

РОЗДІЛ 2. ПОЛІТИЧНІ ІНСТИТУТИ ТА ПРОЦЕСИ

Балан Сергій Вікторович

Зміна парадигми сприйняття інформаційного суверенітету в умовах транзиту до інформаційної держави

УДК 32.329

DOI <https://doi.org/10.24195/2414-9616.2025-3.2>

Балан Сергій Вікторович
кандидат політичних наук, старший науковий співробітник
Інституту держави і права
імені В. М. Корецького Національної академії наук України
вул. Трьохсвятительська, 4, Київ,
Україна
ORCID: 0000-0002-9421-7037

Актуальність даної статті визначається зростанням ролі інформаційного суверенітету як провідної властивості сучасної інформаційної держави, що легітимізує державну владу та уможливорює реалізацію суверенних прав. У статті досліджуються політичні та правові основи інформаційного суверенітету як ключового принципу в архітектурі сучасної інформаційної держави. Проаналізовано концептуальні визначення, історичну еволюцію та інституційні механізми, за допомогою яких держави здійснюють контроль над інформаційним простором. Спираючись на міждисциплінарну літературу, у статті обґрунтовується теза, що інформаційний суверенітет не є сталою юридичною категорією, а є дискурсивним і стратегічним процесом, зміст якого варіюється залежно від національних можливостей та пріоритетів політики окремо взятої національної держави. Висвітлено структурні виклики, пов'язані з цифровою глобалізацією, і підкреслено, як інформаційний суверенітет лежить в основі економічних, політичних, гуманітарних і воєнних вимірів державності. Зрештою, зроблено висновок, що інформаційна держава визначається її здатністю підтримувати та захищати свій інформаційний суверенітет, що робить його центральним організаційним принципом сучасного врядування. У статті також представлено порівняльний аналіз підходів до забезпечення інформаційного суверенітету в різних країнах. Зроблено акцент на відмінностях між нормативною, технічною та юридичною формами суверенітету. Автор стверджує, що ефективне забезпечення інформаційного суверенітету вимагає балансу між контролем і відкритістю, суверенітетом і співпрацею, безпекою і правами людини. Особлива увага приділяється ролі держави у формуванні власної цифрової інфраструктури як ключової передумови збереження політичної автономії в умовах глобальної конкуренції за контроль над інформаційними потоками.

Ключові слова: інформаційний суверенітет, інформаційна держава, інформаційний простір, дезінформація, суверенні права.

Вступ. З настанням інформаційної доби й активного розвитку цифрових технологій докорінно трансформувалося сприйняття природи держави, принципів врядування та суті державного суверенітету. Відтак у цьому контексті поняття інформаційного суверенітету постає в якості ключового принципу, що визначає здатність сучасних держав контролювати, регулювати та захищати інформацію як у межах своїх кордонів, так і за їх межами шляхом вироблення і закріплення універсальних за переліком і сферою поширення правил поведінки з інформацією у мережі. По мірі проникнення цифрових технологій у всі сфери політичного, економічного та соціального життя, держави змушені переосмислювати питання функціонального суверенітету у термінах управління інформацією та забезпечення інформаційної безпеки як самої держави, так і її громадян [4; 7].

Швидке поширення інформаційно-комунікаційних технологій змусило переосмислити структуру сучасного врядування, давши підстави науковцям усе частіше говорити про появу «інформаційної держави» [2]. У цьому контексті концепт інфор-

маційного суверенітету – тобто здатності держави регулювати та захищати інформаційні процеси в межах своєї виключної юрисдикції – набуває центрального значення в сучасній політичній та правовій теорії. Попри те, що поняття інформаційного суверенітету досі еволюціонує, воно відіграє вирішальну роль у визначенні меж національної автономії, легітимності державної влади та законної сили в цифрову епоху.

Інформаційна держава – це не просто держава, яка широко впроваджує і використовує цифрові технології, а та, в якій сама інформація стає центральним об'єктом врядування, джерелом влади та полем конкуренції й конфлікту. Відтак здатність управляти даними, інформаційною інфраструктурою, наративами та технологічними стандартами перетворюється на фундаментальний елемент сучасного державного управління, що складає суть поняття інформаційний суверенітет. Наявність інформаційного суверенітету є однією з головних ознак інформаційної держави, а захист інформаційного суверенітету відповідно – однією з ключових функцій держави на нинішньому етапі розвитку суспільних відносин.

Метою дослідження є з'ясування значення інформаційного суверенітету для функціонування держави нового типу – інформаційної.

Методологічну основу дослідження становлять інституціональний, структурно-функціональний і порівняльний (компаративний) підходи.

