1.2. Співвідношення між державним суверенітетом і цифровим

Традиційна теорія суверенітету, запропонована французьким політиком і філософом Жаном Боденом у шістнадцятому столітті, стосувалась повноважень правителя приймати остаточні рішення. У свою чергу, Жан-Жак Руссо переробив цю концепцію так, щоб вона зосередилася на народному суверенітеті, а не на монархічному; з часом це поняття все більше асоціювалося з демократією, верховенством права та територіальністю.

Сьогодні суверенітет передусім означає незалежність держави по відношенню до інших держав (зовнішній суверенітет), а також верховенство і повноту державної влади відносно до усіх інших організацій у політичній системі суспільства, її монопольне право на законодавство, управління і юрисдикцію усередині країни в межах усієї державної території (внутрішній суверенітет). Розуміючи як демократичний суверенітет, він охоплює народний суверенітет і право громадян здійснювати самовизначення, використовуючи свої невід'ємні права. Вирішальним для всіх цих значень є географічна специфікація, тобто обмеження суверенітету певною територією, що розглядається як функціональна передумова для ефективного здійснення влади[13].

З часів Руссо суверенітет розглядався як центральне поняття для розуміння державної політики. Але в 1990-х роках ця важливість, ослабла, що призвело до розмов про постсуверенний світ, у якому держави залежні від міжнародних організацій та більше не будуть найважливішим і в кінцевому підсумку вищим джерелом влади, де демократія буде тісніше пов'язана з плюралізмом управління і участю, ніж з здатність демосу керувати собою[14].

В умовах трансформації уявлень про державний суверенітет науковці вимушені шукати нові підходи до його розуміння. На думку І. В. Яковюка, оригінальним є підхід до державного суверенітету датських політологів Х.-Х. Хольма і Г. Соренсена, які пропонують розглядати його у трьох аспектах:

[13] Grimm D. Sovereignty: The Origin and Future of a Political and Legal Concept. Columbia University Press. 2015. 192 p.
[14] MacCormick N. Questioning Sovereignty: Law, State, and Nation in the European Commonwealth. Oxford University Press. 1999. DOI: 10.1093/acprof:oso/9780198268765.001.0001.

негативний (юридичний аспект, який передбачає формальне визнання держави з боку інших держав у рамках міжнародного права і можливість певною мірою дійсно панувати на своїй території), позитивний (здатність держави повністю розпоряджатися собою і забезпечувати своїм громадянам необхідний для існування достаток) та операційний (передбачає обмеження суверенітету за допомогою укладання міжнародних договорів в обмін на участь у прийнятті рішень іншими державами)[15].

Згодом зниження значення держави сильно вплинуло на ранні етапи розвитку та управління Інтернетом. Ідея всеохоплюючого державного суверенітету була особливо заперечена двома різними, але пов'язаними, дискусійними напрямками, які значною мірою сформували суспільний та академічний дискурси: *кібервиключність* та *багатостороннє управління Інтернетом.* Проте останнім часом учасники політики успішно намагалися виправдати та підтвердити суверенітет у цифровій сфері проти цих двох точок зору.

Дж. Поле і Т. Тіль приділили значну увагу детальному вивченню цих двох проблем. На їх думку, перший виклик, кібервинятковість, говорить про те, що цифрова сфера якісно відрізняється від аналогового світу, і тому до цифрового простору потрібно ставитися інакше, ніж до всіх попередніх технологічних інновацій[16]. Ця точка зору була особливо популярна під час підйому комерційного Інтернету в 1990-х роках, але все ще очевидна в публічному та академічному дискурсі. Кібервиключне мислення базується на припущенні, що зростаюча важливість комп'ютерного мережевого зв'язку передбачає загибель державного суверенітету шляхом розмивання кордонів[17]. Хоча фактичний розвиток Інтернету не відбувався за межами конкретних правових просторів і не був би можливим без стимулів, наданих ринками, регуляторними режимами чи державними дослідницькими інфраструктурами[18], кібервиключність, яка

---

[15] Яковюк І.В. Державний суверенітет національних держав у складі Європейського Союзу: проблеми визначення. *Вісник Академії правових наук України*. 2004. №3 (38). С. 114-126.
[16] Pohle J. & Thiel T. Digital sovereignty. Internet Policy Review. 2020. 9 (4). https://doi.org/10.14763/2020.4.1532.
[17] Katz J. Birth of a Digital Nation. 1997. URL: https://www.wired.com/1997/04/netizen-3/м.
[18] Mazzucato M. The entrepreneurial state. Demos. 2011. URL: http://oro.open.ac.uk/30159/1/Entrepreneurial_State_-_web.pdf

найчастіше приймає форму ідеології з сильною культурною та економічною підтримкою в Силіконовій долині[19].

