

*Туренко Ана Юрїївна*

*аспірантка НДІ державного будівництва*

*та місцевого самоврядування НАПрН України*

## **ЦИФРОВИЙ СУВЕРЕНІТЕТ І ЙОГО РОЛЬ В ЗАБЕЗПЕЧЕННІ ЕКОНОМІЧНОЇ БЕЗПЕКИ НА ПРИКЛАДІ ЄВРОПЕЙСЬКОГО СОЮЗУ**

Серед європейців зростає занепокоєння тим, що індивіди, бізнес і навіть держави-члени ЄС дедалі більше втрачають контроль над своїми даними, над своєю здатністю до інновацій, а також формувати і забезпечувати дотримання законодавства в цифровому середовищі. У цьому зв'язку зростає підтримка нового політичного підходу, спрямованого на посилення стратегічної автономії Європейського Союзу в цифровій сфері. Це передбачає розробку, оновлення та адаптацію низки чинних правових, регуляторних і фінансових інструментів ЄС, а також більш активне просування європейських цінностей і принципів у таких сферах, як захист даних, кібербезпека та етично розроблений штучний інтелект.

**Ключові слова:** цифровий суверенітет, економічна безпека, Європейський Союз.

*Turenko Anna Yuriievna*

*Postgraduate student of the Research Institute*

*of State Building and Local Self-Government*

*of the National Academy of Legal Sciences of Ukraine*

## **DIGITAL SOVEREIGNTY AND ITS ROLE IN ENSURING ECONOMIC SECURITY ON THE EXAMPLE OF THE EUROPEAN UNION**

There is a growing concern among Europeans that individuals, businesses, and even EU member states are increasingly losing control over their data, their ability to innovate, and to shape and enforce legislation in the digital environment. In this regard, there is growing support for a new policy approach aimed at strengthening the EU's strategic autonomy in the digital sphere. This involves the development, updating and adaptation of a number of existing EU legal, regulatory and financial instruments, as well as more active promotion of European values and principles in areas such as data protection, cybersecurity and artificial intelligence.

**Keywords:** digital sovereignty, economic security, European Union

З проблемою забезпечення економічного і технологічного суверенітету на сучасному етапі розвитку тісно пов'язана проблема цифрового суверенітету<sup>8</sup> [1]. Поняття «цифровий суверенітет» відбиває труднощі, з якими стикаються сучасні держави під час реалізації своїх традиційних функцій. Ці труднощі пов'язані з тим, що національні уряди іноді залежать від могутніх транснаціональних акторів, які мають незаперечну технологічну перевагу, оскільки їм потрібні технологічні послуги (такі як хмарні обчислення) для реалізації своїх функцій. Таким чином, вираз «цифровий суверенітет», безперечно, має як юридичний аспект, оскільки відноситься до прерогатив держави та її здатності регулювати сучасних технологічних гігантів, так і економічний та промисловий аспект. Таким чином, Цифровий суверенітет стосується як здійснення державних прерогатив у кіберпросторі, так і питання технологічної незалежності, також відомого як «стратегічна автономія» [2].

Цифровий суверенітет є важливим фактором у світі конфіденційності. Недивно, що однією з проблем, пов'язаних з цифровим суверенітетом, є те, що незначна кількість великих технологічних компаній контролює величезні обсяги даних про своїх користувачів<sup>9</sup>. І з такою кількістю користувачів і такою кількістю інформації їх політика та дії можуть мати значний вплив.

Для Європейського Союзу цифровий суверенітет не є синонімом протекціонізму, а більше стосується захисту його системи цінностей і принципів у кіберпросторі, а також захист індивідуальних прав (таких як людська гідність, право на недоторканність приватного життя, захист персональних даних свобода вираження поглядів), закріплених у Хартії основних прав ЄС, Європейській конвенції про захист прав людини і