Інституціональний метод було використано для аналізу закономірностей розвитку (інформаційної) держави як соціального інституту та виявлення її головних ознак, до яких належить зокрема інформаційний суверенітет. Структурно-функціональний метод використовувався для аналізу інформаційної держави як системи, структурним елементом якої є інформаційний суверенітет, що виконують певні функції. В межах структурно-функціонального методу інформаційна держава розглядається в якості соціальної системи, однією з головних функцій якої є захист інформаційного суверенітету як ключової властивості, передумови для забезпечення соціального порядку на національному і глобальному рівнях, що гарантує оптимальне функціонування демократичних інститутів і забезпечує можливість дотримання демократичних процедур, а також сталість політичного режиму. Порівняльний метод використовувався для аналізу відмінностей у підходах до практичного забезпечення інформаційного суверенітету.

У цій статті досліджуються політико-правові аспекти інформаційного суверенітету. Стверджується, що в сучасній інформаційній державі інформаційний вимір суверенітету формується внаслідок дискурсивної взаємодії політичних акторів.

Серед вітчизняних науковців, які досліджували різні аспекти інформаційного суверенітету, варто згадати О. Баранова, О. Гічка, В. Горового, О. Довганя, Д. Дубова, С. Куцепал, О. Онищенко, В. Пилипчука, Ю. Половинчак, О. Солодку, Т. Ткачука, О. Ярему та ін.

Результати. За останні дві декади серед дослідників відбулася глибока трансформація уявлень про суть, ознаки і роль інформаційного суверенітету. Під впливом розвитку інформаційно-комп'ютерних технологій зростає загальне розуміння вразливості як глобального, так і національного інформаційного простору від зовнішнього шкідливого втручання, яке часто здійснюється підтримуваними урядами окремих держав організаціями та/або організованими кіберзлочинними угрупованнями шляхом кібератак або (дез)інформаційних кампаній. Відсутність фізичних кордонів національного інформаційного простору посилена обмеженими можливостями впливу переважної більшості держав на власників інформаційної інфраструктури (ПЗ, кабелів, супутників, дата-центрів тощо) та популярних онлайн-платформ (Google, Facebook, X, TikTok тощо) перетворює функцію забезпечення інформаційного суверенітету на стратегічний виклик, ігнорування якого несе низку

екзистенційних загроз. Відтак активно змінюються підходи до визначення суті інформаційного суверенітету, його місця і ролі в структурі державного суверенітету та механізмів забезпечення.

Політичний і територіальний суверенітет, які донедавна вважалися основоположними атрибутами незалежності держави, поступово втрачають пріоритет у переліку об'єктів, які потребують захисту з боку держави, і водночас ключових сфер зовнішнього втручання з боку міжнародних акторів. Натомість інформаційний простір виявився набагато вразливішим до стороннього шкідливого впливу. До того ж критерії оцінки стану інформаційного суверенітету в кожній окремо визначеній державі є занадто суб'єктивними, що суттєво ускладнює процес вироблення й імплементації державних політик, спрямованих на його захист. Так, ще відносно недавно інформаційний суверенітет розглядався здебільшого як один з похідних проявів державного суверенітету і стосувався спроможностей держави контролювати медійний простір за допомогою цензури та обмеження доступу для закордонних медіа. В контексті формування інформаційної держави такі обмеження більше не дають бажаного ефекту через глобалізацію інформаційного простору, каталізатором якої виступає цифровізація суспільно-політичних відносин та сфери державного управління зокрема.

З огляду на зростання важливості забезпечення процесів створення, збору, передачі, зберігання і використання інформації у глобальному вимірі ООН виступила ініціатором проведення Всесвітнього саміту з питань інформаційного суспільства (World Summit on the Information Society, WSIS) – зустрічі на вищому рівні, яку було проведено у два етапи: у Женеві 10–12 грудня 2003 року, що завершилася ухваленням Женевської Декларації принципів «Побудова інформаційного суспільства: глобальний виклик в новому тисячолітті» і Женевського Плану дій; та в Тунісі 16–18 листопада 2005 року, за результатами якої були ухвалені Туніське зобов'язання і Туніський Порядок денний для інформаційного суспільства.

Перший раунд Всесвітнього саміту з питань інформаційного суспільства, що проходив у Женеві у грудні 2003 року, став першою глобальною спробою багатьох зацікавлених сторін (влада, бізнес, громадянське суспільство) виробити спільне бачення інформаційного суспільства, яке розширює можливості та приносить користь усім людям. Визначним досягненням саміту став консенсус довкола Декларації принципів та Плану дій.

