## 1.3. Світовий досвід реалізації цифрового суверенітету

Термін цифровий чи технологічний суверенітет вперше був популяризований у маніфестах конфіденційності, спрямованих на отримання більшого індивідуального контролю над особистою інформацією, що поширюється через соціальні мережі та в контексті споживачів Інтернету. Це допомогло стимулювати нещодавній Загальний регламент Європейського Союзу про захист даних (GDPR) та Рамку захисту конфіденційності США та ЄС.

Західні автори переважно розглядають суверенітет через призму державної юрисдикції над інфраструктурою, програмним забезпеченням та даними, використовуючи термін «цифровий суверенітет». Науковці з просторів СНД визнають важливість контролю за інфраструктурою, але використовують ширший підхід, включаючи у проблематику також питання контролю за транскордонним контентом. Вони розглядають суверенітет через призму загроз у сфері інформаційної безпеки та пов'язують цифровий суверенітет із політичними та правовими режимами обробки даних в Інтернеті.

У сучасних умовах, коли загрози безпеці, пов'язані з розвитком інформаційно-комунікаційних технологій, виходять на передній план політичного порядку денного на світовому та національному рівнях, проблематика забезпечення суверенітету у цифровій сфері набуває не лише академічного, а й прикладного значення. У доповіді групи урядових експертів 68 сесії Генеральної Асамблеї ООН 2013 р. зазначено, що на поведінку держав в інформаційному просторі поширюється державний суверенітет та міжнародні норми, що випливають із принципу державного суверенітету. Згідно з документом, суверенітет також поширюється на юрисдикцію країн над ІКТ-інфраструктурою на їх території. Таким чином, різні визначення цифрового, інформаційного та технологічного суверенітетів виходять із підходу, який сформульований у межах категорії вестфальського суверенітету, орієнтованого недопущення інших акторів до втручання у владні структури всередині кордонів носія суверенітету.

Європейські занепокоєння щодо іноземних технологічних компаній, які виходять далеко за межі закону про конфіденційність. Однією з поширених скарг є низькі — хоча й законні — ставки податків, які сплачують глобальні інтернет-гіганти в Європі, що призвело до відчуття суверенного безсилля, незважаючи на спроби у Франції та інших країнах запровадити податок на цифрові послуги.

Іншим є очевидна неспроможність європейських компаній зрівнятися за масштабами та домінуванням на ринку іноземних постачальників хмарних послуг. У великих європейських столицях зміцнилися настрої, що іноземним компаніям не можна дозволяти захоплювати інші розвиваються ринки, як-от ринки аналізу даних за допомогою штучного інтелекту.

Політичні лідери як у Франції, так і в Німеччині нещодавно висловилися за спроби розробити «європейських чемпіонів» як альтернативу американським хмарним провайдерам. Але на грудень 2019 року докази протилежного були явними: 92% даних західного світу зберігаються в Сполучених Штатах Америки[41].

Шість із десяти найбільших у світі технологічних фірм є американськими, жодна не є європейською. За оцінками аналітичного центру CEPS, що базується в Брюсселі, одна американська компанія — Amazon Web Services (AWS) — володіє третиною світового ринку зовнішніх серверів, на яких розміщені корпоративні дані. Незабаром йдуть Microsoft і Google з часткою ринку 16% і 7,8% відповідно.

Незважаючи на попередні невдалі зусилля Франції з підтримкою держави, щоб зламати цей ринок, Франція готова спробувати знову. Міністр фінансів Бруно Ле Мер нещодавно заявив, що провідні французькі компанії Dassault і OVH розроблять плани щодо виходу на ринок хмарних послуг[42].

У жовтні Париж і Берлін оголосили про новий проєкт, відомий як Gaia-X , для підключення різних хмарних провайдерів по всій Європі за допомогою відкритих стандартів, що дозволить підприємствам і клієнтам вільно

[41] Has Europe left it too late to achieve digital sovereignty? The World Economic Forum's Geostrategy platform. 2019. URL: https://www.weforum.org/agenda/2019/12/has-europe-left-it-too-late-to-achieve-digital-sovereignty.
[42] Там само.

