# 1. РОЛЬ ЦИФРОВИХ ІНФРАСТРУКТУР У ЗАБЕЗПЕЧЕННІ ЦИФРОВОГО СУВЕРЕНІТЕТУ

## 1.1. Співвідношення понять цифрова інфраструктура та цифровий суверенітет

Зростання цифрових мереж у 1990-х призвело до зникнення чітких інформаційних кордонів держави. На перший погляд здається, що цифрова трансформація та глобальна технічна інфраструктура Інтернету кидають виклик державному суверенітету. Принципи територіальності та державної ієрархії виявляються протилежними до гнучкої, змінюваної сукупності глобальних цифрових мереж. Більше того, цифрові додатки та комунікаційні практики створили імпульс, який, суперечить правовому державному управлінню та контролю. Яскраво це було відображено у Декларації незалежності кіберпростору Джона Перрі Барлоу[2]. Проте, сьогодні її частіше розглядається як загроза, ніж обіцянка. Щоб протистояти ризикам для своїх повноважень, уряди держав створюють можливість забезпечення виконання національних законів і вжити державне втручання в цифрову сферу. Протягом багатьох років державні органи створювали та реформували технічні та юридичні інструменти для вирішення питань цифрового управління.

Ще десять років тому ідея цифрового суверенітету асоціювалася з авторитарними країнами на кшталт Китаю, Ірану та Північної Кореї, де через контроль інформаційних технологій закриті політичні режими намагалися захиститися від впливів глобалізованого світу.

Однак в сучасному світі цифрові технології все більше впливають на державну політику. Всім відома ситуація про заборону в США китайського TikTok. Або про те, що Facebook та Twitter маркують, як сумнівні, дописи Дональда Трампа, де він висловлює свою думку щодо результатів виборів.

[2] A Declaration of the Independence of Cyberspace (Feb. 1996). URL: http://www.eff.org/pub/Publications/John_Perry_Barlow/barlow_0296.declaration

Паралельно з цим сьогодні в Європейському Союзі на повний голос заявляють про необхідність визначення терміну «цифровий суверенітет»[3].

Питання цифрового суверенітету, як невід'ємної складової інформаційного, в умовах глобалізації економіки, формування єдиного інформаційного простору, швидкого зростання світового цифрового ринку, розвитку інформаційних технологій, засобів обробки інформації, інформаційних послуг та їх впливу на забезпечення національної та міжнародної безпеки, виходить на перший план. Зростає усвідомлення важливості проблем регулювання суспільних відносин у цифровій сфері, зокрема узгодження підходів до формулювання поняття «цифровий суверенітет», визначення його характеристик для отримання відповіді на питання про правові методи й засоби його забезпечення та збереження.

Для України така правова категорія є особливо важливою в умовах гібридних війн, що ставить питання існування суверенної Української держави в безпосередню залежність від забезпечення інформаційного суверенітету держави, в тому числі цифрового.

В українському понятті «інформаційний суверенітет» вперше з'являється в Законі України «Про інформацію». Відповідно до статті 53 основою інформаційного суверенітету України є національні інформаційні ресурси. До інформаційних ресурсів входить вся належна їй інформація, незалежно від змісту, форм, часу і місця створення. Україна самостійно формує інформаційні ресурси на своїй території і вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними договорами. У статті 54 «Гарантії інформаційного суверенітету» зазначається, що «інформаційний суверенітет України забезпечується: виключним правом власності України на інформаційні ресурси, що формуються за рахунок коштів державного бюджету; створенням національних систем інформації; встановленням режиму доступу інших держав до інформаційних ресурсів України; використанням інформаційних ресурсів на

[3] Рибалко А. Цифровий суверенітет Європейського Союзу та перспективи України. URL: https://csd.org.ua/2020/11/17/czyfrovyj-suverenitet-yevropejskogo-soyuzu-ta-perspektyvy-ukrayiny/

основі рівноправного співробітництва з іншими державами». Проте, змінами, внесеними до цього закону 09.05.2011 р. ці статті були виключені. Законодавцем було враховано висновки експертів Ради Європи та вилучено поняття «інформаційний суверенітет», що, на їх думку, «не належить до принципів, вжитих хоча б в одному договорі про захист прав людини»[4]. Проте, зважаючи на те, що сучасне розуміння демократичного, правового суспільства виходить з поваги і потреби захисту прав, свобод та безпеки людини на основі принципів законності та верховенства права, необхідно досягти балансу між правом на інформацію та вимогами щодо забезпечення інформаційної безпеки держави[5].