Женевська Декларація принципів чітко зафіксувала, що зміцнення системи довіри, включаючи інформаційну безпеку та мережеву безпеку, автентифікацію, конфіденційність та захист прав споживачів, є необхідною умовою для розвитку інформаційного суспільства та зміцнення

довіри серед користувачів ІКТ. В документі наголошується на тому, що глобальну культуру кібербезпеки необхідно просувати, розвивати та впроваджувати у співпраці з усіма зацікавленими сторонами та міжнародними експертними органами. Ці зусилля повинні підтримуватися посиленням міжнародної співпраці. У рамках цієї глобальної культури кібербезпеки важливо посилювати безпеку та забезпечувати захист даних і конфіденційності, одночасно розширюючи доступ і торгівлю. Крім того, необхідно враховувати рівень соціально-економічного розвитку кожної країни та поважати аспекти інформаційного суспільства, орієнтовані на розвиток. Відтак можемо констатувати, що вже на початку XXI століття на глобальному рівні існувало розуміння необхідності посилення інформаційного суверенітету [10].

Понад те, пріоритет розбудови інфраструктури для забезпечення безпеки в мережі Інтернет має відбуватися в багатосторонньому форматі і одночасно охопити всі зацікавлені сторони: державних службовців, бізнесові структури, медіа, наукові кола й аналітичні центри, неурядові організації тощо [10].

Потреба в нарощуванні потенціалу у сфері управління Інтернетом та формуванням відповідних політик була визнана одним із пріоритетів порядку денного також і на Туніському раунді Всесвітнього саміту інформаційного суспільства (WSIS) [12].

У 2020 році у програмі німецького головування в Раді Європейського Союзу «Разом до європейського відновлення» з'явилася згадка про «цифровий суверенітет» («digital sovereignty»), який, за задумом авторів, мав гарантувати Європі найсучасніші навички в галузі ключових цифрових технологій за умови збереження відкритості єдиного європейського ринку. Цифровий суверенітет також має включати створення високопродуктивної, суверенної та стійкої європейської цифрової інфраструктури [9].

Низка міжнародних організацій обговорюють можливі моделі співпраці у створенні програм для посилення безпекової інфраструктури в мережі Інтернет, зокрема Рада Європи і Міжнародна спілка електрозв'язку (ITU). Наразі існує консенсус щодо того, що у довгостроковій перспективі буде необхідним оновлення навчальних програм, в першу чергу, шкільних, задля включення до них тем, пов'язаних з безпекою в мережі Інтернет, таких як: захист власної конфіденційності та безпеки, захист особистої та чужої репутації, мережева етика, повідомлення про насильство тощо. Кілька таких ініціатив вже існують, наприклад: CyberSmart, iKeepSafe, i-Safe, NetSmartz [6, с. 152].

Політична концепція суверенітету у розумінні вільної від зовнішнього втручання влади, якою наділений керівний орган чи вища посадова особа

держави, була запропонована у XVI столітті французьким політичним філософом Жаном Боденом і стосувалася виняткових повноважень правителя ухвалювати остаточні рішення [8]. Традиційно суверенітет розглядався в контексті функціонування держави як інституційної форми організації політичної влади і проявлявся у кількох вимірах – політичному, територіальному, військовому, економічному, культурному, гуманітарному.

У свою чергу, інформаційний суверенітет є відносно новим явищем і стосується законної влади держави регулювати створення, збирання, одержання, зберігання, використання, поширення, охорону і захист інформації в межах своєї юрисдикції, а також захищати свої інформаційні активи від зовнішнього зловмисного втручання. Це поняття є синтезом класичної концепції вестфальського суверенітету та потреби в контролі над інформаційним простором [6].

Важливо розрізняти інформаційний суверенітет і споріднені, але вужчі поняття, такі як цифровий суверенітет, суверенітет даних або кіберсуверенітет. Суверенітет даних передусім стосується юрисдикційного контролю над особистими та організаційними даними, тоді як кіберсуверенітет акцентує увагу на управлінні мережею Інтернет. Натомість інформаційний суверенітет охоплює ширшу політичну, правову та стратегічну спроможність держави формувати та захищати власне інформаційне середовище, а також гарантувати інформаційні права своїм громадянам.

Д. Пол і Т. Тіль визначають інформаційний суверенітет як «здатність держави здійснювати юридичний і технічний контроль над інформаційною інфраструктурою, платформами та потоками контенту, що впливають на її національні інтереси» [8]. Л. ДеНардіс розглядає це поняття як прояв державної влади в кіберпросторі з метою забезпечення інформаційного самовизначення та захисту від іноземних маніпуляцій [3, с. 11]. Обидва підходи підкреслюють подвійний вимір суверенітету – нормативний і інструментальний – який лежить в основі ролі держави як охоронця інформаційного спільного блага.

