DOI: 10.33498/louu-2026-04-199

Марина Чех

аспірантка кафедри філософії
Національного юридичного університету
імені Ярослава Мудрого
(Харків, Україна)
ORCID ID: https://orcid.org/0009-0002-0450-724X
marynachekh@gmail.com

УДК 342.1:004.738.5:341

ІНФОРМАЦІЙНИЙ СУВЕРЕНІТЕТ У ЦИФРОВУ ЕПОХУ: ТРАНСФОРМАЦІЯ ДЕРЖАВНОСТІ ТА МОДЕЛЬ "СУВЕРЕНІТЕТУ ЯК ВІДПОВІДАЛЬНОСТІ"

Анотація. Цифровізація і розвиток штучного інтелекту трансформують класичну модель територіального суверенітету. Транскордонна природа кіберпростору створює розрив між прагненням держав контролювати національний інформаційний простір і децентралізованою логікою потоків даних. Для України ця проблема загострюється в умовах гібридної агресії РФ, де інформаційні операції спрямовані на підрив державності та ідентичності.

Мета статті – соціально-філософське і юридичне обґрунтування концептуальної моделі інформаційного суверенітету України як адаптивно-гібридної системи, заснованої на принципі "суверенітету як відповідальності" та сумісної зі стандартами прав людини.

Доведено еволюцію інформаційного суверенітету від моделі виключного контролю до підходу, у межах якого держава виступає гарантом цифрової гідності та ментальної цілісності громадян. Обґрунтовано необхідність правового захисту ідентичності від інформаційного насильства та запропоновано врегулювання юрисдикційних конфліктів через механізми "цифрового федералізму" й інтеграцію етичних принципів у дизайн інформаційних систем.

У статті сформовано адаптивно-гібридну модель інформаційного суверенітету, що поєднує технологічну стійкість, юрисдикційне врегулювання транскордонних потоків і аксіологічний захист гідності та прав людини. Український досвід демонструє розподілений характер такого суверенітету, де громадяни є активними суб'єктами інформаційної безпеки через розвиток критичного мислення та медіастійкості.

Ключові слова: інформаційний суверенітет; цифровий суверенітет; гібридна війна; міжнародне право; права людини.

Сучасна епоха характеризується глибокою інформатизацією суспільства, що трансформувала індустріальну модель розвитку в інформаційну, де інформація стала стратегічним ресурсом і чинником влади. Цифрові технології, глобальні мережі й системи штучного інтелекту змінили механізми політичного управління, економічної конкуренції та соціальної взаємодії, поставивши під сумнів класичне розуміння державного суверенітету як виключно територіального явища.

Транскордонна природа кіберпростору послаблює монополію держави на контроль інформаційних потоків, формуючи нові виклики для правового регулювання та безпеки. Для України ці процеси мають особливе значення в умовах гібридної війни, де інформаційні впливи виступають інструментом підриву державності та національної ідентичності. Це актуалізує потребу переосмислення суверенітету в інформаційному вимірі та вироблення концептуальної моделі, здатної поєднати технологічну стійкість, міжнародно-правові стандарти й захист прав людини.

1. Відповідність міжнародним принципам права: конфлікти і можливості узгодження

Традиційна концепція суверенітету, що сягає Вестфальського миру 1648 р., ґрунтується на парадигмі виключної та абсолютної влади держави над чітко визначеною територією й постійним населенням[1]. У класичному розумінні суверенітет є "вищою легітимною владою в межах території", що передбачає недоторканність кордонів і принцип невтручання у внутрішні справи[2]. Водночас сучасна еволюція міжнародного права відбувається в умовах гострого зіткнення цієї вестфальської моделі з реаліями цифрової глобалізації. Глобальний простір комунікацій, сформований ІКТ (інформаційно-комунікаційні технології), пролягає "поверх кордонів і національного законодавства", що спричиняє поступову десуверенізацію та послаблення ідеологічного й культурного контролю з боку держав[3]. Дослідники констатують "смерть відстані" та "кінець географії", оскільки інформаційний сектор став глобальним і виходить за межі окремих юрисдикцій[4].

Стрімка цифровізація і розвиток систем штучного інтелекту породили парадокс "суверенітету-інтернаціоналізму": держави прагнуть посилити автономний контроль над алгоритмічними системами, але змушені одночасно поглиблювати транснаціональну співпрацю, адже цифрові технології ігнорують державні кордони[5]. Цей парадокс проявляється у спробах "територіалізувати" кіберпростір, адаптуючи його архітектуру до традиційного поділу на юрисдикції[6]. Якщо раніше суверенітет виступав "захисною оболонкою" держави, то нині він трансформується у комплекс прав і обов'яз-

[1] R Polčák, D J Svantesson, *Information Sovereignty. Data Privacy, Sovereign Powers and the Rule of Law* (Edward Elgar Publishing 2017) 58 https://doi.org/10.4337/9781786439222.

[2] F Pierucci, 'Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace' [2025] 4 Digital Society 29 https://doi.org/10.1007/s44206-025-00189-4.

[3] В Брадов, 'Інформаційний суверенітет держави: глобалізаційний аспект', *International scientific and practical conference "The European development trends in journalism, PR, media and communication" (Wloclawek, Republic of Poland, October 30–31, 2020)* (Baltija Publishing 2020) 8.

[4] В Даніл'ян, 'Інформаційне суспільство та перспективи його розвитку в Україні (соціально-філософський аналіз)' (дис канд філософ наук, 2006) 46.

[5] A Ishkhanyan, 'The sovereignty-internationalism paradox in AI governance: digital federalism and global algorithmic control' [2025] 5(123) Discover Artificial Intelligence 1–14 https://doi.org/10.1007/s44163-025-00374-x.

[6] Pierucci (n 2) 28.

ків, легітимність яких визначається здатністю гарантувати цифрову безпеку та права людини в умовах глобальної взаємозалежності[7].

Центральний юридичний конфлікт розгортається між принципом “інтернет-свободи” і концепцією “інтернет-суверенітету”. Перший підхід, натхненний ідеями Декларації незалежності кіберпростору, виходить із тези про автономність цифрового середовища від державної влади[8]. Другий наголошує на праві держави втручатися в інформаційні потоки задля забезпечення національної безпеки[9]. В авторитарних моделях це призводить до створення закритих національних сегментів мережі, що виправдовується захистом від зовнішніх кібератак[10].