Відповідно до Закону України «Про Національну програму інформатизації» від 4 лютого 1998 року № 74/98-ВР під поняттям «інформаційний суверенітет держави» розуміється здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави[6].

Законодавець декілька разів звертав на цю проблему увагу органів виконавчої влади. Так, відповідне завдання щодо розробки Закону України «Про інформаційний суверенітет та інформаційну безпеку України» було на порядку денному Кабінету Міністрів України ще в 2001 році – згідно з затвердженим планом законопроектної роботи на 2001 рік.

Про необхідність забезпечити інформаційний суверенітет держави згадується і в указі Президента України «Про Доктрину інформаційної безпеки України» від 8 липня 2009 року № 514/2009, що втратив чинність 30 червня 2014 року. У розділі «Основні засади інформаційної безпеки України» вказується, що «основною метою реалізації положень Доктрини інформаційної безпеки України є створення в Україні розвиненого національного інформаційного простору і захист її інформаційного суверенітету».

---

[4] Висновок експертів Ради Європи щодо проекту закону про інформацію. URL: http://www.helsinki.org.ua/index.php?id=1173882959.

[5] Солодка О.М. Забезпечення інформаційного суверенітету держави: правовий дискурс. *Інформація і право*. 2020. № 1(32). URL: http://il.ippi.org.ua/article/view/200311/200450.

[6] **Про Національну програму інформатизації: Закон України від 4 лютого 1998 року № 74/98-ВР. URL:** https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80/ed20201016#Text

Сучасні інформаційні технології дають змогу державам реалізувати власні інтереси, послабити або завдати значної шкоди безпеці конкурентної держави, яка не має дієвої системи захисту від негативних інформаційних впливів. Саме тому сьогодні відбувається змагання держав і великих корпорацій за право контролювати інформаційний простір, впливати на суспільну думку власних громадян та громадян інших країн.

Виходячи із зазначеного визначення та залежно від державної геополітичної, інформаційної та технологічної політики під терміном «цифровий суверенітет» слід розуміти здатність держави створити автономну цифрову інфраструктуру та самостійно здійснювати її керування, управляти інформаційними потоками, обмежувати їх і претендувати на ексклюзивне право визначати національний дискурс та інформаційне поле, а також забезпечувати можливість контролювати і встановлювати правові межі транснаціональним технологічним компаніям, через які перерозподіляються інформаційні потоки.

В свою чергу, цифрова інфраструктура, через яку реалізується цифровий суверенітет, створює умови та формує екосистему розвитку цифрових інновацій. Цифрові інфраструктури є основою цифрової економіки. Держава має важливе значення у створенні як твердої, так і м'якої цифрової інфраструктури. Широкосмуговий доступ із використанням фіксованих та мобільних технологій (4G, 5G) має стати пріоритетним напрямом розвитку твердої інфраструктури. Швидкість, кількість підключень та обсяги передавання даних мають критично важливе значення для економіки Індустрії 4.0 і цифрових сервісів, що ґрунтуються на технологіях штучного інтелекту та предиктивній аналітиці.

Відповідно до проєкту «Україна 2030Е – країна з розвинутою цифровою економікою» основними завданнями уряду повинна стати, по-перше, реалізація проєктів побудови *твердої інфраструктури*, а саме: розбудова фіксованої інфраструктури широкосмугового доступу до мережі Інтернет; інфраструктури мобільного Інтернету; радіоінфраструктури (LoRaWan тощо) для проектів Інтернету речей; інфраструктури громадського доступу до Wi-Fi;

обчислювальної інфраструктури (хмарна, або віртуалізована інфраструктура); створення інфраструктури кібербезпеки.

По-друге, створення *м'якої інфраструктури*, як інфраструктури ідентифікації та довіри (citizen ID, mobile ID, bank ID), інфраструктури відкритих даних, державних послуг (e-government), інтероперабельності, е-комерції та е-бізнесу, транзакційно-процесингову інфраструктуру, інфраструктуру життєзабезпечення, геоінформаційну інфраструктуру, блокчейн-інфраструктуру[7].

Створення інноваційної цифрової інфраструктури залежить від рівня технологічного розвитку національної економіки та рівня забезпечення цифрового суверенітету. У країнах, що мають розвинену виробничу інфраструктуру, спостерігається процес швидкого розвитку саме м’якої інфраструктури (soft infrastructure на відміну від hard infrastructure), що характеризується підвищенням ролі нематеріальних чинників виробництва й інформатизацією суспільства.