Як суб'єкти, які не довіряють усталеним політичним інституціям, прибічники кібервиключності стверджують, що цифрові форми політики сприятимуть децентралізованій організації суспільства, що повинно дозволити краще відповідати на складні вимоги управління сучасним суспільством, ніж традиційні форми політичної організації. З цієї точки зору, очікується, що зовнішній суверенітет, право та територіальність мають менше значення в контексті транснаціональних мереж. Аргументів для цього багато. По-перше, складність вкладених обов'язків і глобальне охоплення мереж не можуть бути належним чином розглянуті в рамках національних юрисдикцій; по-друге, законодавчі процедури надто повільні, щоб не відставати від темпів інновацій цифрових технологій і пов'язаних з ними бізнес-моделей; і по-третє, саме існування цифрового суверенітету з кіберпростором як новою автономною віртуальною сферою, яка не залежить від державного втручання[20].

Крім того, на думку Брижка В. М. та Фурашева В. М., у розрізі забезпечення цифрового суверенітету держави необхідно враховувати й права особи на приватність комунікацій – усе, що пов'язано з техніко-технологічними засобами і способами забезпечення телефонних розмов, електронних повідомлень, особистого поштового листування та інших видів інформаційно-комунікаційних зв'язків. При цьому, в умовах програмно-технологічного розвитку Інтернету приватність комунікацій все більше пов'язується з інформаційною приватністю, тобто з тим, що передбачає захист персональних даних людини, а також інформаційної безпеки людини, суспільства і держави. Ця тенденція безпосередньо стосується нових поглядів у застуванні Інтернету, які отримали назву «Інтернет речей» та «Хмарні технології». Технології типу «Інтернет речей» характеризують те, що кількість матеріальних об'єктів, підключених у світі до Інтернету, стала збільшуватися по відношенню до

[19] Turner F. From counterculture to cyberculture: Stewart Brand, the Whole Earth Network, and the rise of digital utopianism. 2006. University of Chicago Press. URL: https://press.uchicago.edu/ucp/books/book/chicago/F/bo3773600.html .

[20] Barlow J. P. A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation. 1996. URL: https://www.eff.org/cyberspace-independence.

кількості людей, які взагалі користуються глобальними комунікаційними мережами. А «Хмарні технології» визначають перехід від використання програмно-апаратних засобів, що належать окремим суб'єктам господарювання, на модель створення та використання «відкритого об'єднання хмарних обчислень», тобто «хмарних технологій» чи «хмарних сервісів»[21].

Звертаючи увагу на *багатостороннє управління Інтернетом* як на другий напрямок заперечення реалізації державою цифрового суверенітету, необхідно розглянути Декларацію принципів управління Інтернетом, яка прийнята в жовтні 2003 року в Женеві у ході першого етапу Всесвітнього саміту з питань інформаційного суспільства (ВСІС). В прийнятій Женевській Декларації принципів зазначено, що Інтернет розвинувся в загальнодоступний глобальний засіб і що управління його використанням повинне стати одним з основних питань порядку денного інформаційного суспільства.

Представники різних країн світу, які зібралися в Женеві відзначили, що міжнародне управління Інтернетом повинне бути прозорим і демократичним, та здійснюватися на багатосторонній основі, тобто при повній участі всіх заінтересованих сторін, а саме: а) державних органів; б) приватного сектору; в) громадянського суспільства; г) міжнародних організацій.

Управління Інтернетом, як одної з основних складових цифрових інфраструктур, повинне забезпечувати справедливий розподіл ресурсів; полегшувати доступ для всіх; гарантувати стабільне і захищене функціонування Інтернету; враховувати багатомовність. Управління всесвітньою мережею охоплює як технічні питання, так і питання державної політики, і в ньому повинні брати участь усі заінтересовані сторони і відповідні міжурядові і міжнародні організації.

