

УДК 340.12(043)

Руслан Сидорович
Національний університет “Львівська політехніка”,
аспірант Навчально-наукового інституту права,
психології та інноваційної освіти
sudor2023@ukr.net
ORCID ID: <https://orcid.org/0009-0002-1447-0583>

АСПЕКТ ЗБАЛАНСОВАНOSTI ПРИ РЕАЛІЗАЦІЇ ПРИНЦИПУ ВІДКРИТОСТІ І ПРОЗОРОСТІ ІНСТИТУТУ ДЕРЖАВНОЇ СЛУЖБИ: ПИТАННЯ “КІБЕРСУВЕРЕНІЗАЦІЇ”

<http://doi.org/10.23939/law2023.39.028>

© Сидорович Р., 2023

Стаття присвячена визначенню аспектів збалансованості при реалізації принципу відкритості і прозорості інституту державної служби, а також розгляду цієї проблематики в контексті викликів інформаційного суспільства, зокрема щодо “кіберсуверенізації”.

Принцип відкритості та прозорості включає ряд аспектів, тому вагомо, щоб він був рівною мірою забезпечений як у виборчий, так і міжвиборчий період, на етапі нормопроєктування, прийняття рішення та його виконання. Мотивовано, що криза політичної та правової реальності, військові дії, атаки на систему електронного урядування створюють необхідність визначити межі відкритості та доступності діяльності органів публічної влади.

В контексті “кіберсуверенізації” зазначено, що ідея накладання суверенітету в інтернеті, тобто розподіл і контроль інформаційних ресурсів в межах територіальної цілісності держави вважається часто технічно неможливою, однак нещодавні дослідження показали, що спеціалізовані уряди можуть змінити маршрутизацію та потоки даних відповідно до національних уподобань, якщо вони мають на це політичну волю і ресурси.

Вказано, що при реалізації процесу принципу відкритості та прозорості в інституті державної служби вагомим є досягнення балансу між забезпеченістю доступу громадян до інформації та збереженням конфіденційності й безпеки. Важливим аспектом є встановлення чітких процедур та стандартів щодо обробки та розголошення інформації, що враховують нормативну базу та специфіку роботи державних службовців.

При цьому необхідно надавати громадськості доступ до ключової інформації про діяльність інституту, включаючи прийняття рішень та виконання завдань, забезпечення відкритості інтелектуальної власності високого рівня довіри до державних установ та підвищення ефективності їх функціонування.

Паралельно, слід завершити, що деяка інформація може бути обмежена оглядом на її конфіденційний характер або може вплинути на безпеку держави, такі випадки вимагають обґрунтованих заходів з обмеженням доступу до відомостей. Загалом, збалан-

Аспект збалансованості при реалізації принципу відкритості і прозорості інституту...

сованість у реалізації принципу відкритості та прозорості в інституті державної служби є чинником для забезпечення ефективності управління та довіри до владних структур.

Ключові слова: органи державної влади; публічна служба; відкритість; доступність; прозорість; принципи; інформаційне суспільство.

Постановка проблеми. Відкритість і прозорість у державній службі відіграє важливу роль у забезпеченні ефективності та довіри в механізмі державно-владного веління, є фундаментальними основами для розвитку відкритого та інклюзивного спілкування між державою та громадянами. Така практика сприяє підвищенню довіри до державних інституцій та ефективності їх роботи, що своєю чергою сприяє кращому задоволенню потреб громадян та досягненню загального добробуту суспільства.

Прозорість є важливим виміром суспільної цінності. Це підвищує підзвітність державної служби, формує довіру громадян до уряду та культивує демократичний і відповідальний процес управління за участю. Проте забезпечення такого принципу не може бути повною мірою реалізовано, враховуючи сучасні загрози інформаційного, глобалізованого та транзитивного суспільства.

Суттєвим фактом є те, що принцип відкритості та прозорості не передбачає відсутності обмеження доступу до інформації, оскільки таке може бути зумовлено потребою захисту прав та свобод громадян, державною, національною безпекою та іншими факторами.

