штучний інтелект, технологія, захист даних, дезінформація, технофеодалізм, кібербезпека, війна.*

Stoiko Olena. **The concept of digital sovereignty: prerequisites for formation and areas of implementation**

The evolution of the concept of sovereignty and its peculiarities in the era of digitalisation are considered. The main factors that contributed to the emergence of the concept of digital sovereignty are identified and analysed, in particular, the commercialisation of the digital sphere, the growth of threats to internal security, the struggle for technological leadership in the field of AI, and the militarisation of global politics.

© *СТОЙКО Олена Михайлівна* – доктор політичних наук, провідний науковий співробітник Інституту держави і права імені В. М. Корецького НАН України; ORCID: 0000-0002-1021-5270

It is argued that the priority areas in which the digital sovereignty of the state should be implemented are infrastructure, economic autonomy, data localisation, and user autonomy. It is noted that ensuring user autonomy and security raises dilemmas in ensuring human rights and freedoms.

Key words: *digital sovereignty, digitalisation, artificial intelligence, technology, data protection, disinformation, techno-feudalism, cybersecurity, war.*

Вступ. На початку появи інтернет-технологій вони розглядалися як такі, що кидають виклик державному суверенітету завдяки своїй атериторіальності та широкому розповсюдженню. Більше того, піонери сучасних інформаційно-комунікаційних технологій розглядали Інтернет як простір свободи, вільний від будь-якого втручання з боку держави [1]. Однак низка чинників змусила держави дедалі більше уваги приділяти регулюванню цифрової взаємодії як між користувачами фізичними особами, так і між органами публічної влади та юридичними особами. Поширення в мережі дезінформації та численні випадки шахрайства (наприклад, використання діпфейків) переконують громадян у необхідності захисту не лише їх особисто, а й життєво важливих суспільних благ, що вимагає дедалі більшого втручання держави у сферу цифрових технологій. Відповідно навіть у демократичних країнах дедалі більше громадян розраховують на захист з боку держави своєї приватності в Інтернеті, боротьби з дезінформацією та кіберзлочинністю, гарантування чесності виборів тощо. Ці та інші чинники сприяли зростанню популярності концепції цифрового суверенітету, який розуміється і як посилення національної держави, дедалі більше втручання держави в економіку, необхідність нормативно-правового врегулювання використання цифрових технологій на регіональному та глобальному рівнях.

Виклад основного матеріалу. У найбільш загальному визначенні цифровий суверенітет можна звести до необхідності контролю за цифровою сферою на фізичному рівні (ресурси, інфраструктура, пристрої), рівні коду (стандарти, правила, дизайн) та рівні інформації (контент, дані) [2]. Контроль передбачає здатність впливати та обмежувати виробництво (включно з отриманням та переробкою необхідної сировини), дизайн, використання та вихідні дані цифрових технологій.

Перші наукові дослідження цифрового суверенітету датуються другим десятиліттям XXI ст, [3; 4], і на сьогодні ця концепція застосовується щодо низки політичних та економічних сфер, від авторитарних режимів до ліберальних демократій. Вона має цілу низку синонімів (технологічний, мережевий, комп'ютерний, інтернет-суверенітет, кіберсуверенітет, суверенітет даних тощо), а її конкретне наповнення залежить від контексту даної країни та домовленостей між учасниками.

Концепція суверенітету була запропонована Ж. Боденом у XVI ст. і наділяла правителя правом приймати остаточні рішення. Ж.-Ж. Руссо зробив акцент на суверенітеті народу, а не правителя, що заклало основи для утвердження демократичної форми правління та принципу верховенства права. Суверенітет означає насамперед незалежність держави від інших держав (зовнішній суверенітет), а також її верховну владу над усіма повноваженнями на території держави (внутрішній суверенітет). Важливою ознакою суверенітету до останнього часу була територія, що розглядається як функціональна передумова для ефективного здійснення влади [5]. Однак у міру розвитку глобалізації та поглиблення регіонального співробітництва (створення таких наднаціональних органів, як Європейський Союз) суверенітет держави почав розмиватися, що дало підстави стверджувати про появу постсуверенного світу, в якому держави втратили свою провідну роль, поступившись місцем недержавним акторам та горизонтальним мережевим структурам. За таких умов визначальною характеристикою демократії стане не народний суверенітет – здатність народу на власний розсуд приймати рішення, а участь та плюралізм думок [6].

Можна виділи такі основні чинники, які сприяли посиленню ролі держави у цифровій сфері та обґрунтовували необхідність появи концепції цифрового суверенітету: комерціалізація цифрової сфери, зростання загроз внутрішній безпеці, боротьба за технологічне лідерство у сфері ШІ та мілітаризація глобальної політики.