Проблема ускладнюється детермінізмом територіальності: у кіберпросторі “адреса” вузла мережі не має стабільного зв’язку з фізичною юрисдикцією, що підриває можливість застосування локальних законів до глобальних явищ[11]. У міжнародному праві сформувалися дві протилежні школи. Перша – “Sovereignty-as-a-Rule” – розглядає суверенітет як самостійну норму, порушення якої саме по собі є міжнародно-протиправним діянням; відповідно до Правила 4 “Талліннського посібника 2.0” держави не повинні проводити кібероперації, що порушують суверенітет іншої держави[12]. Друга – “Sovereignty-as-a-Principle” – трактує його як загальний принцип, з якого випливають конкретні заборони (невтручання, незастосування сили), але який сам по собі не створює окремої підстави відповідальності[13]. Такі розбіжності формують “сірі зони”, що використовуються для дестабілізуючих операцій у цифровому просторі[14].

З позиції міжнародного захисту прав людини ключова дилема полягає у відповідності заходів інформаційного суверенітету, яка гарантує право вільно шукати та поширювати інформацію незалежно від державних кордонів. Обмеження цього права повинні відповідати трискладовому тесту: бути встановленими законом, мати легітимну мету та бути необхідними й пропорційними в демократичному суспільстві[15]. Доступність інформації

[7] A Mills, ‘Rethinking Jurisdiction in International Law’ The British Yearbook of International Law [2014] 84(1) 187–239 https://doi.org/10.1093/bybil/bru003.

[8] О Радутний, ‘Ілюзія та реальність інформаційного суверенітету’ [2020] 4(35) Інформація і право 24 https://doi.org/10.37750/2616-6798.2020.4(35).221215.

[9] С Куцепал, ‘Інформаційний суверенітет та інформаційна безпека України: виклики та реалії війни’ [2023] 1 Полтавський правовий часопис 78–88 https://doi.org/10.21564/2786-7811.1.290476.

[10] Радутний (н 8) 23.

[11] D R Johnson, D Post, ‘Law and Borders: The Rise of Law in Cyberspace’ [1996] 48(5) Stanford Law Review 1367–1402 https://doi.org/10.2307/1229390.

[12] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (M N Schmitt (ed), 2nd ed. Cambridge University Press 2017) 17 https://doi.org/10.1017/9781316822524.

[13] G P Corn, R Taylor, ‘Sovereignty in the Age of Cyber’ [2017] 111 AJIL Unbound 208 https://doi.org/10.1017/aju.2017.57.

[14] L Chircop, ‘Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0’ [2019] 20(2) Melbourne Journal of International Law 350.

[15] О Солодка, ‘Забезпечення інформаційного суверенітету держави: правовий дискурс’ [2020] 1(32) Інформація і право 85 https://doi.org/10.37750/2616-6798.2020.1(32).200311.

має переважати над виправданням її обмеження[16]. Водночас використання інтернет-шатдаунів, масового стеження чи практик "капіталізму стеження" під приводом безпеки підриває право на приватність та цифрове самовизначення[17].

Для України ця проблема набуває екзистенційного характеру в умовах гібридної агресії, коли інструменти інформаційної свободи використовуються для руйнування державності та національної ідентичності[18]. У цьому контексті постає питання про формування права на захист ipse-ідентичності – ментальної цілісності особистості від зовнішніх маніпулятивних впливів[19].

Можливість формування узгодженої доктрини інформаційного суверенітету пов'язана з визнанням того, що кіберпростір не є terra nullius. Звіти Групи урядових експертів ООН та положення Талліннського посібника підтверджують застосовність суверенітету до діяльності держав у сфері ІКТ та їх юрисдикції над інфраструктурою на власній території[20]. Водночас сучасний суверенітет дедалі частіше інтерпретується не як "право на панування", а як "відповідальність за захист"[21].

У доктринальному вимірі це передбачає поєднання кількох підходів. По-перше, цифрового федералізму, що базується на принципі субсидіарності та багаторівневому управлінні[22]. По-друге, цифрового конституціоналізму, який формує систему гарантій проти зловживань як державної, так і корпоративної влади[23]. По-третє, функціонального суверенітету, що означає здатність держави самостійно визначати траєкторію цифрового розвитку без самоізоляції від глобального ринку[24].

Для України це означає формування адаптивно-гібридної моделі, що інтегрує технологічну (контроль критичної інфраструктури)[25], юрисдикційну (ефективне регулювання цифрових процесів)[26] та аксіологічну (захист

[16] К Ісмайлов, Д Бєлих, 'Інформаційний суверенітет і Доктрина інформаційної безпеки України' [2019] 1 Порівняльно-аналітичне право 206–209.
[17] M Lukings, A H Lashkari, *Understanding Cybersecurity Law in Data Sovereignty and Digital Governance: An Overview from a Legal Perspective* (Springer 2022) 175 https://doi.org/10.1007/978-3-031-14264-2.
[18] В Горбулін (ред), *Світова гібридна війна: український фронт* (НІСД 2017) 392.
[19] О Данильян, О Дзьобань, 'Людина в інформаційному суспільстві: проблема моральної ідентифікації' [2019] 1(40) Вісник НЮУ імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія 10 https://doi.org/10.21564/2075-7190.40.155746.
[20] В Тернавська, 'Концепція державного суверенітету в аспекті глобального інформаційного простору' [2021] 4(39) Інформація і право 85 https://doi.org/10.37750/2616-6798.2021.4(39).248794.
[21] Mills (n 7) 188.
[22] Ishkhanyan (n 5) 6.
[23] K Yilma, 'Reimagining digital constitutionalism' [2026] 15(1) Global Constitutionalism 66 https://doi.org/10.1017/S2045381725100014.
[24] P Timmers, 'Sovereignty in the Digital Age', In H Werthner et al (eds), *Introduction to Digital Humanism: A Textbook* (Springer 2024) 582 https://doi.org/10.1007/978-3-031-45304-5_36.
[25] Р Бондаренко, В Михальчук, 'Інформаційна безпека держави' [2021] 5 Інвестиції: практика та досвід 98 https://doi.org/10.32702/2306-6814.2021.5.95.
[26] В Федюк, 'Інформаційна безпека та інформаційний суверенітет як об'єкти кримінально-правової охорони (на прикладі ст. 111 Кримінального кодексу України)' [2024] 12(54) Наукові перспективи 1385 https://doi.org/10.52058/2708-7530-2024-12(54)-1380-1391.

мови, культури, історичної пам'яті) складові[27]. Така модель передбачає активну роль громадянського суспільства, медіаграмотність і критичне мислення як елементи колективної стійкості[28], а держава має функціонувати як сервіс безпеки, що гарантує право на достовірну інформацію та захист від когнітивних загроз, не порушуючи права на приватність[29].

Отже, відповідність інформаційного суверенітету міжнародним принципам права залежить від здатності держав трансформувати вестфальські ідеали в модель відповідальної взаємозалежності, де захист національного цифрового простору гармонізується з універсальними стандартами прав людини та принципом суверенної рівності держав.