переміщувати свої дані в мережі, за умови забезпечення конфіденційності та безпеки спільних даних. стандарти. У заяві міністерства економіки Німеччини описано Gaia-X як «засіб для створення платформ «Зроблено в Європі»» і стверджує, що це «дозволить компаніям і бізнес-моделям вийти з Європи на конкурентоспроможність у всьому світі». Організатори проекту також очікують, що такий широкий пул даних стане цінним ресурсом для розробки інструментів аналізу даних із залученням штучного інтелекту.

Оскільки все більше державних установ у Європі довіряють дані державного сектору хмарним компаніям США і все більше покладаються на їхнє програмне забезпечення, по всьому континенту зросла занепокоєння щодо здатності уряду США та компаній отримувати збережені дані європейців для власних цілей.

У вересні 2019 р. міністерство внутрішніх справ Німеччини оприлюднило дослідження, яке воно замовило у консалтинговій фірмі PWC про «цифровий суверенітет у державному управлінні». Міністр внутрішніх справ Хорст Зеехофер наголосив на висновку звіту про зростання залежності від стандартизованих програмних продуктів кількох іноземних компаній. «Щоб захистити наш цифровий суверенітет, — сказав він, — ми зменшимо залежність від окремих IT-провайдерів, а також розглянемо альтернативні програми для заміни певного програмного забезпечення»[43].

Це оголошення у Німеччині було оприлюднено після низки рішень на рівні штату більше не використовувати іноземне програмне забезпечення для обробки публічних даних. Наприклад, Microsoft втратила контракти на використання своєї програми Office 365 у школах Гессена після того, як державний орган із захисту даних заперечив, що технологічний гігант може використовувати зібрані дані учнів для власних внутрішніх бізнес-цілей.

Хоча європейські уряди залишають занепокоєння щодо широкого охоплення розвідувальних органів США, останнім часом більшу занепокоєність

[43] Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern. Abschlussbericht. 2019. URL: https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf?__blob=publicationFile.

зосереджується на експансивній екстериторіальній здатності правоохоронних органів США отримувати персональні дані іноземців. Закон США «Про роз'яснення законного використання даних за кордоном» 2018 року або Закон «Про хмари» роз'яснює, що суд США може вимагати від інтернет-платформи з присутністю в США надавати особисту інформацію клієнта для використання в кримінальному розслідуванні або судовому переслідуванні в США, навіть якщо ці дані зберігаються на іноземному сервері.

Європейські уряди починають реагувати на Закон про хмари таким чином, що підкреслює суверенітет. У Швеції урядова організація з цифровізації eSam постановила, що передача даних державного сектору на аутсорсинг американським постачальникам хмарних послуг, які підпадають під дію Закону про хмари, порушить закон цієї країни про публічний доступ до інформації та секретності. У Франції урядова комісія опублікувала доповідь Говена, в якій рекомендує посилити та розширити сферу дії закону про блокування країни, щоб запобігти корпоративному дотриманню односторонніх вимог правоохоронних органів США щодо електронних даних.

Європейський Союз намагається реагувати на такі виклики і вже встановив жорсткі рамки для конфіденційності та захисту даних (GDPR). Уряди Німеччини та Франції ініціювали створення європейського хмарного проєкту Gaia-X. Також Єврокомісія прийняла рекомендацію про спільний підхід до безпеки мереж 5G.

Більш детально звернемося до досвіду Німеччини. Тут федеральна адміністрація в багатьох місцях використовує стандартні продукти від комерційних постачальників програмного забезпечення. Деякі з цих постачальників, схоже, використовують свої джерела живлення на свою користь і задовольняють вимоги клієнтів, напр. Наприклад, підвищена потреба в інформаційній безпеці в державному секторі не може бути вирішена або вирішена лише недостатньо. Це може поставити під загрозу цифровий суверенітет адміністрації і стосується не лише федерального уряду та уряду штатів у цій країні (наприклад, Шлезвіг-Гольштейн), але також є проблемою в інших країнах (наприклад, Королівство Нідерланди, Республіка Корея). Для

федеральної адміністрації короткострокове розслідування залежності від постачальників програмного забезпечення є незамінним, щоб ініціювати відповідні кроки для збереження цифрового суверенітету. Крім того, портфель програмного забезпечення федеральної адміністрації стає все більш централізованим із збільшенням використання стандартних продуктів у результаті проекту «Федеральна консолідація IT»[44]. Цей процес загрожує погіршенням ситуації, але в той же час дає сприятливу можливість цілеспрямовано контролювати розробку та використання програмного забезпечення та зменшувати наявні залежності.