1. Комерціалізація цифрової сфери. Зростання загроз державі з боку технологічних гігантів – приватних корпорацій, які концентрують у своїх руках матеріальний та нематеріальний контроль за життєво важливими суспільними структурами [7]. В епоху платформного капіталізму [8] відкритість інтернет-протоколів, на яких засновані цифрові комунікації, втратила своє значення. До того ж

тотальний контроль, які можуть здійснювати такі корпорації за соціальними мережами та інтернет-сервісами, є одним із найбільш серйозних викликів концепції демократичного суверенітету [9; 10]. Оскільки такі технологічні гіганти практично не підзвітні в рамках традиційних механізмів політичної відповідальності, то це змусило низку розвинених демократій, особливо в Європі, переосмислити вимоги до управління цифровими спільнотами [11].

Дедалі більше прихильників завойовує концепція технофеодалізму, згідно з якою цифрові технологічні платформи (Alpabet, Amazon, Apple, Meta, Microsoft) є «цифровими феодалами», які контролюють цифрову інфраструктуру і для яких користувачі – «цифрові кріпаки» – створюють контент. Вони сплачують «хмарну ренту» за доступ до цифрових ресурсів та завдяки активній діяльності у соцмережах (публікації, перегляд реклами тощо) збільшують вартість компаній. Я. Варуфакіс констатує смерть класичного капіталізму та появу технофеодалізму, в якому на перше місце вийшла «рента», а не «прибуток» від виробництва [12].

2. Зростання загроз внутрішній безпеці. Зростання загроз державі у цифровій сфері має місце з боку як недержавних акторів, так і спецслужб іноземних держав. Поворотним пунктом стало оприлюднення у 2013 році американським спецагентом Е. Сноуденом інформації про глобальне стеження з боку розвідувальних служб США та їх союзників [13]. Випадки зливу таємної інформації після повномасштабного російського вторгнення в Україну також значною мірою ослабили довіру між західними союзниками України.

Це змусило держави вжити заходів для посилення свого контролю за цифровою сферою, з дедалі більшою часткою національного контролю за інфраструктурою, збором та обробкою даних, правовим регулюванням використання цифрових технологій. Показовим прикладом є накладення різноманітних обмежень на використання продукції китайських компаній, зокрема Huawei, у європейських країнах та США. Зовнішнє втручання у виборчий процес як у ході ведення передвиборчої агітації (дезінформація, масова реклама в соціальних мережах тощо), так і в ході підрахунку голосів змусила держави посилити контроль за поширенням інформації у мережі та несанкціонованим доступом до мережевої інфраструктури.

3. Боротьба за технологічне лідерство у сфері штучного інтелекту (ШІ). Дедалі ширше використання систем на основі ШІ та

його потенціал для майбутнього технологічного розвитку змусив держави внести зміни до своєї промислової політики, зробивши акцент на підтримку власних моделей ШІ. Російсько-українська війна поглибила технологічне протистояння не лише між демократичними країнами Заходу та авторитарними режимами, насамперед Китаєм, а й виявила розбіжності в інтересах між Євросоюзом та США.

4. Мілітаризація глобальної політики. Повномасштабне російське вторгнення в Україну в лютому 2022 року виявило неготовність нинішньої системи міжнародних відносин адекватно реагувати на збройну агресію, засвідчило розкол серед країн Заходу (як у рамках НАТО, так і Євросоюзу) щодо пріоритетів у зовнішній політиці. Це призвело до збільшення витрат на оборону, значних інвестицій у розвиток власних цифрових технологій для захисту країни в умовах сучасної технологічної війни та від гібридних загроз із боку авторитарних режимів. Зокрема, держави-члени Євросоюзу збільшили оборонний бюджет та вживають заходів для посилення незалежності від США у військово-технологічній сфері в рамках європейської концепції цифрового суверенітету.

Першочерговими сферами, в яких має реалізуватися цифровий суверенітет держави. є інфраструктура, економічна автономія, локалізація даних та автономія користувачів.

У сфері інфраструктури держава повинна мати можливість самостійно вживати заходів і приймати рішення щодо своєї цифрової інфраструктури та впровадження технологій. Більшість цих вимог стосуються географічного обмеження суверенітету конкретною територією та зусиль держав щодо забезпечення безпеки цифрової інфраструктури та їх повноважень у питаннях цифрового зв'язку, що стосуються їхніх територій і громадян. Однією з перших держав, що усвідомила важливість цифрового суверенітету, насамперед у контексті контролю за поширенням інформації серед своїх громадян, став Китай [14; 15; 16]. Він перший почав пропагувати та розвивати ідею цифрового суверенітету, яка в основному формулювалася як кіберсуверенітет або інтернет-суверенітет. Згодом ці ідеї були адаптовані іншими авторитарними режимами, зокрема росією та Північною Кореєю. Уряди демократичних держав на перше місце ставили питання кібербезпеки, що досить швидко стала складовою національної безпеки та почала охоплю-

вати дедалі більше сфер, у тому числі міжнародні відносини [17]. Хоча їх діяльність критикувалася як така, що суперечить ідеалам ліберальної демократії та несе загрозу правам і свободам людини та громадянина [18].