Проте, у Женевській Декларації принципів визнано, що суверенним правом держав є політичні повноваження, які стосуються питань державної політики, що мають відношення до Інтернету. А також держави мають права й

[21] Брижко В.М., Фурашев В.М. Інформаційне право та інформаційне законодавство: наукове видання. – (НДІІП НАПрН України). Київ: ТОВ "Видавничий дім "АртЕк", 2019. 288 с.

обов’язки у відношенні до міжнародних питань державної політики, які стосуються Інтернету.

Відповідно до рішень Женевського етапу ВСІС Генеральний секретар ООН Кофі Аннан заснував робочу групу з управління Інтернетом (далі – РГУІ) у рамках відкритого для всіх процесу, що забезпечив механізм для участі державних органів, приватного сектору і громадянського суспільства як із тих країн, що розвиваються, так і з розвинутих країн. Мандатом РГУІ було визначено вивчення питання про управління Інтернетом і представлення до 2005 року пропозицій щодо відповідних дій.

В червні 2006 року РГУІ опублікувала звіт, в якому запропонував таке робоче визначення поняття «управління Інтернетом», яке зводиться до такого – розробка і застосування державними органами, приватним сектором і громадянським суспільством, у рамках їх відповідних ролей, спільних принципів, норм, правил, процедур прийняття рішень і програм, що формують розвиток і використання Інтернету.

До областей державної політики робочою групою було віднесено такі чотири питання: 1) що стосуються *інфраструктури і управління найважливішими Інтернет-ресурсами*, включаючи: а) адміністративне управління системою імен доменів і адресами Інтернет-протоколу (IP-адресами); б) управління системою кореневих серверів; в) технічні стандарти; г) однорангова взаємодія та з’єднання комп’ютерів; ґ) інфраструктура телекомунікацій, включаючи інноваційні і конвергентні технології; д) переведення мереж у багатомовний режим; 2) що стосуються *застосування Інтернету*, включаючи: спам; мережеву стабільність і безпеку; кіберзлочинність; 3) пов’язані з Інтернетом, але мають наслідки, що виходять за рамки Інтернету, наприклад питання: а) прав інтелектуальної власності; б) свободи слова і незаконного контенту; в) захисту особової інформації і права на приватне життя; г) прав споживачів; ґ) міжнародної торгівлі; 4) питання, що стосуються різних аспектів розвитку управління Інтернетом, зокрема підвищення цифрової компетентності в країнах, що розвиваються.

Крім того, робоча група визначила роль і *обов'язки державних органів*, які зводяться до таких:

– розробка, координація і здійснення державної політики на національному рівні;

– розробка і координація політики на регіональному і міжнародному рівнях;

– створення сприятливих умов для розвитку інформаційних і комунікаційних технологій;

– наглядові та контрольні функції;

– розробка і прийняття законів, положень і стандартів;

– розробка типових договорів;

– створення прикладів найкращої практики;

– сприяння підвищенню компетентності – як у сфері ІКТ, так і за допомогою ІКТ;

– сприяння науковим дослідженням і дослідно-конструкторським розробкам в області технологій і стандартів;

– сприяння доступу до послуг у сфері ІКТ;

– боротьба з кіберзлочинністю;

– розвиток міжнародного і регіонального співробітництва;

– заохочення розвитку інфраструктури і прикладень ІКТ;

– вирішення загальних питань розвитку;

– сприяння багатомовності і культурному різноманіттю;

– врегулювання спорів та арбітраж.

У свою чергу, РГУІ запропонувала створити глобальний багатосторонній форум для вирішення питань державної політики у відношенні Інтернету, а також чотири варіанти організаційних моделей управління Інтернетом, які б доповнювали роботу форуму[22]:

Модель 1. Створення Глобальної ради з Інтернету (ГРІ), що складалася б із членів, призначуваних урядами з належним урахуванням представництва

[22] Пероганич Ю. Управління Інтернетом. URL: https://informationsociety.wordpress.com/2006/11/17/igf-history/

кожного регіону і при участі інших заінтересованих сторін. Ця рада виконувала б функції міжнародного управління Інтернетом, які у даний час виконує Міністерство торгівлі Сполучених Штатів Америки. Крім того, рада замінила б собою Урядовий консультативний комітет ІКАНН (УКК).

В цій моделі ГРІ має бути пов'язаною з ООН, а реформована й інтернаціоналізована ІКАНН має бути підзвітною раді.