Хоча ідея державного суверенітету має тривалу історію, її застосування до інформаційної та цифрової сфер є відносно новим явищем. Інформаційний суверенітет набув актуальності протягом останніх двох десятиліть у зв'язку з тим, що технології, засновані на великих масивах даних, глобальні інформаційні платформи та кіберконфлікти порушили традиційні уявлення про територіальний контроль держав. Як зазначає Д. Най, зростання кількості і складності кіберзагроз проявило вразливість навіть наймогутніших держав до нетериторіальних форм впливу [7].

Л. ДеНардіс також показує, що рішення на рівні інфраструктури – протоколи, стандарти, марш-

рутизація – стають полем політичної боротьби. У цьому контексті суверенітет перетворюється на функцію контролю над цифровими інфраструктурами, спроможність встановлювати юрисдикцію над даними та участь у формуванні універсальних норм на транснаціональному рівні. Зростаючи залежність держав від інформаційних систем для управління й оборони піднімає інформаційний суверенітет до рівня стратегічного пріоритету [3, с. 7–8].

Інформаційна держава характеризується залежністю від цифрових інфраструктур у сферах управління, нагляду та надання послуг [2]. У цій моделі інформаційний суверенітет стає обов'язковою умовою забезпечення безпеки, автономії та легітимності державної влади.

З точки зору безпеки, інформаційний суверенітет забезпечує межі для протидії кібератакам, кампаніям з дезінформації та несанкціонованому нагляду з боку ворожих іноземних акторів. Він дає змогу державам контролювати стратегічні інформаційні системи, захищати національні бази даних і впроваджувати стандарти кібербезпеки на всіх рівнях.

З точки зору легітимності, державний суверенітет над інформаційним простором є ключовою передумовою для утвердження пріоритету національних правових систем у регулюванні практик використання, збору, обробки, передачі і зберігання даних. В умовах, коли транснаціональні корпорації часто діють поза межами ефективного державного контролю, здатність держави здійснювати юрисдикцію над інформаційною діяльністю дозволяє посилити підзвітність державних інститутів і покращити якість демократичного врядування.

Наявність суверенітету в інформаційній сфері є критично важливою для забезпечення незалежності держави у внутрішній і зовнішній політиці. Адже у ситуації, коли критична інфраструктура, комунікаційні мережі та навіть публічний медійний дискурс залежать від зовнішніх державних або приватних акторів, держави ризикують втратити спроможність реалізовувати суверенні права та ухвалювати суверенні рішення. Таким чином, інформаційний суверенітет є не лише інструментом контролю над інформацією, але й засобом забезпечення стійкості демократичних інституцій і реалізації принципу народовладдя.

Можна виділити кілька ключових ознак інформаційного суверенітету, які одночасно слугують вимірами, в межах яких держави здійснюють ефективний контроль над власним інформаційним простором.

Перша ознака – територіальність. Вона обмежує інформаційний суверенітет визначеним географічним простором, в якому держави претендують на право виключного застосування власного законо-

давства для регулювання процесів поводження з даними і цифровою інфраструктурою.

Друга – сфера юрисдикції. В окремих випадках інформаційний суверенітет може поширюватися на цифрові сервіси та онлайн-платформи, які функціонують за межами фізичних кордонів держави, але чия діяльність впливає на національні інформаційні екосистеми.

Третя – наявність контролю над інфраструктурою. Ця ознака стосується здатності держави володіти, управляти або регулювати ключову цифрову інфраструктуру, таку як центри обробки даних, сервери доменних імен (DNS) та національні точки обміну інтернет-трафіком. Без такого контролю держави залишаються вразливими до зовнішнього впливу на критичні інформаційні потоки.

Четверта – нормативна автономія. Вона дає змогу державам розробляти й впроваджувати власні правові та етичні стандарти управління інформацією. Це особливо важливо в плюралістичному глобальному середовищі, де цінності щодо конфіденційності, свободи вираження поглядів та захисту даних можуть суттєво відрізнятися залежно від регіону і країни.

П'ята – локалізація даних. Це регуляторний механізм, за допомогою якого держави закріплюють нормативну вимогу щодо того, щоб певні категорії даних зберігались і оброблялись винятково на їхній території. Це сприяє ефективному нагляду за інформацією, підвищує рівень безпеки та гарантує судовий доступ до даних у межах юрисдикції держави.