Велика частина портфелю програмного забезпечення федеральної адміністрації Німеччині складається із запатентованого стандартного програмного забезпечення, яке буде використовуватися у великій концентрації в майбутньому навіть після консолідації IT у рамках федеральної консолідації IT (IT-K Bund) окремих постачальників програмного забезпечення, а також можливість того, що вони можуть використати це на свою користь. Інші державні клієнти в Німеччині та за кордоном також визначили це як ризик і працюють над можливими рішеннями. Наприклад, Шлезвіг-Гольштейн прийняв стратегію з відкритим кодом, щоб зменшити частку власних програмних продуктів і, таким чином, залежність від окремих постачальників. Уряд Нідерландів перевірив інформаційну безпеку домінуючого стандартного програмного забезпечення, а потім розпочав переговори з постачальником. Франція та Південна Корея вирішили запровадити програмне забезпечення з відкритим кодом. Нинішні дебати про наслідки санкцій США проти Huawei також ілюструють проблеми, які можуть виникнути через залежність від іноземних постачальників програмного забезпечення[45]. На цьому тлі цю тему необхідно розглянути, зокрема, щодо цифрового суверенітету та інформаційної

[44] Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern. Abschlussbericht. 2019. URL: https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf?__blob=publicationFile.

[45] Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern. Abschlussbericht. 2019. URL: https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf?__blob=publicationFile.

безпеки федеральної адміністрації. Проєкт також пропонує можливість перебудови програмного портфеля федеральної адміністрації та протидії цьому розвитку. Національні та міжнародні приклади показують можливі альтернативні рішення.

Федеральна адміністрація сильно залежить від кількох постачальників програмного забезпечення на всіх рівнях програмного стеку. Особливо це стосується Microsoft, чиї продукти широко використовуються та тісно пов'язані (наприклад, Outlook, Exchange та Windows Server). Тому в цьому дослідженні детально розглянуті продукти Microsoft Office, Windows і Windows Server, які найчастіше використовуються.

Зараз ринок зосереджений на кількох постачальниках програмного забезпечення, що, як правило, віддає перевагу залежностям. Стратегічна орієнтація цих провайдерів загрожує посиленням цих залежностей у майбутньому. Це включає в себе постійне розширення власної цифрової екосистеми, зростаючу конверсію від локальних рішень до хмарних рішень, а також більшу прихильність цих постачальників до розробки програмного забезпечення з відкритим кодом (OSS). На додаток до продуктів, що лідирують на ринку, є також інші запатентовані і відкриті альтернативи, деякі з яких є порівнянними з точки зору продуктивності[46].

Згідно з результатами цього аналізу, залежність від продуктів Microsoft, зокрема, призводить до проблемних точок для федеральної адміністрації, що суперечить стратегічним цілям федерального IT. Насамперед, критичними є обмежена інформаційна безпека та (захист даних) правова невизначеність; обидва моменти, які ставлять під загрозу цифровий суверенітет держави.

Аналіз показує сильну залежність від продуктів Microsoft Office, Windows і Windows Server у федеральній адміністрації. Це створює критичні больові точки. Залежність в основному спричинена сильною мережею IT-ландшафту, звичками використання співробітників та домінуючою позицією Microsoft на

[46] У контексті цього дослідження під «запатентованим» програмним забезпеченням розуміють програмне забезпечення, яке розроблено та ліцензоване комерційними виробниками та вихідний код якого не є загальнодоступним. До «ПЗ з відкритим вихідним кодом» (OSS) відносимо до відкритих і вільних програм (також «FLOSS»). Окремий випадок приватного програмного забезпечення з відкритим кодом не розглядається.

ринку. Цей високий рівень залежності має особливо критичний вплив на інформаційну та юридичну (захист даних) безпеку, яка потенційно піддається ризику, насамперед, через впровадження хмарних рішень та передачу телеметричних даних. Microsoft також набуває більшого впливу на ціноутворення та інновації. Зрештою, ці болючі точки ставлять під загрозу цифровий суверенітет федеральної адміністрації. Без коригувальних заходів ця критична ситуація триватиме після 2025 року, в тому числі через діяльність IT-K Bund.

Таким чином, вбачається, що схожа ситуація відбувається і в Україні, що дозволяю використати проаналізований досвід у вирішенні проблем забезпечення контролю над цифровими інфраструктурами (як твердими, так і м’якими) у межах державної території.