М'яка інфраструктура – це всі послуги, які необхідні для підтримання економічних, медичних, культурних та соціальних стандартів населення, на відміну від жорсткої інфраструктури, яка є фізичною інфраструктурою доріг, мостів тощо. Вона включає як фізичні активи, такі як спеціалізовані будівлі та обладнання, а також нефізичні активи, такі як зв'язок, зведення правил і положень, що регулюють різні системи, фінансування цих систем, системи та організації, в яких готуються професіонали, просуваються кар'єрними сходами, набуваючи досвіду та дисциплінарних стягнень, якщо цього вимагають професійні асоціації. Вона включає в себе такі інститути, як фінансова система, система освіти, система охорони здоров'я, система державного управління, правоохоронні органи, екстрені служби.

Сутність м'якої інфраструктури полягає у наданні населенню спеціалізованих послуг. На відміну від більшої частини сектора послуг

[7] Україна 2030Е – країна з розвинутою цифровою економікою. URL: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html#summary

економіки, надання цих послуг залежить від високорозвинених цифрових систем та великих спеціалізованих об'єктів.

Формування «м'якої інфраструктури» повинно відбуватися через створення системи залучення в господарський оборот об'єктів інтелектуальної власності, розширення каналів поширення інформації, удосконалювання цифрових комунікацій шляхом залучення венчурного капіталу.

Залежно від провідної ідеологічної та / або геополітичної парадигми, в якій живе та чи інша країна, й відбувається керування цифровою інфраструктурою. Деякі держави запроваджують централізоване державне управління, як от Китай, що захищається прямолінійно, запровадивши значну кількість обмежень на своїй території. Держави-члени Європейського Союзу здійснюють регулювання, оперуючи гаслами про захист прав людини.

У першому випадку держави остерігаються переважно втручання та «м'якої сили» інших держав. Класичним прикладом такого остереження є Китай із його проєктом «Золотий Щит», або, як його ще називають, «Великий китайський фаєрвол». Розпізнавальна риса цього проєкту – заборона безлічі сайтів, включно з такими платформами як Facebook, YouTube та їм подібні, а також сувора модерація активності й контенту в мережі[8].

У Європейському Союзі дедалі частіше говорять про цифровий суверенітет, але в контексті цифрової безпеки. Так, у програмному документі «Цифровий порядок денний для Європи»[9] цифрові платформи визнані акторами прогресу для людей, суспільства й економіки. Поставлено задачу створити умови, щоб вони не використовувалися для дестабілізації демократії ЄС, як дезінформація та меседжі ненависті в Інтернеті». Відповіддю має стати Європейський демократичний план дій, який би включав законодавчі ініціативи щодо більшої прозорості, наприклад, політичної реклами в мережі.

---

[8] Шульга О. Цифровий суверенітет і українське суспільство. Час для дискусії настав. URL: https://zn.ua/ukr/tech/cifroviy-suverenitet-i-ukrayinske-suspilstvo-chas-dlya-diskusiyi-nastav-335318_.html

[9] A Digital Agenda for Europe Communication from the Commission to the European Parliament, Council, the European Economic and social Committee and the Committee of the regions Brussels, Brussels, 26.8.2010 COM(2010) 245 final/2. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF

Це лягає в загальну канву стурбованості Євросоюзу не так з приводу «м'якої сили» та ідеологічної боротьби з боку інших країн, як необхідністю вдосконалити своє законодавство та виробити норми для технологічних компаній і транснаціональних корпорацій, що оперують у цифровій сфері й реально впливають на повсякденне життя європейських громадян[4].

Таким чином, європейці наголошують на виробленні правил і контролі за доброчесністю з боку засобів масової комунікації як суб'єктів недоброчесних дій стосовно не тільки держави, а й суб'єктів господарювання та громадян. Показовим прикладом може слугувати скандал навколо компанії Cambridge Analytica, що отримала доступ до особистих даних десятків мільйонів користувачів Facebook без їхнього на те дозволу й використовувала їх для впливу на виборчу кампанію у США 2016 року[10].