Модель 2. Передбачає зміцнення ролі УКК ІКАНН для зняття стурбованості деяких урядів щодо конкретних питань. Ця модель виключає наявність будь-якої конкретної наглядової організації.

Модель 3. Оскільки уряд якої-небудь однієї країни не повинен грати пануючої ролі в міжнародному управлінні Інтернетом, вирішувати політичні питання, що зачіпають національні інтереси могла би Міжнародна рада з Інтернету (МРІ), особливо з урахуванням компетенції ІКАНН. Цей новий орган міг би замінити УКК ІКАНН.

Модель 4. Передбачає створення трьох структур:

– Глобальної ради з політики Інтернету (ГРПІ), в якій брали б участь представники урядів, і яка займалася б розробкою державної політики і приймала рішення з питань міжнародної державної політики у відношенні Інтернету. Участь приватного сектору і громадянського суспільства в раді передбачається в якості спостерігачів.

– Всесвітньої корпорації з присвоєння імен і номерів в Інтернеті (ВІКАНН), яка була б створена шляхом реформування й інтернаціоналізації ІКАНН.

– Глобальний форум з управління Інтернетом (ГФУІ).

Питання управління Інтернетом були виділені в окремий розділ прийнятої в Тунісі під час другого етапу ВСІС в листопаді 2005 року Туніської програми для інформаційного суспільства.

В цій програмі Інтернет названо центральним елементом інфраструктури інформаційного суспільства, а управління Інтернетом – основним питанням порядку денного інформаційного суспільства.

Проведення другого етапу ВСІС в Тунісі 16–18 листопада 2005 р., розпочалося з пропозиції Генеральному секретареві ООН скликати і провести в рамках відкритого для всіх процесу засідання нового органу для ведення політичного діалогу за участю багатьох заінтересованих сторін за назвою Форум з питань управління Інтернетом (ФУІ).

Такий форум було проведено в Афінах в 2006 році. Участь у форумі прийняла й українська делегація, яку очолив заступник Міністра транспорту та зв'язку України. До делегації також увійшли представники Секретаріату Кабінету Міністрів України, Державного департаменту з питань зв'язку та інформатизації (Держзв'язку), Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (ДСТЗІ СБУ), Національної комісії з питань регулювання зв'язку (НКРЗ) України, а також Інтернет асоціації України (ІнАУ).

Після створення Форуму ООН з управління Інтернетом (IGF), перші збори яких відбулися в Афінах у 2006 р., виникло безліч національних та регіональних ініціатив з управління Інтернетом (Ініціативи IG), спрямованих на сприяння обговоренню питань національного та регіонального значення через зв'язок з глобальними темами . Усі ініціативи IG діють незалежно, але віддані тим самим цінностям, що й глобальний IGF: бути відкритими, прозорими та інклюзивними для всіх зацікавлених сторін, працювати на некомерційній основі, гарантувати участь багатьох зацікавлених сторін у всіх заходах, здійснювати процес прийняття рішень за принципом «знизу вгору».

Всі вони утворюють всесвітню мережу національних і регіональних ініціатив (NRI), діяльність якої координується Секретаріатом IGF. Крім національних європейських ініціатив з управління інтернетом (IG), у цьому регіоні існують два регіональні форуми з управління інтернетом (IGF): EuroDIG та SEEDIG.

Управління Інтернетом прямо пов'язано з інформаційною безпекою країн. Тому з метою забезпечення міжнародної інформаційної безпеки 12 вересня 2011 року КНР і РФ спільно з Узбекистаном і Таджикистаном звернулися до Генерального секретаря ООН з листом, де пропонують на 66-й сесії Генеральної

асамблеї розглянути запропонований ними проєкт «Правил поведінки у сфері забезпечення міжнародної інформаційної безпеки» (A/66/359)[23].

Правила звертають увагу на такі моменти:

• пункт «c» звертає увагу на необхідність співпраці в «боротьбі зі злочинною чи терористичною діяльністю із використанням інформаційно-комунікаційних технологій <...> що підриває політичну, економічну й соціальну стабільність держав, їх культурний та духовний стан»;

• у пункті «g» йдеться про «сприяння створенню багатосторонніх, демократичних міжнародних механізмів управління Інтернетом, які б гарантували його стабільне й безпечне функціонування».