---

<sup>8</sup> Слід зазначити, що підходи до тлумачення змісту неоднакові і залежать насамперед від політичного режиму держави. Так, в КНР цифровий суверенітет реалізується згідно з класичним розумінням поняття «суверенітет», тобто захисна його інтерпретація, спрямована на запобігання втручанням у внутрішні справи Китаю з метою збереження цілісності та авторитету Комуністичної партії. КНР також дотримується вимоги щодо суверенної рівності держав в глобальному управлінні. Нарешті, Китай заперечує «багатосторонню участь» Інтернетом, коли технічне співтовариство, приватний сектор та громадянське суспільство відіграють значно більшу роль в управлінні Інтернетом, ніж уряд; у Китаї саме уряд ухвалює остаточні рішення в цій сфері. Схожі позиції займає і рф. Загалом з початку 2000-х років КНР і рф намагаються побудувати так званий суверенний Інтернет як на нижніх рівнях (сервери, протоколи), так і на верхніх рівнях (соціальні мережі, служби обміну повідомленнями) Інтернету.

<sup>9</sup> 92 % даних із Заходу розміщено в США; в топ-20 світових технологічних брендів немає європейських компаній.

основоположних свобод, Загальній декларації прав людини, а також здатності ЄС приймати суверенні рішення.

Одним із прикладів принципу застосування цифрового суверенітету є Європейський регламент про захист даних (GDPR), який встановлює ключові вимоги до обробки даних, пов'язані з європейськими фізичними чи юридичними особами. Він прагне уніфікувати те, як персональні дані обробляються в Інтернеті за допомогою правил і положень, а також із загрозою каральних санкцій. GDPR поширює цей принцип безпеки даних у всьому світі та вимагає, щоб закордонні дилери європейських даних дотримувалися правил. Він також встановлює потенційні штрафи у розмірі майже 25 мільйонів доларів за витік даних.

Технологічний зсув, представлений 5G, поставив під питання цифровий суверенітет держав-членів ЄС та Європейського Союзу загалом (цей висновок буде справедливий і для країн-кандидатів, зокрема України), що побічно також позначається на економічному суверенітеті та безпеці цих держав. Як наслідок, Європейська комісія прагне створити безпечніший цифровий простір, в якому будуть захищені основні права користувачів, і прагне створити рівні умови для бізнесу. З цією метою у 2020 р. було розроблено Закон про цифрові ринки (DMA) та Закон про цифрові послуги (DSA), які разом створюють фундамент цифрової стратегії ЄС щодо адаптації Європи до цифрового століття [3; 4].

Європейський Союз щодо телекомунікацій та 5G не зміг об'єднатися, щоб захистити свої інтереси від американських та азіатських технологічних гігантів: при виборі виробників телекомунікаційного обладнання держави-члени проводять індивідуальну, часом суперечливу політику. Як наслідок, на цифровому рівні загалом спостерігається сильна технологічна залежність європейських країн від GAFAM. Аналогічна існує й у службах. Це дозволяє GAFAM втручатися у функціонування всіх секторів європейської економіки. Слід також згадати такий чинник тиску на економічний суверенітет як екстериторіальність законів США, завдяки чому американські компанії пред'являють позови європейським компаніям з багатьох технологій. У

результаті європейські компанії не мають законних засобів для боротьби і часто віддають свої технологічні напрацювання американцям. Китай, зі свого боку, використовує інший метод отримання доступу до європейських інновацій: він змушує компанії, які прагнуть влаштуватися на його території, створювати спільне підприємство з китайською компанією, таким чином одержуючи доступ до патентів та інновацій. У зв'язку з цим слід визнати, що враховуючи стратегічний характер телекомунікацій, відсутність у ЄС та країн, які прагнуть набути членства в ньому, зокрема України, бачення економічної та стратегічної розвідки створює реальну проблему не лише для автономії держав, а й для промислового шпигунства та технологічної стійкості [5].

