

**КОНЦЕПЦІЯ ЦИФРОВОГО СУВЕРЕНІТЕТУ ДЕРЖАВИ:
МІЖНАРОДНО-ПРАВОВИЙ АСПЕКТ****THE CONCEPT OF DIGITAL SOVEREIGNTY OF THE STATE:
INTERNATIONAL LEGAL ASPECT**

**Лабик А.Р., асистентка кафедри міжнародного права
та порівняльного правознавства**

Чернівецький національний університет імені Юрія Федьковича

**Яремчук В.В., д.філос.,
асистент кафедри міжнародного права
та порівняльного правознавства**

Чернівецький національний університет імені Юрія Федьковича

Стаття присвячена дослідженню поняття цифрового суверенітету як нової категорії міжнародно-правової науки, активна розробка якої розпочалася не більше п'яти років тому у відповідь на прискорені темпи глобалізації та розширення впливу мережі Інтернет, що все частіше кидають виклик традиційному розумінню держави, суверенітету, територіального верховенства. Поступова дифузія цифрових технологій у більшість сфер життя суспільства перетворюється на справжній виклик для урядів держав і світової спільноти, оскільки низький ступінь регламентації і контролю даної галузі веде до цілої низки ризиків, пов'язаних із кібершахрайством, викраденням інформації, несанкціонованим використанням і поширенням персональних даних, іншими порушеннями прав людини.

У статті досліджено передумови виникнення концепції цифрового суверенітету, проаналізовано окремі випадки його реалізації державами. На основі з'ясування суті державного суверенітету, запропонованого Ж. Боденом та його послідовниками, розкрито правову природу цифрового суверенітету як властивості держави, зумовленої її роллю в регулюванні кіберпростору. Розглянуто види підходів до визначення цього поняття, які наразі панують у політичній та науковій думці. За основу такої систематизації взято суб'єктний склад права на цифрову автономію, тобто можливості самостійно ухвалювати рішення та вчиняти дії, пов'язані з діяльністю на теренах телекомунікаційних мереж. Перша теорія обґрунтовує цифровий суверенітет держави, тим самим санкціонуючи втручання останньої до цифрової сфери. Основними мотивами такого втручання виступають контроль (авторитаристський підхід) або безпека кіберсередовища (ліберальний підхід). Друга концепція наділяє цифровим суверенітетом великі технологічні корпорації та переслідує мету забезпечення розвитку національних галузей економіки й обмеження допуску іноземних надавачів послуг до власного ринку. Третя – виражається у цифровій автономії індивіда, наділеного повноваженнями самостійно ухвалювати необхідні рішення та контролювати власну діяльність у цифровому середовищі.

Ключові слова: цифровий суверенітет, суверенітет держави, цифрові права людини, цифрова автономія, міжнародно-правове регулювання Інтернету.

The article is devoted to the study of the concept of digital sovereignty as a new category of international legal science, which began to be actively developed no more than five years ago in response to the accelerated pace of globalisation and the expanding influence of the Internet, which increasingly challenge the traditional understanding of the State, sovereignty and territorial supremacy. The gradual diffusion of digital technologies into most spheres of society is turning into a real challenge for governments and the international community, as the low degree of regulation and control of this industry leads to a number of risks associated with cyber fraud, information theft, unauthorised use and dissemination of personal data, and other human rights violations.

The article examines the prerequisites for the emergence of the concept of digital sovereignty and analyses some cases of its implementation by States. Based on the definition of state sovereignty proposed by J. Baudin and his followers, the author reveals the legal nature of digital sovereignty as a property of the state due to its role in regulating cyberspace. The author examines the types of approaches to the definition of this concept which currently prevail in political and scientific thought. The basis for this systematisation is the subjective composition of the right to digital autonomy, i.e. the ability to make decisions and take actions related to activities within telecommunication networks independently. The first theory justifies the digital sovereignty of the state, thereby authorising the latter's intervention in the digital sphere. The main motives for such intervention are control (authoritarian approach) or security of the cyber environment (liberal approach). The second concept grants digital sovereignty to large technology corporations and aims to ensure the development of national industries and restrict the access of foreign service providers to their own market. The third concept is expressed in the digital autonomy of the individual, who is empowered to make the necessary decisions and control his or her own activities in the digital environment.