Інформаційний суверенітет проявляється в кількох формах, як-от: юридичній, технічній та нормативній. Юридичний суверенітет означає можливість ухвалення та застосування дієвого законодавства, що регулює збір, зберігання, використання та поширення інформації. Такі правові інструменти, як Загальний регламент ЄС про захист даних (General Data Protection Regulation, GDPR) або закон про «суверенний інтернет» у Росії, ілюструють, як правові норми можуть по-різному перетворюватися на інструменти контролю за інформаційним простором.

Технічний суверенітет передбачає розвиток і впровадження національних цифрових рішень, включно з технологіями шифрування, протоколами передачі і обробки інформації, національними системами кібербезпеки та цифровою інфраструктурою. Ця форма суверенітету є особливо важливою для подолання зовнішньої залежності та забезпечення стійкості держави до кіберзагроз та інформаційних атак.

Нормативний суверенітет полягає у просуванні національного бачення регулювання інформаційної сфери, участь у глобальних дебатах щодо управління інтернетом, укладанні міжнародних угод і відстоюванні нормативних, зокрема етичних, підходів, що відповідають внутрішнім інтер-

есам. Держави, які мають вплив на формування глобальних правил цифрового порядку, фактично беруть участь у формуванні і реалізації глобального дискурсивного суверенітету.

Інформаційний суверенітет діє на кількох рівнях. В першу чергу, на національному рівні держави розробляють і реалізують державні політики у сфері регулювання практик поводження з інформацією, затверджують внутрішні регуляторні режими, створюють державні органи, відповідальні за захист даних, та формують національні стратегії інформаційної та кібербезпеки.

На наднаціональному рівні регіональні організації, такі як, наприклад, Європейський Союз, просувають інформаційний суверенітет шляхом створення колективних стандартів, гармонізації законодавства та затвердження спільних механізмів забезпечення його дотримання. Яскравими прикладами таких стандартів в ЄС є Акт про цифрові ринки (Digital Markets Act, DMA) та Акт про управління даними (Data Governance Act, DGA).

На глобальному рівні держави взаємодіють із багатосторонніми інституціями, такими як Міжнародний союз електрозв'язку (ITU) та Форум з управління інтернетом (IGF), щоб формувати міжнародні норми та впливати на архітектуру транснаціонального цифрового врядування.

Внутрішній вимір інформаційного суверенітету безпосередньо залежить від здатності держави подолати цифровий розрив і забезпечити інклюзивний доступ до інформаційної інфраструктури всім громадянам. Національна стійкість в інформаційну добу вимагає сталих інвестицій у цифрову інфраструктуру, кібербезпеку, управління відкритими даними та підвищення рівня інформаційної грамотності населення.

Й. Курбалія у своїй роботі наголошує на важливості координації зусиль між державою і приватним сектором у питаннях розбудови спроможностей інформаційної держави [6, с. 165]. У свою чергу, Ш. Зубофф наголошує, що розширення можливостей громадян задовольняти свої інтереси та реалізовувати права в інформаційній державі є ключовим фактором підтримки її демократичної легітимності [13]. Без справедливого доступу до інфраструктури і технологій та критичної обізнаності громадян у використанні сучасних інформаційно-комунікаційних технологій інформаційний суверенітет перетворюється на проєкт еліт, відірваний від широкого загалу, якому він за задумом покликаний слугувати.

В середині 90-х років XX століття була поширеною думка, що Інтернет є якимось унікальним простором, який може запропонувати альтернативу політиці сучасного світу. У своїй відомій Декларації незалежності кіберпростору Д. Барлоу зазначив, що Інтернет за своєю суттю є позанаціональним і антисуверенним, до якого суверенітет держав не

може застосовуватися [1]. Це твердження базувалося на переконанні в тому, що Інтернет є простором вільним від усіх видів влад, сферою абсолютної свободи [6, с. 7]. Проте зрозуміло, що така кіберанархічна теорія є утопічною за своєю суттю.