Аналіз дослідження проблеми. Сутнісні характеристики, питання оновлення та дієвості концепції відкритості влади було аналізом багатьох фахівців, зокрема І. М. Жаровської, Т. З. Гарасиміва, В. Б. Ковальчука, Ю. М. Бисаги та інших.

Набагато ширше питання трансформації принципу відкритості в інформаційній модифікації нової моделі суспільства досліджували представники зарубіжної доктрини, зокрема Succiniello M., Nasi G., Y. S. Zamani, Sh. S. Dawes та інші.

Метою статті є визначення аспектів збалансованості при реалізації принципу відкритості і прозорості інституту державної служби, а також розгляд цієї проблематики в контексті викликів інформаційного суспільства, зокрема щодо “кіберсуверенізації”.

Виклад основного матеріалу. Загалом принцип відкритості та прозорості включає ряд аспектів і вагомо, щоб він був рівною мірою забезпечений як у виборчий, так і міжвиборчий період, на етапі нормопроєктування, прийняття рішення та його виконання. Забезпечення загальної громадськості та зацікавленим сторонам доступу до необхідної та актуальної інформації включає надання інформації про рішення, політику, бюджет та інші аспекти роботи державних органів. Прийняття рішення повинно бути відкритим, з можливістю публічного обговорення та залучення громадськості, своєю чергою державні органи повинні регулярно подавати звіти про свою діяльність, включаючи результати, витрати та іншу важливу інформацію, забезпечення можливостей для громадськості брати участь у процесах прийняття рішень та обговорення питань, які стосуються суспільства загалом.

У контексті сучасного інформаційного суспільства, де зростає значення технологій та цифрових засобів спілкування, відкриваються нові форми відкритості державної влади. Однією з них є електронне урядування, або e-Government. Ця парадигма передбачає використання інформаційних технологій для покращення доступу громадян до публічної інформації, зокрема, через електронні платформи та веб-портали органів влади.

Технологічний прогрес уможливив відкриті державні ініціативи багатьох урядів, які публікують державні дані в зручних для користувача форматах і сприяють цифровій прозорості [1]. Ці ініціативи відкритого уряду використовують різні інструменти для аналізу, візуалізації та інтерпретації даних у цифрових форматах, щоб забезпечити зручність для користувачів. Підвищена

прозорість реалізується в цьому процесі шляхом розкриття інформації про урядові операції та створення більшої відкритості для прийняття урядових рішень і операцій. Роль громадян також була трансформована в цьому процесі: від виключно одержувачів до користувачів і творців даних.

Крім того, сучасні соціальні мережі та платформи для обговорення громадських питань стають додатковим каналом для взаємодії між владою та громадянами, що модерує можливості для публічної дискусії, збору публічної думки та залучення громадськості до процесів прийняття рішень. Іноземні науковці відзначають багатоаспектність застосування сучасних технологій у стратегічному розвитку публічних організацій з різноманітністю технологічних впливів на стійкість комунікації державних службовців, головним чином через відсутність досвіду і скромні компетенції застосування сучасних засобів комунікації на практиці, а також недостатність уваги до сучасних комунікаційних технологій у рамках політики та політичних пріоритетів. Інформаційне суспільство надає додаткові засоби реалізації прав та свобод громадян [2]. А також модернізує комунікацію між органами державної влади та громадськістю, і доречно було б, щоб правова політика держави впроваджувала прогностичну цілісність та імплементувала позитивні додаткові можливості в функціонування інституту публічної служби.

Більш тісна співпраця з громадськими організаціями, активістами та експертами також стає елементом відкритості державної влади, залучення зацікавлених сторін (наприклад, представників національних меншин) до діалогу, сприяє більш обґрунтованому та взаємоприйнятному прийняттю рішень.