2. Етична і філософська оцінка інформаційного суверенітету

Сучасна етична оцінка інформаційного суверенітету вимагає докорінного перегляду класичної парадигми суверенітету як виключного панування (dominium) над територією та ресурсами. У традиційному вестфальському розумінні суверенітет поставав як "захисна оболонка" державної влади, що гарантувала її автономію та невтручання у внутрішні справи. Проте в умовах цифрової трансформації та глобальної мережевої взаємозалежності таке розуміння втрачає нормативну достатність. Суверенітет дедалі більше легітимується не фактом контролю, а здатністю відповідально забезпечувати права, безпеку та гідність людини[30].

Класична філософія держави, представлена, зокрема, Г. В. Ф. Гегелем, визначала державу як "реальність моральної ідеї" та вищу форму об'єктивізації свободи[31]. У цій оптиці суверенітет є іманентною якістю державної влади, що володіє верховенством на власній території. Водночас перехід до інформаційної цивілізації зумовлює еволюцію цієї категорії: від "права на виключне владарювання" – до концепції "суверенітету як відповідальності"[32]. Державний суверенітет більше не може слугувати "ліцензією" на порушення прав людини або інструментом самоізоляції; він передбачає позитивний обов'язок гарантувати стабільність життєвого простору громадян у цифровому середовищі[33].

[27] Є Мануйлов, Ю Калиновський, 'Аксіологічний вимір інформаційної безпеки української держави' [2017] 3 Вісник Національного університету "Юридична академія України імені Ярослава Мудрого". Серія: Філософія, філософія права, політологія, соціологія 17.
[28] Бондаренко, Михальчук (н 25) 100.
[29] С Люлько, С Сунєгін, 'Інформаційний суверенітет держави: сутнісні характеристики' *VIII International Scientific and Practical Conference "Education and science of today: intersectoral issues and development of sciences" (May 9, 2025, Cambridge, UK)* 180–181 https://doi.org/10.36074/logos-09.05.2025.034.
[30] Timmers (n 24) 572.
[31] Г В Ф Гегель, *Основи філософії права, або Природне право і державознавство* (пер. з нім., Юніверс 2000) 115.
[32] Горбулін (н 18) 196.
[33] Солодка (н 15) 82.

Суверенітет як відповідальність (Левінас, Рікер)

Етична антропологія Е. Левінаса уможливлює радикально переосмислити інформаційний суверенітет через категорію відповідальності за Іншого[34]. За Левінасом, відповідальність передує свободі та є до-онтологічною основою людського буття[35]. У площині інформаційних відносин це означає, що держава може претендувати на регулювання цифрового простору лише остільки, оскільки воно спрямоване на захист ментальної цілісності особистості, її права на істину та недоторканність внутрішнього світу[36]. Свобода слова і свобода інформації втрачають абсолютний характер і постають як свободи-відповідальності, пов'язані з етичними наслідками поширення деструктивного чи маніпулятивного контенту.

У контексті гібридної війни це набуває особливої ваги. Інформаційна агресія спрямована не лише на поширення неправди, а на деформацію колективної пам'яті та руйнування моральної ідентичності суспільства[37]. Дезінформація діє як "інформація, що перевертає дію", позбавляючи людину здатності приймати автономні рішення[38]. У такій ситуації інформаційний суверенітет України трансформується у механізм захисту морального суверенітету нації – її духовних цінностей, історичної пам'яті та культурної самототожності[39].

П. Рікер, розвиваючи концепцію "спроможної людини" (l'homme capable), надає суверенітету виміру суб'єктності та авторства[40]. Суверенітет – це здатність діяти, відповідати за наслідки власних рішень і зберігати ipse-ідентичність у часі[41]. Для держави це означає спроможність самостійно формувати інформаційну політику, не підпадаючи під зовнішній маніпулятивний контроль. Для особи – здатність зберігати цілісність "Я" в умовах алгоритмічного тиску та нав'язаних наративів. Отже, інформаційний суверенітет постає як етико-правовий механізм протидії "інформаційному насильству" – прихованому впливу на психічні структури людини з метою програмування її поведінки[42].

Суверенітет через проєктування і цифровий гуманізм

У цифрову епоху відповідальність повинна бути інтегрована безпосередньо в архітектуру технологій. Концепція "Sovereignty-by-design" передбачає,

[34] Див.: Еманюель Левінас, *Між нами. Дослідження. Думки-про-іншого* (пер. з фр., Дух і Літера, 1999) 291.
[35] О Дзьобань, *Філософія інформаційного права: світоглядні й загальнотеоретичні засади* (Майдан 2013) 198.
[36] Є Мануйлов, Ю Калиновський, 'Інформаційний суверенітет України: сучасні виклики та загрози духовній сфері' [2019] 3(42) Вісник НЮУ імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія 32.
[37] Мануйлов, Калиновський (н 36) 22, 25.
[38] J-F Lebraty, 'La maîtrise de l'information source de souveraineté: le cas des C4iSR' Lebraty, J.-F. [2010] 1(1) Prospective et stratégie 119 https://doi.org/10.3917/pstrat.001.0103.
[39] Радутний (н 8) 34.
[40] Див.: Поль Рікер, *Сам як інший* (пер. з фр., 2. вид., Дух і Літера 2002) 456.
[41] Данильян, Дзьобань (н 19) 12.
[42] Дзьобань (н 35) 245.

що етичні принципи не є зовнішньою надбудовою, а закладаються у код, протоколи та алгоритми з моменту їх створення[43]. Людина має залишатися суб'єктом прийняття рішень, а не об'єктом алгоритмічного маніпулювання[44]. У кантівській традиції це означає збереження статусу людини як "мети в собі", а не засобу для збору даних чи отримання прибутку[45].

Цифровий гуманізм наголошує, що технології повинні слугувати людству, а не навпаки[46]. Антропоморфізація машин і делегування їм моральних рішень суперечить самій природі відповідальності, оскільки лише людина здатна "давати причини" (giving reasons) своїм діям[47]. Тому системи штучного інтелекту, які впливають на права та свободи громадян, мають функціонувати за принципом "human-in-the-loop", забезпечуючи можливість перегляду та оскарження автоматизованих рішень[48].

Негативним прикладом виступають моделі масового стеження і соціального скорингу, що перетворюють державу на "цифрового Левіафана" і підривають людську автономію[49]. Такі практики демонструють, що технологічний контроль без етичних обмежень руйнує саму основу легітимності суверенітету.