В ООН сторони розпочали супровід своєї пропозиції. Так, представник делегації КНР при ООН Лі Ксяомеі зазначила, що китайська сторона висловлює жаль з приводу того, що до останнього часу на міжнародному рівні не було прийнято регулюючих документів, які мали б сприяти встановленню міжнародної інформаційної безпеки.

Негативно з цього приводу висловились представники США й Австралії. Вальтер Рейд зазначив, що питання кіберсфери виходять за рамки обговорення в межах ООН і потребують масштабного врахування міжнародного гуманітарного законодавства як головної структури при обговоренні таких ініціатив. Фактично аналогічної позиції дотримувався й Пітер Вулкот, зазначивши, що обговорення кібертематики в ООН буде надзвичайно складним, а багатоаспектність проблеми робить неможливим її обговорення в межах комітету. У цьому контексті складно не згадати, що у вересні 2011 р. між США та Австралією було підписано додаткові угоди щодо спільної протидії кіберзагрозам і посилення двосторонньої співпраці з даного питання. Крім того, Австралія повністю підтримує існуючий багатосторонній підхід управління Інтернетом і принципово проти державного контролю за Інтернетом[24].

[23] China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations. 2011. URL: http://www.fmprc.gov.cn/eng/zxxx/t858978.htm

[24] Дубов Д. В. Майбутнє кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців : аналіт. доп. Київ. НІСД, 2012. 32 с.

Більш розгорнутими й категоричними були оцінки даної ініціативи з боку представників держструктур США, на думку яких подібні проєкти спрямовані на спроби домогтися від ООН схвалення на посилення контролю над Інтернет-простором у своїх країнах.

Крім США, запропонована китайсько-російська ініціатива викликала негативну реакцію з боку ОБСЄ: представник ОБСЄ з питань свободи ЗМІ заявила, що подібні ініціативи є неприпустимими, оскільки потенційно можуть бути використані для зведення бар'єрів на шляху потоку інформації чи обміну думками. Вона звернула увагу тих країн, які подали відповідне звернення, що у червні 2011 р. представники ООН, ОБСЄ, Організації американських держав і Африканської комісії з прав людини і народів прийняли Спільну декларацію про свободу вираження поглядів в Інтернеті й зазначила, що саме цей документ має бути базовим у цьому питанні[25].

Заслуговує на увагу колективний лист від неурядових організацій до Голови 66-ї Генасамблеї ООН, в якому запропонований Кодекс (правила) критикується за чотирма напрямами:

• у пункті «g» про багатостороннє управління мережею Інтернет не прописано участь громадянського суспільства, що може перетворити таке управління на суто міждержавне;

• у пункті «h» у формуванні культури інформаційної безпеки провідна роль належить державі й державно-приватному партнерству, у той час як з цього процесу виключені елементи громадянського суспільства;

• у пункті, що присвячений «загальній повазі до прав людини» присутнє істотне уточнення – «повага до багатоманіття історії, культури і соціальної структури всіх країн», що може бути використано для звуження універсальності прав людини, закріплених у документах Генасамблеї ООН;

• основну претензію викликав пункт «c», де разом з боротьбою зі злочинною чи терористичною діяльністю з використанням інформаційно-комунікаційних технологій пропонується включити протидію діяльності, що

[25] Там само.

«підриває політичну, економічну й соціальну стабільність держав, їх культурні та духовні традиції». У такій постановці питання дане положення перевищує допустимі обмеження на свободу вираження думки, що закладені в ст. 19 (3) Міжнародного пакту про громадянські та політичні права й може бути використане для обмеження (цензурування) свободи слова.

Такий саме критичний характер мало і обговорення Правил під час міжнародної конференції з питань діяльності в кіберпросторі, що відбулася у листопаді 2011 р. у Лондоні під девізом «Бачення. Надії. Страхи» (The Vision, the Hopes, the Fears) з ініціативи британського МЗС яка зібрала 700 делегатів із 60-ти країн, що представляли як урядові, так і комерційні структури[26].