Key words: digital sovereignty, state sovereignty, digital human rights, digital autonomy, international legal regulation of the Internet.

Постановка проблеми. Стрімкий розвиток цифрових технологій, свідком якого стало людство, відкрив неімовірні перспективи для кожного: від нових можливостей в освіті, науці, медицині до полегшення ведення побуту та урізноманітнення дозвілля. Здавалося б, ще наприкінці 1990-х років «розумний» дім був лише плодом уяви письменників-фантастів та сценаристів художніх фільмів у жанрі кіберпанку і наукової фантастики. Тим не менше, сьогодні будь-хто може скористатися благами систем автоматизації житла за наявності достатніх ресурсів. Більше того, Україна уже п'ятий рік реалізує концепцію «Держава у смартфоні» через вебпортал і мобільний застосунок «Дія», яка практично не має аналогів у світі. Українці чи не першими отримали змогу скористатися державними послугами онлайн та використовувати електронні документи, що за юридичною силою були прирівняні до паперових.

Зростання ролі інтернет-технологій, запровадження 5G-зв'язку, еволюція штучного інтелекту стали поштовхом для прискорення цифровізації економіки та суспільства. Суттєво пришвидшились темпи оцифрування величезної кількості даних у різноманітних сферах, що передбачає перетворення інформації в машиночитний формат для спрощення процесів її збирання, зберігання та аналізу. Разом з тим, це спричинило також зростання ризиків, пов'язаних зі збереженням та захистом особистих даних користувачів, отриманих через процедури онлайн-ідентифікації та автентифікації, трансформації паперових носіїв у цифрові. Оскільки кіберпростір був тісно вплетений до приватного життя особи, її персональна інформація, профіль в соціальних мережах, діяльність і поведінка в Інтернеті стали його невіддільною частиною [1, с. 62]. Це, у свою чергу, привело до зародження у практиці окре-

мих держав та міжнародних організацій концепції цифрових прав людини, покликані вберегти приватних осіб від ризиків, породжених всеохопною цифровізацією. Варто нагадати, що Європа стала справжнім «першопроходцем» у даній сфері, адже саме тут було закладено основи міжнародно-правового визнання та нормативної регламентації цифрових прав [2, с. 260].

Безперечно, сучасні тенденції в галузі цифровізації та глобалізації залишають суттєвий відбиток на правах і свободах людини, розширюючи не лише їх перелік, а й зміст. Прикметно, що це не єдиний напрямок їх впливу – не варто недооцінювати виклики, з якими стикаються держави, вимушені адаптувати внутрішнє законодавство та національні правозахисні механізми до умов сьогодення. Враховуючи специфіку цифрових технологій, які часто мають мінливий, хаотичний, та, разом з тим, всеохопний характер, можливість їх контролю видається щонайменше проблематичною, якщо не неможливою. У зв'язку з цим, принципи державного суверенітету і територіальності вступають у протиріччя із універсальністю та гнучкістю сучасних телекомунікаційних мереж. Ще 1996 року американський поет і один із засновників сучасного Інтернету, вільного та доступного для кожного, Джон Перрі Барлоу у своїй скандальній Декларації незалежності кіберпростору прогнозував зникнення держав і неспроможність державного суверенітету протистояти свободі глобальних мереж, які не мають кордонів та фізичного виразу [3]. Звісно, сьогодні це передбачення здається малоімовірним та згадується переважно як погроза у відповідь на ухвалення Акта про пристойність у сфері комунікацій США, проте спонукає замислитись над значенням держав у процесах цифровізації. Протягом майже трьох десятиліть останні робили все можливе, щоб переконати громадськість у власній виключній ролі щодо гарантування безпечності глобальних мереж, свободи слова, захисту персональних даних тощо. Поступове удосконалення правових механізмів та адаптація національних правових систем до викликів ХХІ століття змогли закріпити мандат урядів на втручання до цифрової сфери [4, с. 2]. Як наслідок, останнім часом у політичних та наукових колах почала формуватися концепція цифрового суверенітету держави.