Інформаційна етика й демократична легітимність

Демократична легітимність у цифровому суспільстві ґрунтується на прозорості, підзвітності та етичній комунікації. В умовах "рефлексивної модернізації" влада легітимізується через відкритість і здатність до діалогу з громадянським суспільством[50]. Інформаційний суверенітет виконує функцію етичного фільтра, що забезпечує "ментальну вакцинацію" проти стратегічних дезінформаційних кампаній[51].

Водночас держава зобов'язана гарантувати громадянам доступ до достовірної інформації, адже "знання управлятиме незнанням". Закритість породжує недовіру та ризик узурпації влади[52]. Алгоритмічна модерація контенту, формування "ехо-камер" і "бульбашок фільтрів" підривають пуб-

[43] I Fries, M Grabatin, M Hofmeier (eds), *Sovereign by Design: The LIONS Approach to Digital Sovereignty* (Logos Verlag Berlin GmbH 2024) 7.
[44] J Nida-Rümelin, K Staudacher, 'Philosophical Foundations of Digital Humanism', In H Werthner et al. (eds), *Introduction to Digital Humanism: A Textbook* (Springer 2024) 18 https://doi.org/10.1007/978-3-031-45304-5_2.
[45] Lukings, Lashkari (n 17) 250.
[46] H Werthner, 'Digital Transformation, Digital Humanism: What Needs to Be Done', In: H Werthner et al. (eds), *Introduction to Digital Humanism: A Textbook* (Springer 2024) 130 https://doi.org/10.1007/978-3-031-45304-5_8.
[47] Nida-Rümelin, Staudacher (n 44) 25.
[48] S T Koeszegi, 'AI @ Work: Human Empowerment or Disempowerment?' In: H Werthner et al. (eds), *Introduction to Digital Humanism: A Textbook* (Springer 2024) 187 https://doi.org/10.1007/978-3-031-45304-5_12.
[49] Lian Yuming, *Sovereignty Blockchain 2.0: New Forces Changing the World of Future* (Springer 2022) 221 https://doi.org/10.1007/978-981-19-3862-7.
[50] Даніл'ян (н 4) 130.
[51] Куцепал (н 9) 86.
[52] Дзьобань (н 35) 183.

лічну сферу та поляризують суспільство[53]. Приватні цифрові платформи фактично набувають статусу "технологічних суверенів", вплив яких інколи перевищує регуляторні можливості держав[54].

Формування "Homo informaticus" – особистості, здатної до критичної рефлексії та самодетермінації в умовах інформаційного надлишку, – стає стратегічним завданням держави[55]. Захист ipse-ідентичності людини у цифровому просторі набуває характеру нового морально мотивованого права, що повинно бути інтегроване в доктрину інформаційного суверенітету[56].

Отже, інформаційний суверенітет у сучасному розумінні є не лише інструментом контролю чи безпеки, а комплексною етико-правовою категорією, що поєднує відповідальність держави, автономію особи та демократичну легітимність. Його зміцнення в Україні має спиратися на поєднання технологічного захисту, когнітивної стійкості громадян та аксіологічного відтворення гуманістичних цінностей через освіту і стратегічні комунікації[57]. Лише за умови такого синтезу інформаційний суверенітет постає як гарант гідності, свободи й історичної самототожності в цифрову епоху.

3. Формування концептуальної моделі інформаційного суверенітету

На основі системного аналізу вітчизняних і зарубіжних джерел, а також сучасних державно-правових практик пропонується цілісна концептуальна модель інформаційного суверенітету України як адаптивно-гібридна та трирівнева система. Вона розглядає суверенітет не як статичний атрибут державної влади, а як динамічний процес, що реалізується через взаємодію політичних, технологічних та етичних чинників на різних рівнях соціальної організації[58]. Така модель постає механізмом забезпечення "юридичної самостійності держави", тобто здатності не підпорядковуватися чужій волі в інформаційній сфері та зберігати суб'єктність у глобальному цифровому просторі[59].

Модель інтегрує три взаємозалежні виміри – державний (технологічно-інфраструктурний і наднаціональний), організаційно-юрисдикційний і аксіологічно-когнітивний (індивідуальний), які у своїй сукупності формують холістичну архітектуру інформаційного суверенітету. Слабкість будь-якого з них неминуче підриває стійкість системи загалом[60].

---

[53] C Heitzinger, S Woltran, 'A Short Introduction to Artificial Intelligence: Methods, Success Stories, and Current Limitations', In: H Werthner et al. (eds), *Introduction to Digital Humanism: A Textbook* (Springer 2024) 146 https://doi.org/10.1007/978-3-031-45304-5_9.

[54] Polčák, Svantesson (n 1) 130.

[55] Данильян, Дзьобань (н 19) 16.

[56] Там само 9.

[57] Мануйлов, Калиновський (н 27) 16.

[58] S Fratini, E Hine, C Novelli, H Roberts, L Floridi, 'Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models' [2024] 3(59) Digital Society 17 https://doi.org/10.1007/s44206-024-00146-7.

[59] Ісмайлов, Бєлих (н 16) 209.

[60] Ishkhanyan (n 5) 11.

1) Державний рівень: стратегічна автономія, кібермогутність і мережева влада

Перший рівень стосується здатності держави забезпечувати юрисдикційний контроль над цифровою інфраструктурою та даними як стратегічним ресурсом. У сучасній правовій доктрині спостерігається перехід від "інфраструктурної теорії", де інтернет розглядається як суто технічна мережа, до "теорії доменів", яка трактує кіберпростір як сферу реалізації суверенних повноважень[61].

Технологічно-інфраструктурний компонент передбачає багатошарову модель контролю, що охоплює фізичну інфраструктуру (дата-центри, магістральні мережі), технологічну самодостатність і захист національного сегмента мережі[62]. Розвиток власного програмного забезпечення і стандартів покликаний мінімізувати ризики "технологічної колонізації" з боку глобальних IT-гігантів[63].

У світовій практиці сформувалися різні моделі реалізації цього рівня. Китайська концепція "кібер-суверенітету" орієнтується на формування "національного корпусу даних" із жорстким державним аудитом і фільтрацією зовнішніх впливів[64]. Європейський підхід, навпаки, базується на "стратегічній автономії" та цифровому конституціоналізмі – через гармонізовані стандарти (GDPR, AI Act) і розвиток незалежних ініціатив на кшталт GAIA-X[65]. Українська модель не є ізоляційною (на відміну від RuNet), а спрямована на створення захищеного середовища для зберігання державних реєстрів і критичних даних, що забезпечує "юридичну самостійність" у розпорядженні ресурсами[66].