Ще однією сферою, в якій держави почали активно утверджувати свій цифровий суверенітет, стала економічна, що передбачало посилення автономії національної економіки від іноземних постачальників технологій та послуг. У випадку Євросоюзу йшлося про захист свого внутрішнього ринку від домінування американських технологічних компаній як у сфері послуг, так і виробництва технологічних пристроїв. Також низка держав змінила свою стратегію промислового розвитку, прагнучи здійснити цифрову трансформацію цілих секторів економіки. Це стосувалося як традиційних галузей і секторів (телекомунікації, медіа, логістика), так і нових секторів економіки, пов'язаних з ІТ, і насамперед спрямованих на сприяння інноваційній спроможності вітчизняної економіки та підтримку місцевих виробників. Такі кроки також були розкритиковані у західних демократіях як такі, що породжують цифровий протекціонізм та створюють бар'єри для цифрової торгівлі [19].

Третьою сферою утвердження цифрового суверенітету стала політика локалізації даних, що накладала обмеження на зберігання, переміщення та/або обробку даних у певних регіонах та юрисдикціях. Це обґрунтовувалося необхідністю обмежити доступ іноземних розвідувальних служб та корпорацій чи фірм до певних типів даних, наприклад промислових або особистих даних [20]. Як в авторитарних, так і в демократичних країнах заяви та запропоновані заходи, що підкреслюють автономію та самовизначення держав і безпеку критично важливих цифрових інфраструктур, зустріли жорстку критику. Як політичні діячі, так і спостерігачі, такі, як науковці та технічні експерти, побоюються, що зусилля, спрямовані на забезпечення ІТ-безпеки та регулювання питань, пов'язаних з Інтернетом, на національному рівні, можуть завадити відкритому та загальнодоступному характеру Інтернету і зрештою призвести до ретериторіалізації глобального Інтернету, спричинивши його фрагментацію на національні сегменти [21].

Ще одним виміром цифрового суверенітету є одночасне забезпечення автономії та безпеки користувачів, що більш характерно для демократичних країн. Підкреслюючи важливість індивідуального

самовизначення, ці вимоги зосереджуються на автономії громадян у їх ролі працівників, споживачів та користувачів цифрових технологій і послуг. Громадяни розглядаються як споживачі та користувачі цифрових технологій, які мають бути здатними приймати свідомі, раціональні рішення та відповідно діяти. Посилення цих властивостей вимагає проведення від держави не лише просвітницької політики, а й впровадження механізмів захисту із максимальним дотриманням прав і свобод людини та громадянина.

Досягти цього можна за допомогою різноманітних економічних стимулів для розробки зручних для користувачів насамперед вітчизняних технологій, а також впровадження технічних функцій, що забезпечують ефективне шифрування, захист даних і більш прозорі бізнес-моделі. Крім того, проводяться заходи щодо підвищення медіа- та цифрової грамотності громадян, тим самим зміцнюючи компетенції та впевненість користувачів і споживачів у цифровій сфері та розвиваючи критичне мислення й свідоме ставлення користувачів до технологій та власних даних. Водночас акцент на автономії та безпеці споживачів сприяє зміцненню національної безпеки, але може призвести до обмеження фундаментальних прав користувачів, таких, як приватність або свобода вираження поглядів.

Отже, концепція цифрового суверенітету охоплює досить широку сферу питань, включаючи не тільки питання комунікаційної інфраструктури, а й набагато ширшу цифрову трансформацію суспільств. Цифровий суверенітет часто використовується для позначення впорядкованої, ціннісно орієнтованої, регульованої та безпечної цифрової сфери. Використання цієї концепції має сприяти розв'язанню складних проблем індивідуальних прав і свобод, колективної та інфраструктурної безпеки, посилення демократичних інституцій та людиноцентричного технологічного розвитку.