Стан дослідження. Хоч питання ролі держави у процесах цифровізації та регулювання кіберпростору виникли ще в середині 90-х років минулого століття, ідея цифрового суверенітету зародилася порівняно нещодавно і залишається розробленою на досить низькому теоретичному рівні. Це зумовлено тривалим домінуванням у наукових колах думки про несумісність таких понять як державний суверенітет та глобальні мережі. Тим не менше, із 2019-2020 рр. спостерігаємо підвищення уваги до даного інституту, що зумовлено зростанням потреб світового співтовариства щодо гарантування безпеки цифрового простору, захисту персональних даних особи, забезпечення їх справедливого балансу зі свободою діяльності в Інтернеті та свободою ЗМІ. Так, проблеми з'ясування сутності та визначення підходів до розуміння концепції цифрового суверенітету досліджували Дж. Поль, Т. Тіль, С. А. Ааронсон, А. Баумс, А. Бендік, Ф. Бріа, Ж.-М. Шену, Р. Крімерз, К. Гоббс, Л. Флоріді, К. Л. Тан та інші.

Метою статті є з'ясування сутності поняття цифрового суверенітету на основі аналізу сучасних концепцій його розуміння у рамках міжнародно-правової науки.

Виклад основних положень. Незважаючи на те, що концепція цифрового суверенітету перебуває на етапі свого становлення, приклади її реалізації можемо знайти в нормативних актах та заявах багатьох держав. Зокрема, ще в 2020 році держсекретар США М. Помпео оголосив про намір уряду заборонити соціальну мережу «TikTok», пояснюючи це ризиками для національної безпеки Сполучених Штатів. Враховуючи значну популярність мережі,

аналітики вказували на можливості для Китаю збирати особисті дані американських громадян та впливати на формування громадської думки в Сполучених Штатах. Відповідна заборона була реалізована із набуттям чинності Акта про захист американців від програм, контрольованих іноземними противниками 19 січня 2025 року [5, с. 370; 6]. Обмеження щодо користування «TikTok» на робочих пристроях державних службовців із березня 2023 року діє також у Великій Британії. Таке рішення уряду було обґрунтоване необхідністю гарантування безпеки даних, доступ до яких можна отримати через девайси посадовців [7]. У 2020 році, після провалу плану підготовки власної централізованої програми по збору та аналізу інформації щодо осіб, хворих на COVID-19, яка б не базувалася на API, отриманому від Google або Apple, британський уряд повністю відмовився від реалізації проекту. Того ж 2020 року Суд ЄС визнав недійсною угоду про захист персональних даних між ЄС та США в рамках діяльності щодо передачі інформації європейських користувачів на американські процесори, оскільки Сполучені Штати не надали достатніх гарантій безпеки особистих даних [5, с. 370]. Окрім цього, у липні 2020 року на початку свого піврічного головування у Раді Європейського Союзу уряд Німеччини заявив про намір «встановити цифровий суверенітет як лейтмотив європейської цифрової політики». Це була одна із небагатьох офіційних заяв, у яких було використано термін «цифровий суверенітет» як підґрунтя ідеї щодо контролю на всесвітньою мережею та захисту суспільства від різноманітних викликів цифровізації [4, с. 2].

Переходячи власне до поняття цифрового суверенітету, відзначимо, що наразі ні в міжнародному праві, ні в національних правових системах не існує його визначення. Більше того, сам термін використовується надзвичайно рідко. З огляду на це, формулювання дефініцій та тлумачення сутності цього поняття відбувається виключно на доктринальному рівні. Для того, щоб з'ясувати, що ж таке цифровий суверенітет, розпочнемо із державного суверенітету як такого.