Для подолання парадоксу між національним контролем і глобальною взаємозалежністю доцільною є модель цифрового федералізму, що спирається на принцип субсидіарності та координацію з міжнародними партнерами[67]. У цьому проявляється гібридність українського підходу – поєднання внутрішньої автономії з міжнародною інтеграцією (CERT-UA, НАТО, ЄС)[68].

2) Організаційно-юрисдикційний рівень: суверенітет як відповідальність і корпоративна автономія

Другий рівень охоплює право й обов'язок державних і приватних організацій самостійно визначати параметри використання власних інформаційних активів, забезпечуючи їх захист від несанкціонованого доступу, включаючи втручання іноземних урядів. На цьому рівні суверенітет

[61] Ishkhanyan (n 5) 4.
[62] Солодка (н 15) 82.
[63] Тернавська (н 20) 81.
[64] Yuming (n 49) 54, 82.
[65] Pierucci (n 2) 2.
[66] Радутний (н 8) 30.
[67] Ishkhanyan (n 5) 3, 8.
[68] Люлько, Сунєгін, (н 29) 180.

трансформується з "права на обмеження" у "службу для захисту прав людини"[69].

Йдеться про встановлення балансу між приватністю комунікацій і потребами національної безпеки[70], а також про створення правових механізмів протидії "патріациду" – гібридним стратегіям знищення політичної суб'єктності через інформаційні інструменти[71]. Регулювання діяльності зарубіжних суб'єктів у "сірих зонах" національного простору має відбуватися так, щоб "доступність інформації переважала над виправданням її обмеження", окрім випадків чітко визначеної загрози безпеці[72].

Технологічним інструментом зміцнення організаційного суверенітету є впровадження "суверенного блокчейну", який формує "інтернет порядку" відповідно до національного законодавства[73]. Використання відкритих стандартів і верифікованих компонентів мінімізує ризики залежності від іноземних постачальників[74]. У цьому сенсі організації стають "квазісуверенними" акторами цифрової екосистеми, відповідальними за безпеку даних своїх клієнтів і співробітників[75].

3) Аксіологічно-когнітивний рівень: інформаційне самовизначення та ментальний імунітет

Третій, фундаментальний рівень моделі пов'язаний із захистом інформаційного самовизначення особистості. Він передбачає забезпечення контролю індивіда над власною цифровою ідентичністю та захист "когнітивного суверенітету" від маніпулятивного впливу[76].

У контексті "капіталізму стеження" особисті дані перетворюються на товар, а алгоритми – на інструменти поведінкового програмування[77]. Концептуальна модель передбачає протидію "алгоритмічному колоніалізму", коли зовнішні платформи вилучають дані населення без реальної згоди, підриваючи автономію громадян[78]. Технологічним втіленням індивідуального суверенітету є Self-Sovereign Identity (SSI), що дає змогу особі володіти своїми цифровими мандатами без централізованих посередників[79]. Права на дані

[69] О Буткевич, 'Сучасне міжнародне право: продовження «холодної війни» чи початок нової епохи?', В Репецький, В Гутник (ред), *Сучасні проблеми міжнародного права. Liber Amicorum до 60-річчя проф. М. В. Буроменського* (Фенікс 2017) 61.
[70] Солодка (н 15) 80.
[71] Буткевич (н 69) 60.
[72] Тернавська (н 20) 88.
[73] Yuming (n 49) 184.
[74] A Weber, S Reith, M Kasper et al., *Sovereignty in Information Technology: Security, Safety and Fair Market Access by Openness and Control of the Supply Chain* (KIT-ITAS 2018) <https://www.itas.kit.edu/english/2018_009.php> (accessed 27.04.2026).
[75] Lukings, Lashkari (n 17) 68.
[76] Ibid 247.
[77] S Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019) 122.
[78] F Musiani, 'Reassessing "infrastructuring digital sovereignty": digital self-determination as a set of infrastructure-embedded practices' [2025] 10 Frontiers in Sociology https://doi.org/10.3389/fcomm.2025.1562072.
[79] Lukings, Lashkari (n 17) 248.

стають складовою людської гідності й мають захищатися на рівні фундаментальних прав[80].

Водночас цей рівень охоплює формування "ментального імунітету" суспільства – здатності протистояти "бойовим наративам" і маніпуляціям історичною пам'яттю[81]. Захист IPSE-ідентичності громадянина виступає умовою національної консолідації[82].

Феномен "ІТ-армії України" демонструє розподілену відповідальність у цифрову епоху: суверенітет захищає не лише держава, а й кожний громадянин як "самостійна одиниця захисту"[83].

Синтез моделі: адаптивність і гібридність

Пропонована концептуальна модель є холістичною та адаптивною. Вона постійно трансформується у відповідь на нові кіберзагрози та "інформаційні цунамі"[84]. Її гібридність полягає в поєднанні стратегічної автономії з міжнародною кооперацією та у визнанні розподіленої відповідальності між державою, організаціями й громадянами[85].

Отже, інформаційний суверенітет постає як етичний і юридичний фільтр, що забезпечує "ментальну вакцинацію" нації, зберігаючи відкритість до глобального інформаційного обміну та демократичних цінностей[86]. Лише збалансоване поєднання державної стратегічної автономії, організаційної технологічної незалежності та індивідуального самовизначення створює дієвий правовий щит для захисту національних інтересів України у глобальному цифровому просторі[87].

Традиційне міжнародне право сьогодні опинилося в ситуації, яку дослідники влучно означують як "кризу голого імператора": вестфальська концепція територіальності дедалі частіше виявляється "непристойно роздягненою" перед реаліями транскордонного цифрового простору, де дані циркулюють незалежно від географічних кордонів, а юрисдикційні межі втрачають визначеність[88]. За цих умов інформаційний суверенітет уже не може спиратися виключно на фізичну локалізацію серверів чи інфраструктури. Його концептуальна модель має базуватися на принципі "суттєвого зв'язку" (substantial connection) між суб'єктом, даними та захищуваним інтересом[89]. Саме такий підхід дає змогу звільнити право від "зашморгу те-

[80] Yuming (n 49) 181.
[81] Горбулін (н 18) 392.
[82] Данильян, Дзьобань (н 19) 10.
[83] Радутний (н 8) 22.
[84] О Ярема, 'Зміст інформаційного суверенітету у контексті державного суверенітету' [2022] 3 Юридичний науковий електронний журнал 191 https://doi.org/10.32782/2524-0374/2022-3/43.
[85] Куцепал (н 9) 78.
[86] Люлько, Сунєгін (н 29) 180.
[87] Ishkhanyan (n 5) 11.
[88] Polčák, Svantesson (n 1) 154.
[89] Pierucci (n 2) 2.

риторіальності" та переосмислити суверенітет як динамічну, процесуальну категорію.