Додатково, аспектом є створення та підтримка відкритих даних (Open Data), які дають можливість громадськості використовувати та аналізувати інформацію, яка надається державними органами. Така систематизація означає надання загальнодоступних, машинночитабельних та повних даних, які можуть бути вільно використані і розширені, включаючи різноманітні дані, які охоплюють суттєві галузі функціонування влади для людини, такі як економіка, освіта, охорона здоров'я, навколишнє природне середовище, соціальні послуги тощо. Відкриті дані дозволяють громадянам, дослідникам та підприємствам використовувати цю інформацію для аналізу, створення нових продуктів та послуг, а також моніторингу роботи владних структур. Такий підхід стимулює інновації в різних сферах громадянського суспільства.

Усі ці форми відкритості сприяють збільшенню нової прозорості та відкритості державної влади, забезпечуючи більш активну участь громадян у прийнятих рішеннях та підвищуючи рівень довіри до влади.

Представники американської школи права вказують, що існує напруженість щодо оприлюднення урядової інформації, яка може підлягати неправильному тлумаченню через відсутність описових метаданих або потребу в експертних системах відліку чи специфічних аналітичних навичках. Ці проблеми часто виникають, коли інформація використовується не для тих цілей, для яких вона була зібрана. Така інформація зазвичай не збиралася з метою оприлюднення, управління рідко здійснюється структурованим способом, що ускладнює використання та інтерпретацію іншими та стає більш схильним до неправильного розуміння та неправильного використання. Крім того, деяка інформація вважається надто конфіденційною або небезпечною для оприлюднення (наприклад, відомості про атомні електростанції, військові об'єкти чи електромережі) [3].

Проте криза політичної та правової реальності, військові дії, атаки на систему електронного урядування створює необхідність визначити межі відкритості та доступності діяльності органів публічної влади. Сьогодні слід говорити про проблеми "кіберсуверенітету". В останні роки дискусія про цифровий суверенітет перейшла з авторитарних держав на західні, ліберальні держави, такі держави, як Росія та Китай, відстоюють ідею абсолютизації "кіберсуверенітету" протягом приблизно двох десятиліть, зосереджуючись на концепції інформаційної безпеки, що означає державний контроль над міжнародними і внутрішніми потоками інформації та безперервністю режиму [4]. Сумнозвісний Великий китайський брандмауер і нещодавні російські плани створення Рунету є технологічним втіленням цих уявлень про суверенітет, блокуючи доступ до несанкціоно-

ваного вмісту та обов'язкову маршрутизацію інформації всередині країни, що призводить до абсолютизації контролю за громадськістю і відповідно можливість блокування публічної інформації, її поширення.

Західні країни традиційно чинили опір вказаній доктрині кіберсуверенітету, віддаючи перевагу ідеї відкритого та вільного інтернету з точки зору цифрової економіки та захисту фундаментальних прав і засуджуючи інформаційну безпеку як троянського коня для запровадження контролю над контентом. Проте в останні роки західні країни почали приймати наратив цифрового суверенітету та стратегічної автономії для вирішення проблем цифрового зовнішнього втручання державних акторів і залежності від іноземних урядів та іноземних великих технологічних платформ та інфраструктур, таким чином “демократизуючи” мову суверенітету в глобальній цифровій сфері за межами авторитарних держав [5].

Розглядувана ідея накладання суверенітету в інтернеті, тобто розподіл і контроль інформаційних ресурсів в межах територіальної цілісності держави вважається часто технічно неможливим. Одним із часто почутих технічних аргументів проти суверенітету в інтернеті є те, що розподілена архітектура інтернету та логіка маршрутизації не здатні впоратися з нав'язуванням меж суверенітету. Однак нещодавні дослідження показали, що спеціалізовані уряди можуть змінити маршрутизацію та потоки даних відповідно до національних уподобань, якщо вони мають на це політичну волю і ресурси. Наприклад, Росія фактично відокремила Крим від української маршрутизації та вбудувала його в російські мережі, зробивши Крим “російським” з точки зору потоків цифрових даних [6].

Вважаємо за необхідне визначити збалансований підхід у функціонуванні публічно-владних інституцій, тому визначимо теоретико-правові аспекти легітимності обмеження доступу до публічної інформації.