Засновником теорії державного суверенітету вважається французький філософ Жан Боден, який на основі ідей своїх попередників зумів виокремити наріжний камінь абсолютної влади монарха – суверенітет. Дослідник обґрунтовував унікальність правового становища суверена, якого вважав джерелом закону та найвищою владою в державі, що стоїть вище всіх інших осіб. Монарх, на думку Ж. Бодена, не підпорядковувався жодним законам: ні тим, що були ухвалені ним самим, ні тим, що існували до нього. Єдиним винятком із цього твердження були закони Божі і закони природи. Акцентуючи увагу на такій характеристиці суверенітету як необмеженість, філософ визначав його як «абсолютну та постійну владу, яку римляни називають величчю, що означає вищу владу повелівати» [8, с. 314]. Значні трансформації, яких зазнали суспільні відносини з XVI століття і до нашого часу, змусили науковців переосмислити концепцію, розвинену Ж. Боденом та його послідовниками. Відкидаючи існування «часткового» суверенітету, сучасні дослідники, разом з тим, обґрунтовують відхід від «абсолютності» як необхідність в умовах глобалізації. Тим не менше, це не змінює суті державного суверенітету, який розкривається через зовнішній (незалежність від будь-якої іншої влади) та внутрішній (верховенство влади щодо всіх суб'єктів у межах кордонів держави) аспекти [9, с. 11-12]. Він визначає можливості кожної держави самостійно здійснювати верховенство влади на власній території без втручання ззовні.

Поняття цифрового суверенітету на сьогодні суттєво залежить від національних умов, географічного розташування, усталених практик і традицій, які склалися у тому чи іншому регіоні. Наразі можемо говорити про існування трьох підходів до визначення цифрового суверенітету.

Критерієм для їх систематизації слугує категорія суб'єкта цифрового самовизначення. Отже, згідно із першою теорією, єдиним суб'єктом, уповноваженим на здійснення цифрового суверенітету, виступає держава. Лише їй належать права щодо вжиття дій і прийняття рішень у відповідній сфері, які, проте, обмежені її кордонами. Варто відзначити, що прихильники даного підходу розділяються на дві окремі течії: одні зосереджують увагу на здійсненні контролю за кіберпростором (можна простежити на прикладі Китаю та інших авторитарних держав), другі основний акцент роблять на інформаційній гігієні та безпеці (дана теорія зародилася та була розвинена в Європі). Найголовнішими ознаками концепції цифрового самовизначення держави є її регіональний характер, локалізація даних, широкі повноваження щодо обмеження доступу до телекомунікаційних мереж. Другий підхід заснований на автономії національної економіки та самовизначенні технологічних компаній. Подібно до першої теорії, його реалізація зумовлена, насамперед, питаннями безпеки, проте не обмежується ними. Основний акцент його прихильники роблять на розвитку конкурентоспроможності та національної автономії місцевих телекомунікаційних компаній, зниженні залежності від іноземних технологій, підвищенні інноваційних потужностей держави. Йому також притаманний локальний характер інформації і цифрових послуг, та, на відміну від теорії цифрової автономії держави, він вирізняється менш жорстким контролем та більшою свободою кіберпростору. І, нарешті, третя концепція, яка виникла найпізніше, побудована на індивідуальному самовизначенні користувача. На відміну від традиційного державоцентричного розуміння суверенітету, цей підхід зосереджений на автономії окремих осіб, здатних свідомо і самостійно приймати будь-які рішення чи вчиняти будь-які дії, що стосуються її як одержувача відповідних цифрових послуг. У даному випадку державі виділено другорядну роль суб'єкта, який не контролює, а лише задовольняє потреби індивіда щодо гарантування ефективного шифрування, безпеки даних, підвищення цифрової грамотності тощо [4, с. 8-12].