1) Тріада "суб'єкт – дані – інтерес" як фундамент інформаційного правопорядку

Перехід від територіального до зв'язкового (nexus-based) суверенітету означає визнання того, що дані є не статичним об'єктом власності, а динамічним процесом, включеним у мережу соціальних, технологічних і правових відносин[90]. У цьому контексті пропонується трикомпонентна модель.

Суттєвий зв'язок (фактичний рівень) – це питання реального контролю та технічної спроможності. Йдеться не про "землю", а про контроль над логічними інтерфейсами, алгоритмами, ключами доступу та архітектурою системи[91]. Наприклад, якщо українські державні реєстри розміщені в хмарних середовищах іноземного провайдера, суттєвий зв'язок із ними зберігається не через територію, а через управління криптографічними ключами, протоколами доступу та нормативним режимом обробки даних. Суверенітет тут набуває характеру процесуального контролю, а не фізичної локалізації.

Легітимний інтерес (нормативний рівень) – це вимір права, а не техніки. Держава може претендувати на юрисдикцію лише тоді, коли існує визнаний міжнародним правом зв'язок між нею та відповідними даними: захист національної безпеки, персональних даних громадян, критичної інфраструктури[92]. За відсутності такого обґрунтування втручання перетворюється на форму "цифрового колоніалізму" або "трафікування даних"[93]. Отже, інформаційний суверенітет повинен мати чітке аксіологічне підґрунтя та відповідати міжнародним стандартам прав людини.

Збалансування суверенітетів передбачає відмову від бінарної логіки "мій/чужий". У цифрову епоху над одними й тими самими даними можуть співіснувати кілька форм суверенітету – державний, організаційний, індивідуальний, – які не виключають, а взаємодоповнюють один одного залежно від інтенсивності контролю та характеру інтересу[94]. Такий підхід відкриває можливість для кооперативної моделі юрисдикції, що знижує ризик конфліктів і сприяє формуванню мережевої правової екосистеми.

2) Цифровий конституціоналізм як механізм легітимації інформаційного суверенітету

Легітимність інформаційного суверенітету не може ґрунтуватися лише на факті контролю; вона потребує нормативного обмеження влади через принципи цифрового конституціоналізму. Без цього держава ризикує

[90] Polčák, Svantesson (n 1) 144.
[91] Polčák, Svantesson (n 1) 181.
[92] Polčák, Svantesson (n 1) 142.
[93] A Kokas, *Trafficking Data: How China Is Winning the Battle for Digital Sovereignty* (Oxford University Press 2022) 24 https://doi.org/10.1093/oso/9780197620502.001.0001.
[94] Polčák, Svantesson (n 1).

трансформуватися в "цифрового Левіафана", що під приводом безпеки встановлює тотальний алгоритмічний нагляд[95].

Цифровий конституціоналізм пропонує адаптацію засад верховенства права до алгоритмічного суспільства, де обмеженню підлягає не лише держава, а й приватні технологічні корпорації, які фактично виконують квазісуверенні функції управління інформаційними потоками[96]. У цьому вимірі інформаційний суверенітет постає як розподілена система стримувань і противаг між державою, бізнесом та громадянським суспільством.

Перспективним інструментом виступає модель "Sovereignty-by-design", де правові та етичні стандарти інтегруються безпосередньо в архітектуру цифрових систем[97]. Це означає, що захист прав людини закладається на рівні коду, а не лише декларативно проголошується в законі. Показовим є європейський підхід "стратегічної автономії", який, на відміну від ізоляціоністських моделей "суверенного інтернету", прагне поєднати технологічний контроль із прозорими стандартами захисту гідності та приватності[98].

3) Від контролю до відповідальності: український вимір

У XXI ст. інформаційний суверенітет перестав бути теоретичною абстракцією та став питанням фізичного й політичного виживання держави в умовах гібридних конфліктів[99]. Втрата контролю над інформаційним компонентом веде до ерозії державності загалом[100]. Досвід російської агресії проти України переконливо демонструє, що інформаційна сфера є ключовою ареною протиборства, де "бойові наративи" використовуються для руйнування ідентичності та програмування поведінки населення[101].

Водночас сучасний суверенітет має реалізовуватися через концепцію "суверенітету-відповідальності". У філософському вимірі цей підхід корелює з ідеєю до-онтологічної відповідальності за Іншого, де держава існує насамперед як гарант гідності громадянина[102]. Суверенітет у цифрову епоху не є "ліцензією на всевладдя", а постає як обов'язок гарантувати ментальну цілісність особистості, захищати історичну пам'ять та національну ідентичність від інформаційного насильства[103].

Ключовим викликом для України є поєднання захисту інформаційного простору з дотриманням свободи вираження поглядів. Суверенне право регулювати кіберпростір не повинно суперечити міжнародним стандартам,

[95] Yuming (n 49) 135.
[96] E Celeste, 'Digital constitutionalism: A new systematic theorisation' [2019] 33(1) International Review of Law, Computers & Technology 76 https://doi.org/10.1080/13600869.2019.1562604.
[97] Timmers (n 24) 581.
[98] G Hulkó, J Kálmán, A Lapsánszky, 'The politics of digital sovereignty and the European Union's legislation: navigating crises' [2025] 7 Frontiers in Political Science https://doi.org/10.3389/fpos.2025.1548562.
[99] Горбулін (н 18) 12.
[100] V Torichnyi, T Biletska, O Rybshchun, D Kupriyenko, Y Ivashkov, A Bratko, 'Information and propaganda component of the Russian Federation hybrid aggression: conclusions for developed democratic countries on the experience of Ukraine' [2021] 25(3) Trames 357 https://doi.org/10.3176/tr.2021.3.06.
[101] Ісмайлов, Бєлих (н 16) 206.
[102] Дзьобань (н 35) 263.
[103] Буткевич (н 69) 61.

зокрема вимогам законності, легітимної мети та необхідності в демократичному суспільстві[104]. Інформаційний суверенітет має діяти як правовий фільтр, що нейтралізує зовнішні маніпуляції, водночас забезпечуючи прозорість і відкритість державного управління[105].

Висновки. Практична реалізація цієї моделі потребує розвитку когнітивної стійкості суспільства. Захист суверенітету стає справою не лише інституцій безпеки, а й кожного громадянина, який у цифровому середовищі виступає "самостійною одиницею захисту"[106]. Феномен мережевого опору та самоорганізації демонструє, що інформаційний суверенітет набуває розподіленого характеру, поєднуючи державну стратегію та громадянську ініціативу.