Водночас важливо усвідомлювати, що інформаційний суверенітет не є універсально визначеним правовим інститутом, а лише дискурсивним і перформативним твердженням, конкретний зміст і обсяг якого варіюється залежно від політичних систем і технологічних можливостей конкретних держав та/або їх об'єднань, що беруть участь у дискусії навколо встановлення глобальних правил використання мережі. Відтак інформаційний суверенітет є відносним: він виникає як певний результат переговорів між національними урядами, найбільшими корпораціями-власниками онлайн-платформ і мережевої інфраструктури, представниками громадянського суспільства та технічними спільнотами щодо регуляторних правил збору, обміну, зберігання та використання інформації, а також технічних протоколів передачі даних і захисту мереж від зовнішніх втручань. І це перетворює інформаційний суверенітет на дискурсивний процес постійного утвердження меж його конституювання і легітимізації, який підпадає як під внутрішньополітичні обмеження, так і під зовнішній тиск з боку глобальних стейкхолдерів, зокі цифрового суверенітету відображають глибинні нормативні суперечності – між відкритістю і контролем, демократією і централізацією, інноваціями та безпекою [8]. Відтак дискурсивний інформаційний суверенітет суттєво відрізняється від держави до держави, відображаючи різні можливості регулювати онлайн-платформи, розвивати власну цифрову інфраструктуру та впливати на глобальне управління Інтернетом. Залежить він також і від часу, оскільки постійний розвиток інформаційно-комунікаційних технологій вимагає регулярного оновлення правил і норм міждержавної взаємодії під час використання інформації.

Забезпечення інформаційного суверенітету стало стратегічним пріоритетом для більшості національних урядів, адже він безпосередньо впливає на економічну конкурентоспроможність, політичну стабільність, культурну ідентичність і обороноздатність держави. Як зазначила С. Браман, інформаційна політика перестала бути маргіальною і перетворилася на основу державного управління, впливаючи на все – від організації інститутів влади до контролю над продукуванням знань [2].

Л. Флоріді та Ш. Зубофф наголошують, що розвиток цифрових екосистем формує людську поведінку, підсилює суспільну довіру до інституцій та активізує громадянську участь. Нездатність забезпечити власний інформаційний суверенітет наражає держави на ризики дезінформаційних кампаній, кібератак та асиметричного впливу

з боку транснаціональних акторів. Результатом такого шкідливого зовнішнього впливу стає деградація інфраструктури (військової, фінансової, транспортної, телекомунікаційної тощо), а разом з нею стагнує і довіра громадян до влади через відчуття незахищеності. Таким чином, інформаційний суверенітет – це не лише питання самовизначення, але й питання виживання в геополітично суперечливому інформаційному просторі, а також питання легітимності державної влади і тривалості перебування політичних партій і окремих політиків у виборних органах законодавчої і виконавчої влади [4; 13].

Попри свою стратегічну важливість, реалізація інформаційного суверенітету стикається з низкою серйозних викликів.

Домінування глобальних технологічних платформ, головні офіси яких переважно розташовані у США, суттєво обмежує здатність інших держав застосовувати норми власного законодавства по відношенню до таких компаній чи притягувати їх до відповідальності за недотримання національних стандартів. Ці компанії контролюють критично важливі сегменти інформаційної інфраструктури – від пошукових систем і соціальних мереж до хмарних сервісів і електронної пошти – фактично діючи як приватні суверени по відношенню до інших суб'єктів інформаційних відносин [13]. Не варто забувати, що й технічна інфраструктура (кабелі, супутники, дата-центри тощо) перебувають у приватній власності провідних телекомунікаційних компаній, що створює чимало можливостей для зловживань з їхнього боку.

Кіберзалежність, попри свої економічні й технічні переваги, створює взаємні вразливості. Кібератака на один сегмент взаємопов'язаної системи може спричинити ланцюгову транскордонну реакцію, що значно знижує ефективність односторонніх нескордированих автономних заходів для запобігання негативним наслідкам [5].

Транскордонні обміни даними ще більше ускладнюють питання територіальної юрисдикції. Хмарні сервіси, які зберігають дані в різних країнах, піддаються традиційне уявлення про територіальний контроль. Навіть коли існують юридичні приписи, їх практичне виконання в межах різних юрисдикцій залишається проблематичним.

Нарешті, гібридні загрози, такі як: дезінформація, іноземні операції впливу та скоординована неавтентична активність, – підривають довіру громадськості та розбалансовують демократичні процеси. Ці форми інформаційної агресії експлуатують інформаційні вразливості у спосіб, який складно ідентифікувати та нейтралізувати на національному рівні за допомогою доступних уряду інструментів.

Боротьба за інформаційний суверенітет ілюструється через різні національні підходи. У Євро-

пейському Союзі Загальний регламент про захист даних (GDPR) став глобальним еталоном захисту персональних даних. Завдяки екстериторіальній дії він зобов'язує іноземні компанії дотримуватись європейських стандартів конфіденційності. Регламент утверджує бачення суверенітету даних, засноване на фундаментальних правах і верховенстві права.