По-перше, таким аспектом є конфіденційність та безпека. Деякі інформаційні дані можуть бути конфіденційними, такими як особиста інформація, державні та військові таємниці, що вимагають їх обмеженого доступу для забезпечення безпеки осіб та країни загалом.

По-друге, обмеження може потребувати дипломатична та міжнародна діяльність, оскільки вказане потребується для захисту національних інтересів та досягнення дипломатичних цілей.

По-третє, безпека громадськості як основна функція держави також може визнаватися легітимною при поширенні інформації, котра спричиняє паніку, громадські заворушення, або може порушити планові заходи щодо боротьби з тероризмом, тому відкритість обмежується для захисту громадян.

Також, по-четверте, урядові органи можуть обмежувати доступ до даних, які стосуються комерційних угод, щоб запобігти можливому витoku конфіденційності комерційної інформації.

І останнє, певні чутливі дані особистого етичного характеру також не підлягають розголошенню. Принципи етики та особистої конфіденційності можуть вимагати обмеження доступу до деякої інформації, зокрема, що стосується людей, їхнього здоров'я та приватного життя.

Таким чином, прозорість роботи органів влади має бути збалансована з іншими цінностями та вимогами, щоб забезпечити ефективне та відповідне управління, уникаючи при цьому можливих негативних наслідків. Важливим є те, щоб обмеження публічної інформації були обґрунтованими, пропорційними та дотриманими принципів правової держави та демократії, а також мали казусний індивідуально-розглядуваний характер. Наприклад, інформація про стан здоров'я державного службовця (припустімо, вживання ним наркотичних речовин) не може бути предметом легітимного правомірного обмеження, поряд з цим інформація про стан здоров'я його неповнолітніх дітей буде тією морально-етичною сферою, де відкритість даних не допустима.

Висновок. При реалізації процесу принципу відкритості та прозорості в інституті державної служби вагомим є досягнення балансу між забезпеченістю доступу громадян до інформації та збереженням конфіденційності й безпеки. Важливим аспектом є встановлення чітких процедур та

стандартів щодо обробки та розголошення інформації, що враховують нормативну базу та специфіку роботи державних службовців.

При цьому необхідно надавати громадськості доступ до ключової інформації про діяльність інституту, включаючи прийняття рішень та виконання завдань, забезпечення відкритості інтелектуальної власності високого рівня довіри до державних установ та підвищення ефективності їх функціонування.

Паралельно, слід завершити, що деяка інформація може бути обмежена оглядом на її конфіденційний характер або може вплинути на безпеку держави, такі випадки вимагають обґрунтованих заходів з обмеженням доступу до відомостей. Загалом збалансованість у реалізації принципу відкритості та прозорості в інституті державної служби є чинником для забезпечення ефективності управління та довіри до владних структур.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cucciniello M., Nasi G. Transparency for Trust in Government: How Effective is Formal Transparency? *International Journal of Public Administration*, 2014. Vol. 37:13, P. 911–921, DOI: 10.1080/01900692.2014.949754.
2. Laužikas M., Miliūtė A. Impacts of modern technologies on sustainable communication of civil service organizations. *Entrepreneurship and sustainability issues*. 2020. Vol. 7, N 3 DOI: 10.9770/jesi.2020.7.3(69)2495 .
3. Dawes Sh. S. Stewardship and usefulness: Policy principles for information-based transparency. *Government Information Quarterly*. 2010. Vol. 27, Is. 4. P. 377–383.
4. Creemers R.J.E.H. China's conception of cyber sovereignty: rhetoric and realization. In: Broeders D. & Berg B. van den (Eds.) *Governing Cyberspace: Behavior, Power, and Diplomacy*. Digital Technologies and Global Politics Lanham: Rowman & Littlefield, 2020. P. 107–142.
5. Kadenko N., Broeders D., van Eeten M., Borgolte K., Fiebig T. Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Government Information Quarterly*. 2023. Vol. 40, Is. 4, October 2023, 101862.
6. Douzet F., Pétiñaud L., Salamatian L., Limonier K., Salamatian K., Alchus T. Measuring the fragmentation of the Internet: The case of the Border Gateway Protocol (BGP) during the Ukrainian crisis 2020. 12th international conference on cyber conflict (CyCon). 2020. P. 157–182, 10.23919/CyCon49761.2020.9131726.