Присутні як в авторитарних, так і в демократичних країнах, претензії та пропоновані заходи, що підкреслюють автономію та самовизначення держав і безпеку критично важливих цифрових інфраструктур, зустріли жорстку критику. Як політичні суб'єкти, так і суб'єкти господарювання, а також науковці та технічні експерти, побоюються, що зусилля, спрямовані на ІТ-безпеку та регулювання інтернет-проблем на національному рівні, завадять відкритій та загальнодоступній природі Інтернету, що зрештою призведе до ретериторіалізації глобального Інтернету, спричинивши його фрагментацію у національні сегменти Інтернету[11]. Це, у свою чергу, може мати значні негативні економічні та політичні наслідки для відповідних країн через їх цифрову та географічну ізольованість.

Існує й друга категорія претензій на цифровий суверенітет, яка тісно пов'язана, але відрізняється від фокусування на державній автономії. Це підкреслює високі та часто протилежні економічні ставки навколо цифрового середовища та акцентує увагу на автономії національної економіки по відношенню до іноземних постачальників технологій та послуг. Як і попередня

[10] Сафаров А. Скандал з витоком даних у Facebook: як це сталося? URL: https://p.dw.com/p/2vq0i.
[11] Milton Mueller. Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace, Cambridge, UK: Polity. 2017. 140 pp.

категорія тверджень, твердження, що зосереджуються на економічному самовизначенні, були передусім викликані усвідомленим домінуванням на ринку технологічних компаній з США і все більше також Китаю. Аналогічно, конкретні заходи та інструменти, які уряди застосовують для компенсації цих дисбалансів у цифровій економіці, частково збігаються із заходами, спрямованими на посилення безпеки технологічних систем та національної автономії. Але на відміну від першої категорії, ці заходи зазвичай є частиною загальної стратегії економічної та промислової політики країни, спрямованої на цифрову трансформацію цілих секторів економіки. Таким чином, вони стосуються як традиційних галузей (телекомунікації, медіа, логістика), так і нових економічних секторів, пов'язаних із ІТ, і насамперед мають на меті сприяння інноваційній потужності вітчизняної економіки. Крім того, зростаюча кількість правових інструментів зосереджена на цифровій / електронній торгівлі та прагне регулювати потоки даних, що надходять через цифрові мережі[12].

Аналітики звертають увагу, що компанії Google, Apple, Facebook, Amazon і Microsoft збирають величезні обсяги персональних даних для просування реклами. Але ці ж дані можна використати з метою формування політичних симпатій. Крім том, дискусію викликає ідея відстежування соціальних контактів для стримання розповсюдження COVID-19.

Як й інші країни, Україна зіштовхується з величезним впливом технологічних корпорацій, які забезпечують роботу та доступ до всесвітньої цифрової інфраструктури. Тому Україна як держава вимушена активно боротися за цифровий суверенітет в умовах інформаційних та гібридних воїн.

Проте, в цьому напрямку не проводить жодної активної політики. Вирішено деякі тактичні завдання через блокування російської соцмережі «Вконтакте» та низки російських сайтів. Однак в глобальному кіберсвіті Україна залишається лише об'єктом – ринком збуту та джерелом поповнення кадрів для світових корпорацій. Наша держава не може брати участь у проєктах ЄС щодо

[12] Burri M. (2017). The Regulation of Data Flows through Trade Agreements. Georgetown Journal of International Law, 48(1), 408–448.

цифрових комунікацій, оскільки перспективи повноправного членства з правом голосу для України є туманними. А віддавати контроль за власним цифровим простором, не маючи впливу на прийняття рішень, немає сенсу.

Таким чином, держави, які претендують на збереження своєї суб'єктності на світовій арені, зобов'язані звернутися до питання забезпечення цифрового суверенітету. Адже до сфери його реалізації входять: вітчизняні цифрові інфраструктури, власний національний сегмент Інтернету, засоби захисту, пошукові системи, соціальні мережі, засоби масового зв’язку та багато іншого. В ідеалі, цифровий суверенітет, може бути забезпечений лише за наявності розвиненої цифрової інфраструктури, зокрема: власної апаратної платформи (мережевої та ПК), інтернет-інфраструктури, медійної інфраструктури ЗМІ, ТБ та якісного доступу до Інтернету, систем пропаганди, ідеології та, безперечно, розвиненої законодавчою базою. Законодавче забезпечення цифрового суверенітету має виражатися у закріпленні його цілей, принципів регулювання та повноважень органів державної влади.

Концепція цифрового суверенітету продовжить набувати ще більшої політичної популярності в найближчі роки, враховуючи широке розгортання надзвичайно інвазивних цифрових технологій, починаючи від штучного інтелекту та Інтернету речей та технологій e-Government.