Підхід ЄС до інформаційного суверенітету зосереджується на захисті даних, цифровій автономії та розвитку конкурентоспроможної цифрової економіки. Ключові нормативні акти – GDPR, Акт про дані (Data Act), а також ініціативи на кшталт Європейської стратегії щодо даних – спрямовані на забезпечення конфіденційності даних громадян ЄС, просування європейських інновацій та зменшення залежності від іноземних технологічних постачальників.

По суті, підхід ЄС до забезпечення інформаційного суверенітету є багатовимірним: він поєднує захист даних, цифрову автономію та економічну конкурентоспроможність задля створення цифрового середовища, вигідного для громадян і бізнесу.

Росія запровадила більш сек'юритизовану модель. Закон про суверенний інтернет надає владі повноваження ізолювати російський сегмент інтернету у разі загроз, а також вимагає маршрутизації трафіку через державні точки контролю. Хоча це посилює контроль, одночасно викликає занепокоєння щодо цензури та цифрової ізоляції.

Закон про «суверенний інтернет» передбачає встановлення спеціального обладнання і програмового забезпечення, щоб стежити за тисячами ключових вузлів російського інтернету. Це обладнання має направляти дані в центральний моніторинговий центр, що матиме повноваження і можливості блокувати інформацію, яку влада вважає загрозою для держави, а також ізолювати так званий «рунет» від решти всесвітньої інтернет-павутини у разі іноземної кібератаки.

Китай розвинув одну з наймасштабніших архітектур інформаційного суверенітету. Китайські закони про кібербезпеку та безпеку даних встановлюють суворі вимоги щодо локалізації, інспекції та цензури. Ці закони слугують як стратегічним, так і ідеологічним цілям, зміцнюючи контроль Комуністичної партії Китаю над інформаційним простором.

Інформаційна держава – це нова форма політичної організації, в якій державне управління зосереджене навколо стратегічного контролю над інформацією та інформаційною інфраструктурою. У цій моделі організації державної влади збереження інформаційного суверенітету є не допоміжним завданням, центральною функцією держави. Як стверджує Л. Келло, держава тепер має захищати не лише фізичні кордони, а й віртуальні домени, де загрози виникають з коду, операцій зовнішнього впливу та інфраструктурної

залежності [5]. Л. ДеНардіс показує, що контроль над інформаційною інфраструктурою є формою геополітичної влади [3], тоді як С. Браман стверджує, що інформаційне управління трансформує саму природу суверенітету [2]. Інформаційна держава забезпечує виконання законів, охороняє кордони, навчає громадян і проектує силу – усе це за допомогою цифрових інструментів. Її легітимність і функціональність залежать від того, наскільки ефективно вона здатна захистити свою інформаційну екосистему.

Як слушно зауважують Д. Пол та Т. Тіль: «Сьогодні цифровий суверенітет став набагато ширшим поняттям, яке охоплює не лише питання інтернет-комунікації та підключення, а й набагато ширшу цифрову трансформацію суспільств. Цифровий суверенітет – особливо в Європі – зараз часто використовується як скорочення для впорядкованої, ціннісно керованої, регульованої, а отже, розумної та безпечної цифрової сфери. Вважається, що він вирішує багатогранні проблеми індивідуальних прав і свобод, колективної та інфраструктурної безпеки, політичної та правової забезпеченості та чесної економічної конкуренції» [8].

Висновки. По мірі еволюції інформаційної держави необхідність захисту інформаційного суверенітету постає не як факультативна опція, а як необхідність. Інформаційний суверенітет дає змогу державам зберігати демократичну цілісність, захищати критичну інфраструктуру та відстоювати політичну автономію перед обличчям транснаціональних цифрових компаній-гігантів, зберігати легітимність серед громадян. Водночас прагнення до інформаційного суверенітету повинне поєднуватися із зобов'язаннями щодо захисту прав громадян, відкритості, доступу до інновацій та міжнародної співпраці. Знайти цей баланс – одне з головних завдань XXI століття для науковців, політиків і мережевих технологів.

Розвиток інформаційної спроможності держави є ключем до розуміння трансформації суверенітету в цифрову епоху. Д. Най показує, що сьогодиншній інформаційний суверенітет уже не є абсолютним – він є умовним, сформованим співпрацею з приватними акторами, вразливістю до кіберзагроз і глобальною конкуренцією за право брати участь в ухваленні цифрових норм. Інформаційний суверенітет повинен розглядатися як динамічний елемент міжнародного порядку.

Хоча концепція інформаційного суверенітету є відносно новою, вона стрімко стала визначальною рисою сучасного державного управління. У міру того як держави стикаються з викликами домінування платформ, кібервоєн, транскордонних потоків даних і наглядового капіталізму, здатність контролювати цифрову сферу стала необхідною умовою автономії, легітимності та безпеки.