Отже, концептуальна модель інформаційного суверенітету має бути адаптивно-гібридною та спиратися на три взаємозв'язані виміри: технологічну спроможність контролю (інфраструктура та дані), юрисдикційне верховенство (правове регулювання на основі "суттєвого зв'язку") та аксіологічну відповідальність (захист гідності, пам'яті, мови та прав людини)[107]. Лише перехід від реактивної оборони до проактивного формування власного стратегічного наративу дасть змогу Україні зберегти суб'єктність у глобальному інформаційному суспільстві[108].

Отже, інформаційний суверенітет у XXI ст. – це не стіна, а мембрана; не ізоляція, а відповідальна інтеграція; не привілей влади, а обов'язок перед людиною. Саме в цьому полягає його нова парадигма як процесуально-етичної моделі сучасної державності.

REFERENCES

Bibliography

Authored books

1. Kokas A, *Trafficking Data: How China Is Winning the Battle for Digital Sovereignty* (Oxford University Press 2022) 24 https://doi.org/10.1093/oso/9780197620502.001.0001.
2. Lukings M, Lashkari A H, *Understanding Cybersecurity Law in Data Sovereignty and Digital Governance: An Overview from a Legal Perspective* (Springer 2022) 175 https://doi.org/10.1007/978-3-031-14264-2.
3. Yuming L, *Sovereignty Blockchain 2.0: New Forces Changing the World of Future* (Springer 2022) 221 https://doi.org/10.1007/978-981-19-3862-7.
4. Zuboff S, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019) 122.
5. Dzoban O, *Filosofiia informatsiinoho prava: svitohliadni y zahalnoteoretychni zasady* (Maidan 2013) (in Ukrainian).
6. Riker P, *Sam yak inshyi* (per. z fr., 2. vyd., Dukh i Litera 2002) (in Ukrainian).

[104] Радутний (н 8) 23.
[105] Горбулін (н 18) 243.
[106] Радутний (н 8) 22.
[107] Тернавська (н 20) 87.
[108] Ісмайлов, Бєлих (н 16) 209.

Edited and translated books

7. Fries I, Grabatin M, Hofmeier M (eds), *Sovereign by Design: The LIONS Approach to Digital Sovereignty* (Logos Verlag Berlin GmbH 2024) 7.

8. Heitzinger C, Woltran S, 'A Short Introduction to Artificial Intelligence: Methods, Success Stories, and Current Limitations', In: H Werthner et al. (eds), *Introduction to Digital Humanism: A Textbook* (Springer 2024) 146 https://doi.org/10.1007/978-3-031-45304-5_9.

9. Koeszegi S T, 'AI @ Work: Human Empowerment or Disempowerment?' In: H Werthner et al. (eds), *Introduction to Digital Humanism: A Textbook* (Springer 2024) 187 https://doi.org/10.1007/978-3-031-45304-5_12.

10. Nida-Rümelin J, Staudacher K, 'Philosophical Foundations of Digital Humanism', In H Werthner et al. (eds), *Introduction to Digital Humanism: A Textbook* (Springer 2024) 18 https://doi.org/10.1007/978-3-031-45304-5_2.

11. Polčák R, Svantesson D J, *Information Sovereignty. Data Privacy, Sovereign Powers and the Rule of Law* (Edward Elgar Publishing 2017) 58 https://doi.org/10.4337/9781786439222.

12. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (M N Schmitt (ed), 2nd ed. Cambridge University Press 2017) 17 https://doi.org/10.1017/9781316822524.

13. Timmers P, 'Sovereignty in the Digital Age', In H Werthner et al (eds), *Introduction to Digital Humanism: A Textbook* (Springer 2024) 582 https://doi.org/10.1007/978-3-031-45304-5_36.

14. Werthner H, 'Digital Transformation, Digital Humanism: What Needs to Be Done', In: H Werthner et al. (eds), *Introduction to Digital Humanism: A Textbook* (Springer 2024) 130 https://doi.org/10.1007/978-3-031-45304-5_8.

15. Bondarenko R, Mykhalchuk V, Informatsiina bezpeka derzhavy [2021] 5 Investytsii: praktyka ta dosvid 98 https://doi.org/10.32702/2306-6814.2021.5.95 (in Ukrainian).

16. Hehel H V F, *Osnovy filosofii prava, abo Pryrodne pravo i derzhavoznavstvo* (per. z nim., Yunivers 2000) (in Ukrainian).

17. Horbulin V (red), *Svitova hibrydna viina: ukrainskyi front* (NISD 2017) 392 (in Ukrainian).

18. Levinas E, *Mizh namy. Doslidzhennia. Dumky- pro- inshoho* (per. z fr., Dukh i Litera, 1999) (in Ukrainian).

Journal articles

19. Celeste E, 'Digital constitutionalism: A new systematic theorisation' [2019] 33(1) International Review of Law, Computers & Technology 76 https://doi.org/10.1080/13600869.2019.1562604.

20. Chircop L, 'Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0' [2019] 20(2) Melbourne Journal of International Law 350.

21. Corn G P, Taylor R, 'Sovereignty in the Age of Cyber' [2017] 111 AJIL Unbound 208 https://doi.org/10.1017/aju.2017.57.

22. Fratini S, Hine E, Novelli C, Roberts H, Floridi L, 'Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models' [2024] 3(59) Digital Society 17 https://doi.org/10.1007/s44206-024-00146-7.

23. Hulkó G, Kálmán J, Lapsánszky A, 'The politics of digital sovereignty and the European Union's legislation: navigating crises' [2025] 7 Frontiers in Political Science https://doi.org/10.3389/fpos.2025.1548562.

24. Ishkhanyan A, 'The sovereignty-internationalism paradox in AI governance: digital federalism and global algorithmic control' [2025] 5(123) Discover Artificial Intelligence 1–14 https://doi.org/10.1007/s44163-025-00374-x.

25. Johnson D R, Post D, 'Law and Borders: The Rise of Law in Cyberspace' [1996] 48(5) Stanford Law Review 1367–1402 https://doi.org/10.2307/1229390.

26. Lebraty J-F, 'La maîtrise de l'information source de souveraineté: le cas des C4iSR' Lebraty, J.-F. [2010] 1(1) Prospective et stratégie 119 https://doi.org/10.3917/pstrat.001.0103.

27. Mills A, 'Rethinking Jurisdiction in International Law' The British Yearbook of International Law [2014] 84(1) 187–239 https://doi.org/10.1093/bybil/bru003.

28. Musiani F, 'Reassessing "infrastructuring digital sovereignty": digital self-determination as a set of infrastructure-embedded practices' [2025] 10 Frontiers in Sociology https://doi.org/10.3389/fcomm.2025.1562072.

29. Pierucci F, 'Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace' [2025] 4 Digital Society 29 https://doi.org/10.1007/s44206-025-00189-4.