1. Barlow J. P. A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation (1996). URL: https://www.eff.org/ cyberspace-independence **2.** Chander A., Sun H. Sovereignty 2.0. Georgetown Law Faculty Publications and Other Works, 2404. URL: https://doi.org/10.2139/ssrn.3904949 **3.** Mueller M.L. Will the internet fragment? Sovereignty, globalization and cyberspace. Oxford: Polity, 2017. 140 p. **4.** Couture S., Toupin S. What does the notion of 'sovereignty' mean when referring to the digital? New Media & Society. 2019. Vol. 21. № 2. P. 2305–2322. **5.** Grimm D. Sovereignty: The

Origin and Future of a Political and Legal Concept. New York: Columbia University Press, 2015. 192 p. **6.** MacCormick N. Questioning Sovereignty: Law, State, and Nation in the European Commonwealth. Oxford: Oxford University Press, 1999. 222 p. **7.** Christl W. Corporate Surveillance In Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions. [Report, 2017]. URL: http://crackedlabs.org/en/ corporate-surveillance. **8.** Srnicek N. The challenges of platform capitalism. Understanding the logic of a new business model. *Juncture*. 2017. Vol. 23. №4. P. 254–257. **9.** Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019. 704 p. **10.** Hindman M. The Internet trap: How the digital economy builds monopolies and undermines democracy. Princeton: Princeton University Press, 2018. 274 p. **11.** van Dijck J. Governing digital societies: Private platforms, public values. *Computer Law & Security Review.* 2020. Vol. 36. URL: https://doi.org/10.1016/j.clsr.2019.105377. **12.** Varoufakis Y. Technofeudalism: What Killed Capitalism. Vintage, 2024. **13.** Tréguer F. 2018. US Technology Companies and State Surveillance in the Post-Snowden Context: Between Cooperation and Resistance. (Research Report No. 5; UTIC Deliverables, 2018. URL: https://halshs.archives- ouvertes.fr/halshs-01865140. **14.** Creemers R. 2020. China's Conception of Cyber Sovereignty. *Governing Cyberspace: Behavior, Power and Diplomacy* / ed. by D. Broeders, B. van den Berg. London: Rowman & Littlefield, 2020. P. 107-145. **15.** Jiang M. Authoritarian Informationalism: China's Approach to Internet Sovereignty. *SAIS Review of International Affairs.* 2010. Vol. 30. №3. P. 71–89. **16.** Zeng J., Stevens T., Chen Ya. China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of «Internet Sovereignty». *Politics & Policy.* 2017. Vol. 45. № 3. P. 432–464. **17.** Hansen L., Nissenbaum H. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly.* 2009. Vol. 53. №4. P. 1155–1175. **18.** Möllers N. Making Digital Territory: Cybersecurity, Technonationalism, and the Moral Boundaries of the State. *Science, Technology, & Human Values*. 2020. Vol. 46. № 1. P. 112–138. https://doi. org/10.1177/0162243920904436. **19.** Aaronson S.A., Leblond P. Another digital divide: The rise of data realms and its implications for the WTO. *Journal of International Economic Law.* 2018. Vol. 21. №2. P. 245–272.**20.** Hill J.F. The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders. *Lawfare Research Paper Series.* 2014. Vol. 2. №3. P. 1–41. **21.** Mueller M.L. Will the internet fragment?: Sovereignty, globalization and cyberspace. Oxford: Polity, 2017. 140 p.

Stoiko Olena. **The concept of digital sovereignty: prerequisites for formation and areas of implementation**

The evolution of the concept of sovereignty and its peculiarities in the era of digitalisation are considered. The main factors that contributed to the emergence of the concept of digital sovereignty are identified and analysed, in particular,

the commercialisation of the digital sphere, the growth of threats to internal security, the struggle for technological leadership in the field of AI, and the militarisation of global politics. The commercialisation of the digital sphere is driven by growing threats to the state from tech giants – private corporations that hold material and immaterial control over vital social structures. Threats to the state's internal security are growing, both from non-state actors and foreign intelligence services. The struggle for technological leadership in the field of artificial intelligence (AI) is driven by the fact that the increasingly widespread use of AI-based systems and their potential for future technological development has forced states to make changes to their industrial policies, placing an emphasis on supporting their own AI models. The Russian-Ukrainian war has not only deepened the technological confrontation between the democratic countries of the West and authoritarian regimes, primarily China, but has also revealed differences in interests between the European Union and the United States.

The militarisation of global politics was the result of Russia's full-scale invasion of Ukraine in February 2022, which revealed the current system of international relations' inability to respond adequately to armed aggression and highlighted divisions among Western countries (both within NATO and the European Union) over foreign policy priorities.

It is argued that the priority areas in which the digital sovereignty of the state should be implemented are infrastructure, economic autonomy, data localisation, and user autonomy. It is noted that ensuring user autonomy and security raises dilemmas in ensuring human rights and freedoms.

The concept of digital sovereignty covers a fairly broad range of issues, including not only communication infrastructure, but also the much broader digital transformation of societies. Digital sovereignty is often used to refer to an orderly, value-oriented, regulated and secure digital sphere. The use of this concept should contribute to solving complex problems of individual rights and freedoms, collective and infrastructure security, strengthening democratic institutions and human-centred technological development.

Key words: digital sovereignty, digitalisation, artificial intelligence, technology, data protection, disinformation, techno-feudalism, cybersecurity, war.