У цій статті доведено, що інформаційний суверенітет – це не статичний юридичний інститут, а безперервний, дискурсивний процес. Він відображає як дискурсивні претензії, так і матеріальні спроможності, а його форма і функції варіюються залежно від національного контексту. Забезпечення цього типу суверенітету є життєво важливим не лише для захисту критичної інфраструктури, а й для збереження демократичних норм, економічного розвитку та культурної цілісності.

В епоху формування інформаційної держави суверенітет над інформацією вже не є питанням вибору – це питання виживання. Держава, яка не зуміє забезпечити свою інформаційну автономію, зіткнеться з дедалі більшою ерозією політичного суверенітету під тиском зовнішніх акторів і внутрішньої фрагментації. Оскільки цифрові технології продовжують змінювати основи політичного життя, саме інформаційний суверенітет залишатиметься головною віссю майбутніх дискусій про владу, право і легітимність.

ЛІТЕРАТУРА:

1. Barlow, J.P. (1996) *A Declaration of the Independence of Cyberspace*. URL: <https://www.eff.org/cyberspace-independence>
2. Braman, S. (2006). *Change of State: Information, Policy, and Power*. Cambridge, MA: MIT Press. 545 p.
3. DeNardis, L. (2014). *The Global War for Internet Governance*. New Haven, CT: Yale University Press. 296 p.
4. Floridi, L. (2014). *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford: Oxford University Press. 148 p.
5. Kello, L. (2017). *The Virtual Weapon and International Order*. New Haven, CT: Yale University Press. 320 p.
6. Kurbalija, J. (2016). *An Introduction to Internet Governance* (7th ed.). Geneva: DiploFoundation. 192 p.
7. Nye, J. S. (2010). *Cyber Power*. Belfer Center for Science and International Affairs, Harvard Kennedy School. <https://www.belfercenter.org/publication/cyber-power>
8. Pohle, J., & Thiel, T. (2020). Digital Sovereignty. *Internet Policy Review*, 9(4). <https://doi.org/10.14763/2020.4.1532>
9. *Programme for Germany's Presidency of the Council of the European Union 'Together for Europe's recovery'. 1 July to 31 December 2020*. URL: <https://www.eu2020.de/resource/blob/2360248/e0312c50f910931819ab67f630d15b2f/06-30-pdf-programm-en-data.pdf>
10. World Summit on Information Society. Geneva Declaration of Principles and Plan of Action. 10–12 December 2003. URL: http://wsis2003.geneva.org/pdf/WSIS_GDP_PA.pdf
11. World Summit on Information Society. Tunis Commitment. URL: <https://www.itu.int/net/wsis/docs2/tunis/off/7.html>

12. World Summit on Information Society. Tunis Agenda for the Information Society. URL: <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html>

13. Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs. 704 p.

Changing the paradigm of perception of information sovereignty in the context of transit to an informational state

Balan Sergii Victorovich

Candidate of Political Sciences,
Senior Research Fellow
V. M. Koretsky Institute of State
and Law of National Academy of Sciences
of Ukraine
Triochsvyatitska str., 4, Kyiv, Ukraine
ORCID: 0000-0002-9421-7037

The relevance of this article is determined by the growing role of information sovereignty as a leading property of the modern information state, which legitimizes state power and enables the realization of sovereign rights. This article explores the political and legal foundations of information sovereignty as a core principle in the architecture of the modern informational state. It analyzes conceptual definitions, historical evolution, and the institutional mechanisms through which states assert control over digital information flows. The article further delineates the features, types, and levels of information sovereignty, highlighting the challenges posed by digital globalization, cyber threats, and cross-border information dependency. Drawing on interdisciplinary literature, the article argues that information sovereignty is not a fixed legal status but a discursive and strategic process that varies according to national capabilities and policy priorities. The discussion highlights the structural challenges posed by digital globalization and emphasizes how information sovereignty underpins the economic, political, humanitarian, and military dimensions of statehood. Ultimately, the article concludes that the informational state is defined by its ability to maintain and defend its information sovereignty, making it a central organizing principle of contemporary governance.

The article also presents a comparative analysis of approaches to ensuring information sovereignty across different countries. It highlights the distinctions between normative, technical, and legal forms of sovereignty. The author argues that effective implementation of information sovereignty requires a balance between control and openness, sovereignty and cooperation, security and human rights. Particular attention is given to the role of the state in developing its own digital infrastructure as a key precondition for maintaining political autonomy amid global competition for control over information flows.

Key words: information sovereignty, informational state, information space, disinformation, sovereign rights.