Як зазначено у проєкті Стратегії кібербезпеки України (2021 – 2025 роки), підготовленої РНБО, Україна буде сприяти подальшому дотриманню міжнародного права та стандартів у галузі прав людини, заохочуватиме застосування найкращих практик, а також активізує свої зусилля щодо запобігання зловживанню новими технологіями. Для цього держава активізує свою участь і партнерство в міжнародних процесах стандартизації та сертифікації у сфері кібербезпеки, розширить представництво в міжнародних, регіональних та інших органах стандартизації, організаціях, що займаються розробленням стандартів та сертифікацією у цій сфері[27].

У питаннях розроблення стандартів у сферах нових технологій (зокрема щодо штучного інтелекту, хмарних технологій, квантових обчислень та квантових комунікацій) та базової архітектури Інтернету Україна виходить з того, що Інтернет має залишатися глобальним та відкритим, технології повинні орієнтуватися на людину, забезпечувати її базові свободи, гарантувати невтручання у її особисте життя, забезпечувати її конфіденційність у кіберпросторі, а будь-які обмеження в цій частині повинні здійснюватися лише відповідно до закону. Використання технологій має бути законним, безпечним та етичним. Водночас у зв'язку з ускладненням міжнародної безпеки в

[26] Офіційний сайт конференції: Nations discuss cyber security. 2011. URL: http://www.cyberwarnews.info/2011/11/01/nations-discuss-cyber-security/.

[27] Проєкт стратегії кібербезпеки України (2021 – 2025 роки). URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf

кіберпросторі Україна займатиме більш активну позицію в дискусіях ООН та інших міжнародних форумах для просування, координації та консолідації її позиції у сфері кібербезпеки, зменшуючи небезпеки мілітаризації кіберпростору[28].

Проте, повернемо увагу до реалізації цифрового суверенітету, акцент у якому робиться на ідеї, що держава або регіон повинні мати можливість самостійно приймати рішення щодо своєї цифрової інфраструктури та розгортання технологій. Більшість із цих претензій стосуються географічного обмеження суверенітету певною територією та зусиль держав щодо забезпечення безпеки своїх цифрових інфраструктур та повноважень державних органів щодо питань цифрового зв'язку, що стосуються їхніх територій та громадян.

Можна виділити два напрямки цієї лінії мислення. З одного боку, відбувається зростання мережевої комунікації як загрози існуючим політичним системам. Китай був першою країною, яка відреагувала на це, пропагуючи та розвиваючи ідею свого цифрового суверенітету, як кібер-суверенітет або інтернет-суверенітет[29]. Основні ідеї пізніше були адаптовані іншими авторитарними країнами, особливо Росією. З іншого боку, західні держави також звернулися до потреби контролю в цифрових питаннях, де обґрунтування створення архітектури контролю було переважно через безпеку.

Проте, з появою глобальних мереж держави дедалі більше відчували свою вразливість, що виражається у питаннях контролю та управління цифровими інфраструктурами. Комп'ютерна безпека була віднесена до національної безпеки і поширилася на все більше сфер[30]. У цьому процесі значно зросла роль держави і контролю над інфраструктурою. А «після одкровень Сноудена 2013 року акцент на державній автономії та безпеці став основним елементом дискурсів про цифровий суверенітет»[31].

---

[28] Проєкт стратегії кібербезпеки України (2021 – 2025 роки). URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf

[29] Pohle J. & Thiel T. (2020). Digital sovereignty. Internet Policy Review, 9 (4). https://doi.org/10.14763/2020.4.1532.

[30] Nissenbaum H. (2005). Where Computer Security Meets National Security. Ethics and Information Technology, 7(2), 61–73. https://doi.org/10.1007/s10676-005-4582-3.

[31] Hintz, A., & Dencik, L. (2016). The politics of surveillance policy: UK regulatory dynamics after Snowden. Internet Policy Review, 5(3). https://doi.org/10.14763/2016.3.424.