Загалом проаналізований підхід до систематизації концепцій цифрового суверенітету має значну цінність для подальших наукових досліджень, оскільки демонструє реальне ставлення різних країн світу до цього поняття, його визнання чи заперечення. Разом з тим, йому притаманні також окремі недоліки, одним із яких є довільне використання категорії «суверенітет» щодо фізичних та/або юридичних осіб. Відзначимо, що в контексті дослідженої проблематики більш доцільним видається термін «автономія», який розкриває можливості конкретного користувача або компанії самостійно визначати власну траєкторію у цифровому просторі та нести всі ризики, які з цього випливають. Сюди не входять повноваження із прийняття управлінських рішень та здійснення контролю в даній галузі, що власне і випливає зі змісту запропонованих авторами концепцій. Тож, очевидно, що саме перша теорія – цифрової автономії держави – відповідає класичним уявленням про державний суверенітет. Відповідно до неї, цифровий суверенітет можна визначити як політико-правову властивість держави, що виражається у встановленні нею нормативного механізму регламентації та контролю за діяльністю надавачів і користувачів цифрових послуг у межах її державної території.

Висновки. Насамкінець відзначимо, що, зважаючи на відносно недовгу історію існування концепції цифрового суверенітету, ця сфера відкриває безліч можливостей для подальших наукових досліджень. Розвиток інформаційних технологій і глобальна цифровізація породжують незліченну кількість правових питань, які наразі залишаються невирішеними. Серед них: визначення характеру і меж втручання держави до цифрового простору, роль міжнародних організацій у регулюванні даної сфери, обмеження свободи діяльності особи в Інтернеті та її підстави, необхідність створення міжнародних стандартів регулювання кіберпростору, механізми захисту прав людини у всесвітній мережі та багато інших. Таким чином, розробка концепції цифрового суверенітету має суттєве значення для вдосконалення як міжнародно-правового, так і внутрішньодержавного регулювання цифрового простору, адаптації права до викликів сьогодення.

ЛІТЕРАТУРА

1. Tan K. L., Chi C. H., Lam K. Y. Survey on digital sovereignty and identity: From digitization to digitalization. *ACM Computing Surveys*, 2023. № 56 (3). P. 61-96. URL: <https://dl.acm.org/doi/abs/10.1145/3616400> (дата звернення: 28.02.2025).
2. Лабик А. Р., Строїч М. І., Іліка М. І. Виклики міжнародно-правової регламентації права на забуття в Інтернеті. *Науковий вісник Ужгородського Національного Університету. Серія Право*. 2024. Випуск 86. С. 258-263. URL: <http://visnyk-pravo.uzhnu.edu.ua/article/view/321390/311925> (дата звернення: 28.02.2025).
3. Barlow J. P. A Declaration of the Independence of Cyberspace. Davos, 1996. URL: <https://www.eff.org/cyberspace-independence> (дата звернення: 28.02.2025).
4. Pohle J., Thiel T. Digital sovereignty. *Internet Policy Review*. 2020. № 9 (4). P. 1-19. URL: <https://doi.org/10.14763/2020.4.1532> (дата звернення: 28.02.2025).
5. Floridi L. The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & technology*. 2020. № 33. P. 369-378. URL: <https://link.springer.com/article/10.1007/s13347-020-00423-6> (дата звернення: 28.02.2025).
6. У США заборонено TikTok. Чому і що буде далі? *BBC news Україна*. 19.01.2025. URL: <https://www.bbc.com/ukrainian/articles/cr3wyqvzll9o> (дата звернення: 28.02.2025).
7. TikTok banned on UK government devices as part of wider app review. *Government: news*. 16.03.2023. URL: <https://www.gov.uk/government/news/tiktok-banned-on-uk-government-devices-as-part-of-wider-app-review> (дата звернення: 28.02.2025).
8. Мельниченко В. С. Абсолютність державного суверенітету в уявленнях мислителів XVI–XIX ст. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. № 4 (84). С. 311-317. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/09/46-2.pdf> (дата звернення: 28.02.2025).
9. Державний суверенітет в умовах глобалізації: теорія та практика : монографія / Н. А. Бабарикіна, Н. В. Горло, М. Ф. Заболотна, О. М. Кіндратець, Т. І. Сергієнко; за заг. ред. О. М. Кіндратець. Запоріжжя : Запорізький національний університет, 2022. 226 с. URL: <https://dspace.znu.edu.ua/jspui/handle/12345/11735> (дата звернення: 28.02.2025).