Європейський Союз і провідні держави-члени перебувають у пошуку адекватної відповіді на зазначені виклики [6]. Перед європейцями постала дилема: або створити європейського постачальника послуг, здатного конкурувати з американськими гіперскалерами, або побудувати стратегічну автономію в найбільш критичних секторах (наприклад, в автомобілебудуванні, охороні здоров'я, енергетиці та ін.), використовуючи комбінацію постачальників хмарних послуг (у тому числі неєвропейських), за умови дотримання ними правил щодо портативності, інтеперабельності та суверенітету даних. Перший варіант був реалізований у Франції у 2012 – 2015 роках компаніями Numergy та Cloudwatt, запущеними SFR та Orange за підтримки французького уряду, але зрештою був зупинений через недостатню кількість користувачів. Альтернативою стало ініційоване в 2021 р. Німеччиною, Францією та Італією створення довіреної хмари для державного сектору та чутливих сфер, де проникнення хмарних технологій вважається пріоритетом і де неєвропейські хмарні технології приймаються за умови, що вони повністю експлуатуються європейськими компаніями (Orange, Deutsche Telekom та ін.) [7].

## ЛІТЕРАТУРА

1. Новіков Є. А. Мережа трансферу технологій та її вплив на технологічну безпеку (основні аспекти). *Право та інновації*. 2015. № 3 (11). С. 39-44.

2. Digital sovereignty. URL: <https://www.sciencespo.fr/public/chaire-numerique/en/thematic-research/digital-and-data-sovereignty/>.

3. L'Europe est impuissante face aux géants du numérique ! Vraiment ? URL: [https://france.representation.ec.europa.eu/informations/leurope-est-impuissante-face-aux-geants-du-numerique-vraiment-2022-06-30\\_fr](https://france.representation.ec.europa.eu/informations/leurope-est-impuissante-face-aux-geants-du-numerique-vraiment-2022-06-30_fr).

4. Des GAFA européens sont-ils possibles ? Rapport rédigé par les membres du Comité Economie & Finance du Cercle Orion. 2021. URL: <https://static1.squarespace.com/static/5c56d14cf4e5317cafc282cd/t/603aa249e1d214172d1212bc/1614455371496/Cercle+Orion+-+Des+GAFAM+europ+ee%C4%A3ens+sont-ils+possibles.pdf>.

5. Souveraineté numérique européenne : 5G et aveu d'échec. 2022. URL: <https://portail-ie.fr/analysis/3030/souverainete-numerique-europeenne-5g-et-aveu-dechec>.

6 Яковюк І. В. Інноваційна стратегія ЄС: уроки для України. *Право та інноваційне суспільство : електронне видання*. 2014. Вип. 2(3).

7. Tardieu H. & Otto B. (2021). Souveraineté digitale : Puissance européenne pour les Données et le Cloud, in *varietate concordia. RED*, 3, 107–113. <https://doi.org/10.3917/red.003.0107>.

## REFERENCES

1. Novikov E.A. Technology transfer network and its impact on technological security (main aspects). *Law and Innovation*. 2015. № 3 (11). Pp. 39-44.

2. Digital sovereignty. URL: <https://www.sciencespo.fr/public/chaire-numerique/en/thematic-research/digital-and-data-sovereignty/>.

3. L'Europe est impuissante face aux géants du numérique ! Vraiment ? URL: [https://france.representation.ec.europa.eu/informations/leurope-est-impuissante-face-aux-geants-du-numerique-vraiment-2022-06-30\\_fr](https://france.representation.ec.europa.eu/informations/leurope-est-impuissante-face-aux-geants-du-numerique-vraiment-2022-06-30_fr).

4. Des GAFA européens sont-ils possibles ? Rapport rédigé par les membres du Comité Economie & Finance du Cercle Orion. 2021. URL: <https://static1.squarespace.com/static/5c56d14cf4e5317cafc282cd/t/603aa249e1d214>

172d1212bc/1614455371496/Cercle+Orion+-  
+Des+GAFAM+europ+ee%C4%A3ens+sont-ils+possibles.pdf.

5. Souveraineté numérique européenne : 5G et aveu d'échec. 2022. URL: <https://portail-ie.fr/analysis/3030/souverainete-numerique-europeenne-5g-et-aveu-dechec>.

6. Yakoviyk I. V. Innovation strategy of the EU: lessons for Ukraine. *Law and innovative society: electronic edition*. 2014. Issue. 2(3).

7. Tardieu H. & Otto B. (2021). Souveraineté digitale : Puissance européenne pour les Données et le Cloud, in *varietate concordia. RED*, 3, 107–113. <https://doi.org/10.3917/red.003.0107>.