

УДК 004.056:342.9

JEL Classification: H83, K23, O33, L86

DOI: <https://doi.org/10.64076/eecsr250708.04>

Філатов В. В.,

аспірант кафедри державного
управління і місцевого самоврядування,
Національний технічний університет
"Дніпровська політехніка", м. Дніпро

СУЧАСНІ ЦИФРОВІ ПЛАТФОРМИ У ПУБЛІЧНІЙ ВЛАДІ: ВИКЛИКИ ПРАВОВОГО РЕГУЛЮВАННЯ ДІДЖИТАЛІЗАЦІЇ

В умовах стрімкої діджиталізації та посилення правових режимів, зокрема під час воєнного стану, суспільство стикається не лише з трансформацією соціальних і державних інститутів, але й із необхідністю переосмислення підходів до забезпечення прав людини, інформаційної безпеки та сталого функціонування публічного простору. Опанування масштабів цифрової трансформації сьогодні нерідко супроводжується тенденцією до надмірної централізації, розширення контролю держави й окремих корпорацій над інформаційними потоками, даними та поведінкою користувачів. Це породжує значні ризики, серед яких – звуження громадянських свобод, порушення приватності, посилення нерівності доступу до цифрових ресурсів та суб'єктивізація критеріїв інформаційної безпеки.

У відповідь на ці виклики альтернативою стає розвиток децентралізованої цифрової екосистеми, в якій ключовими суб'єктами виступають не лише державні органи, а й самі громадяни, місцеві громади, незалежні експерти й громадські організації. Йдеться про побудову мережевих моделей цифрового врядування, які використовують інструменти блокчейн, peer-to-peer технології, автономні локальні дата-центри та відкриті цифрові платформи для розподілу відповідальності, ресурсів та даних між усіма учасниками. Таким чином створюється багаторівнева система управління, де ухвалення рішень і обробка інформації стають максимально відкритими, прозорими й контрольованими знизу.

Відкрите управління даними та прозорість цифрових процесів мають бути закладені в архітектуру таких платформ із самого початку: громадськість отримує інструменти прямого впливу на правила, алгоритми й регуляторні дії через незалежні наглядові органи, цифрових омбудсменів, громадські ради та механізми колективної медіації конфліктів. Це підвищує суспільну довіру до цифрових інструментів і зменшує ризик інформаційних маніпуляцій або зовнішньо керованих впливів.

Особливе значення набуває розвиток цифрової резильєнтності (стійкості) спільнот: замість одноманітних, уніфікованих стандартів кожна громада може формувати власні стратегії реагування на цифрові загрози, зважаючи на локальні ресурси, виклики та досвід. Посилення самоорганізації місцевого рівня, створення локальних етичних кодексів та стандартів у цифровій сфері дає змогу гнучко адаптуватися до змін і протидіяти загрозам розриву між центральною та периферійною інфраструктурою.

У цьому контексті співпраця між державою, громадянським суспільством і приватним сектором повинна розвиватися не як відносини "керівник-підлеглий", а як партнерська, горизонтальна взаємодія, заснована на прозорості, взаємному контролі й публічному залученні до ухвалення рішень. Такий підхід сприяє формуванню цифрового простору, дружнього до прав людини: приватність, свобода висловлювань та рівний доступ до інформації стають не декларативними цінностями, а інституційною нормою. Зрештою, розбудова відкритої й децентралізованої цифрової екосистеми – це шлях до захисту не лише інформаційного суверенітету держави, а й гідності, автономії та безпеки кожної людини. Навіть у періоди особливих (воєнних) правових режимів цей підхід посилює соціальну єдність, зміцнює довіру у суспільстві та створює основу для сталого демократичного розвитку в цифрову епоху.

У сучасних дослідженнях британських науковців питання децентралізації цифрової інфраструктури та захисту прав людини в умовах цифрової трансформації займають помітне місце.

У сучасній британській літературі значна увага приділяється питанням етичного врегулювання цифрових платформ, рівного доступу до цифрових ресурсів і ролі децентралізації для збереження свободи та приватності в умовах цифрової трансформації. Зокрема, досліджується вплив сучасних

цифрових інфраструктур на громадянські права, підкреслюючи, що розподілені цифрові моделі сприяють залученню громади до контролю над даними, підвищенню прозорості та забезпеченню справедливого доступу до цифрових благ. Так, С.Лівінгстон (S.Livingstone) наголошує, що децентралізація у цифровому врядуванні посилює позиції користувача й дозволяє формувати більш стійке до зовнішнього тиску й маніпуляцій публічне середовище [1]. У свою чергу, Л.Едвардс (L.Edwards) акцентує на необхідності ефективного правового регулювання цифрових прав та демократичного залучення громадян у цифрову політику, особливо в умовах воєнного та надзвичайного стану. На її думку, лише поєднання правових інструментів із незалежним громадським наглядом дозволяє гарантувати баланс між безпекою й фундаментальними правами, зокрема правом на приватність та свободу вираження поглядів у цифрову епоху [2].

Таким чином, погляди провідних британських дослідників підтверджують ефективність запропонованого підходу до розвитку децентралізованої, інклюзивної та етично врегульованої цифрової екосистеми, орієнтованої на захист прав людини навіть у кризових суспільних контекстах. Також варто аналізувати роль розподілених цифрових систем у забезпеченні публічної прозорості, підкреслюючи, що створення децентралізованих інформаційних платформ суттєво знижує ризики маніпуляції даними, надмірного державного контролю та нерівного доступу до інформації для різних соціальних груп. При цьому захист фундаментальних цифрових прав має забезпечуватися не тільки нормативними механізмами, а й широкою участю громадськості у виробленні політик управління даними, постійним оновленням етичних стандартів та відкриттям алгоритмів до громадського аудиту.

Список використаних джерел

1. Livingstone, S., & Third, A. (2020). Children and young people's rights in the digital age: An emerging agenda. *New Media & Society*, 22(7), 1282–1299. https://www.researchgate.net/publication/312090897_Children_and_young_people's_rights_in_the_digital_age_An_emerging_agenda.
2. Edwards, L. (2019). *Law, Policy and the Internet*. Oxford: Hart Publishing. <https://academic.oup.com/ijlit/article-abstract/27/2/204/5425255?redirectedFrom=fulltext&login=false>.