REFERENCES

1. Cucciniello M., Nasi G. (2014). *Transparency for Trust in Government: How Effective is Formal Transparency?* *International Journal of Public Administration*, 37:13, P. 911–921, DOI: 10.1080/01900692.2014.949754 [in English];
2. Laužikas M., Miliūtė A. (2020). *Impacts of modern technologies on sustainable communication of civil service organizations*. *Entrepreneurship and sustainability issues*. 7 (3) DOI: 10.9770/jesi.2020.7.3(69)2495 [in English];
3. Dawes Sh. S. (2010) *Stewardship and usefulness: Policy principles for information-based transparency*. *Government Information Quarterly*. 27 (4), P. 377–383 [in English];
4. Creemers R.J.E.H. (2020). *China's conception of cyber sovereignty: rhetoric and realization*. In: Broeders D. & Berg B. van den (Eds.) *Governing Cyberspace: Behavior, Power, and Diplomacy*. Digital Technologies and Global Politics Lanham: Rowman & Littlefield, P. 107–142 [in English];
5. Kadenko N., Broeders D., van Eeten M., Borgolte K., Fiebig T. (2023). *Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions*. *Government Information Quarterly*. 40 (4) 101862 [in English];
6. Douzet F., Pétiñaud L., Salamatian L., Limonier K., Salamatian K., Alchus T. *Measuring the fragmentation of the Internet: The case of the Border Gateway Protocol (BGP) during the Ukrainian crisis* (2020). 12th international conference on cyber conflict (CyCon). P. 157–182, 10.23919/CyCon49761.2020.9131726 [in English].

Дата надходження: 11.08.2023 р.

Ruslan Sydorovych

Lviv Polytechnic National University,
Educational and Scientific Institute of Law,
psychology and innovative education
sudor2023@ukr.net

ORCID ID: <https://orcid.org/0009-0002-1447-0583>

**THE ASPECT OF BALANCE IN THE IMPLEMENTATION OF THE PRINCIPLE
OF OPENNESS AND TRANSPARENCY OF THE CIVIL SERVICE INSTITUTE:
THE ISSUE OF “CYBER SOVEREIGNTY”**

The article is devoted to the definition of aspects of balance in the implementation of the principle of openness and transparency of the civil service institute, as well as consideration of this issue in the context of the challenges of the information society, in particular, in relation to “cyber-sovereignization”.

The principle of openness and transparency includes a number of aspects so that it is equally ensured both in the election and inter-election periods, at the stage of normative design, decision-making and its implementation. It is motivated by the fact that the crisis of political and legal reality, military actions, attacks on the electronic government system creates the need to determine the limits of openness and accessibility of the activities of public authorities.

In the context of “cybersovereignization” it is stated that the idea of imposing sovereignty on the Internet, that is, the distribution and control of information resources within the territorial integrity of a state is often considered technically impossible, but recent studies have shown that specialized governments can change the routing and data flows according to national preferences if they want to have the political will and resources for it.

It is indicated that when implementing the process of the principle of openness and transparency in the civil service institute, it is important to achieve a balance between ensuring citizens’ access to information and preserving confidentiality and security. An important aspect is the establishment of clear procedures and standards for the processing and disclosure of information that take into account the regulatory framework and the specifics of the work of civil servants.

At the same time, it is necessary to provide the public with access to key information about the institute’s activities, including decision-making and execution of tasks, ensuring the openness of intellectual property, a high level of trust in state institutions and increasing the efficiency of their functioning.

At the same time, it should be concluded that some information may be limited to review due to its confidential nature or may affect the security of the state, such cases require reasonable measures to restrict access to information. In general, balance in the implementation of the principle of openness and transparency in the civil service institute is a factor for ensuring the effectiveness of management and trust in the power structures.

Keywords: state authority; public service; openness; accessibility; transparency; principles; information society.