Яскравими прикладами підтримуваних державою практик та ідей, що випливають із цього дискурсивного напряму, є багато останніх пропозицій щодо локалізації даних. Вони прагнуть обмежити зберігання, переміщення та/або обробку даних певними областями та юрисдикціями і, як правило, виправдовуються необхідністю обмежити доступ іноземних розвідувальних і комерційних агенцій до певних типів даних, наприклад, промислових чи особистих. Багато таких пропозицій також викликані іншими мотивами, такими як розширення доступу до даних громадян з боку розвідників і правоохоронних органів і бажання отримувати прибутки для таких суб'єктів, як місцеві інтернет-сервіси. постачальників[32]. У багатьох країнах, включаючи Бразилію та Індію, пропозиції щодо локалізації даних наразі реалізовувалися лише у фрагментованій формі або залишалися обмеженими в конкретних контекстах[33]. Показовим випадком запропонованої ініціативи з локалізації даних в Європі є Ідея шенгенської маршрутизації (визначення маршруту прямування інформації між мережами. Маршрутизатор (або роутер від англ. router) приймає рішення, що базується на IP-адресі отримувача пакету), тобто пропозиція уникнути маршрутизації потоків даних всередині Європи через пункти обміну та маршрути за межами Європи. Ідея, яку запропонував Deutsche Telekom, найбільший інтернет-провайдер у Німеччині та найбільша телекомунікаційна організація в Європейському Союзі, була гаряче обговорювана як у суспільній, так і в політичній сфері, але в кінцевому підсумку не знайшла достатньої політичної підтримки[34].

Яскравим прикладом ініціативи, спрямованої на посилення економічної автономії, є європейський хмарний сервіс Gaia-X, який було анонсовано спільно Францією та Німеччиною і ще не запущено. Проєкт планує підключити малих і середніх постачальників хмарних послуг у Європі за допомогою спільного стандарту, який дозволить їм запропонувати відкриту, безпечну та надійну

[32] Hill, J. F. (2014). The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders. Lawfare Research Paper Series, 2(3), 1–41.
[33] Panday J., & Malcolm J. (2018). The Political Economy of Data Localization. Partecipazione e conflitto, 11(2), 511–527. https://doi.org/10.1285/i20356609v11i2p511.
[34] Kleinhans J.-P. Schengen-Routing, DE-CIX und die Bedenken der Balkanisierung des Internets. Netzpolitik. (2013, November 13). URL: https://netzpolitik.org/2013/schengen-routing-de-cix-und-die-bedenken-der-balkanisierung-des-internets/.

європейську альтернативу найбільшим у світі постачальникам хмарних послуг (наприклад, Amazon, Google, Microsoft), водночас поважаючи європейські цінності та стандарти захисту даних. Ініціатива активно просувається політичними діячами як важливий крок до європейського суверенітету даних[35], що є ще одним тісно пов'язаним поняттям.

Мета досягти більшої незалежності від іноземних технологій та сприяти інноваційній потужності вітчизняної промисловості є центральним елементом дискурсів про цифровий суверенітет. В США та ЄС деякі заходи додатково виправдовуються метою захисту споживачів, пропонуючи технологічні послуги, які поважають права користувачів, а також національні закони та норми, такі як правила захисту даних[36]. У багатьох країнах, що розвиваються, таких як Індія, запропоновані заходи також часто спрямовані зменшення домінуючого становища західних технологічних корпорацій на глобальному Півдні, що призводить до нових форм експлуатації[37][38]. Не дивно, що подібні заяви та ініціативи були зустрінуті скептицизмом і запереченням у деяких західних країнах, де політика та бізнес-суб'єкти поспішили назвати такі ідеї «зведенням бар'єрів або перешкод для цифрової торгівлі»[39]. Але в той час як у США, де поняття цифрового суверенітету має переважно негативне значення, потенційно перешкоджаючим вважається широкий спектр політик, включаючи цензуру, фільтрацію, локалізацію та додатковий (занадто сильний) захист інтелектуальної власності. Відповідні заходи та правила для запобігання дезінформації та захисту конфіденційності — в інших регіонах і країнах, таких як Європа та Канада, були запропоновані більш вузькі визначення, які враховують конкретні торговельні обмеження через проблеми конфіденційності та культурні винятки[40].

---

[35] Summa H. A. How GAIA-X is Paving the Way to European Data Sovereignty. Dotmagazine. 2020, March. URL: https://www.dotmagazine.online/issues/cloud-and-orientation/build-your-own-internet-gaia-x.

[36] 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. 2(3), 1–41.

[37] Pinto R. Á. (2018). Digital Sovereignty or Digital Colonialism? New tensions of privacy, security and national policies. Sur, 15(27), 15–27. https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism/

[38] Kwet M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. Race & Class, 60(4), 3–26. https://doi.org/10.1177/0306396818823172

[39] 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. 21(2), 245–272. https://doi.org/10.1093/jiel/jgy019

[40] Там само.