30. Torichnyi V, Biletska T, Rybshchun O, Kupriyenko D, Ivashkov Y, Bratko A, 'Information and propaganda component of the Russian Federation hybrid aggression: conclusions for developed democratic countries on the experience of Ukraine' [2021] 25(3) Trames 357 https://doi.org/10.3176/tr.2021.3.06.

31. Yilma K, 'Reimagining digital constitutionalism' [2026] 15(1) Global Constitutionalism 66 https://doi.org/10.1017/S2045381725100014.

32. Butkevych O, 'Suchasne mizhnarodne pravo: prodovzhennia «kholodnoi viiny» chy pochatok novoi epokhy?', V Repetskyi, V Hutnyk (red), *Suchasni problemy mizhnarodnoho prava. Liber Amicorum do 60-richchia prof. M. V. Buromenskoho* (Feniks 2017) (in Ukrainian).

33. Danylian O, Dzoban O, Liudyna v informatsiinomu suspilstvi: problema moralnoi identyfikatsii [2019] 1(40) Visnyk NIuU imeni Yaroslava Mudroho. Seriia: Filosofiia, filosofiia prava, politolohiia, sotsiolohiia 10 https://doi.org/10.21564/2075-7190.40.155746 (in Ukrainian).

34. Fediuk V, Informatsiina bezpeka ta informatsiinyi suverenitet yak obiekty kryminalno-pravovoi okhorony (na prykladi st. 111 Kryminalnoho kodeksu Ukrainy) [2024] 12(54) Naukovi perspektyvy 1385 https://doi.org/10.52058/2708-7530-2024-12(54)-1380-1391 (in Ukrainian).

35. Ismailov K, Bielykh D, Informatsiinyi suverenitet i Doktryna informatsiinoi bezpeky Ukrainy [2019] 1 Porivnialno-analitychne pravo 206–209 (in Ukrainian).

36. Kutsepal S, Informatsiinyi suverenitet ta informatsiina bezpeka Ukrainy: vyklyky ta realii viiny [2023] 1 Poltavskyi pravovyi chasopys 78–88 https://doi.org/10.21564/2786-7811.1.290476 (in Ukrainian).

37. Manuilov Ye, Kalynovskyi Yu, Aksiolohichnyi vymir informatsiinoi bezpeky ukrainskoi derzhavy [2017] 3 Visnyk Natsionalnoho universytetu "Iurydychna akademiia Ukrainy imeni Yaroslava Mudroho". Seriia: Filosofiia, filosofiia prava, politolohiia, sotsiolohiia 17 (in Ukrainian).

38. Manuilov Ye, Kalynovskyi Yu, Informatsiinyi suverenitet Ukrainy: suchasni vyklyky ta zahrozy dukhovnii sferi [2019] 3(42) Visnyk NIuU imeni Yaroslava Mudroho. Seriia: Filosofiia, filosofiia prava, politolohiia, sotsiolohiia 32 (in Ukrainian).

39. Radutnyi O, Iliuziia ta realnist informatsiinoho suverenitetu [2020] 4(35) Informatsiia i pravo 24 https://doi.org/10.37750/2616-6798.2020.4(35).221215 (in Ukrainian).

40. Solodka O, Zabezpechennia informatsiinoho suverenitetu derzhavy: pravovyi dyskurs [2020] 1(32) Informatsiia i pravo 85 https://doi.org/10.37750/2616-6798.2020.1(32).200311 (in Ukrainian).

41. Ternavska V, Kontseptsiia derzhavnoho suverenitetu v aspekti hlobalnoho informatsiinoho prostoru [2021] 4(39) Informatsiia i pravo 85 https://doi.org/10.37750/2616-6798.2021.4(39).248794 (in Ukrainian).

42. Yarema O, Zmist informatsiinoho suverenitetu u konteksti derzhavnoho suverenitetu [2022] 3 Yurydychnyi naukovyi elektronnyi zhurnal 191 https://doi.org/10.32782/2524-0374/2022-3/43 (in Ukrainian).

Theses

43. Danilian V, Informatsiine suspilstvo ta perspektyvy yoho rozvytku v Ukraini (sotsialno-filosofskyi analiz) (dys kand filosof nauk, 2006) (in Ukrainian).

Conference papers

44. Bradov V, Informatsiinyi suverenitet derzhavy: hlobalizatsiinyi aspekt, *International scientific and practical conference "The European development trends in journalism, PR, media and communication" (Wloclawek, Republic of Poland, October 30–31, 2020)* (Baltija Publishing 2020) (in Ukrainian).

45. Liulko S, Suniehin S, 'Informatsiinyi suverenitet derzhavy: sutnisni kharakterystyky', *VIII International Scientific and Practical Conference "Education and science of today: intersectoral issues and development of sciences" (May 9, 2025, Cambridge, UK)* 180–181 https://doi.org/10.36074/logos-09.05.2025.034 (in Ukrainian).

Websites

46. Weber A, Reith S, Kasper M et al., *Sovereignty in Information Technology: Security, Safety and Fair Market Access by Openness and Control of the Supply Chain* (KIT-ITAS 2018) <https://www.itas.kit.edu/english/2018_009.php> (accessed 27.04.2026).

Maryna Chekh

INFORMATION SOVEREIGNTY IN THE DIGITAL AGE: THE TRANSFORMATION OF STATEHOOD AND THE MODEL OF "SOVEREIGNTY AS RESPONSIBILITY"

Abstract. Digitalization and the development of artificial intelligence are transforming the classical model of territorial sovereignty. The transboundary nature of cyberspace creates a gap between states' aspirations to control the national information domain and the decentralized logic of data flows. For Ukraine, this challenge is intensified under conditions of Russia's hybrid aggression, where information operations are aimed at undermining statehood and identity.

The purpose of the article is to provide a sociophilosophical and legal substantiation of a conceptual model of Ukraine's informational sovereignty as an adaptivehybrid system, grounded in the principle of "sovereignty as responsibility" and compatible with human rights standards.

The study demonstrates the evolution of informational sovereignty from a model of exclusive control to an approach in which the state acts as guarantor of citizens' digital dignity and mental integrity. It substantiates the necessity of legal protection of identity against informational violence and proposes the regulation of jurisdictional conflicts through mechanisms of "digital federalism" and the integration of ethical principles into the design of information systems.

The article develops an adaptivehybrid model of informational sovereignty that combines technological resilience, jurisdictional regulation of crossborder flows, and axiological protection of dignity and human rights. The Ukrainian experience illustrates the distributed nature of such sovereignty, where citizens become active subjects of information security through the cultivation of critical thinking and media resilience.

Keywords: informational sovereignty; digital sovereignty; hybrid warfare; international law; human rights.