

Микита Володимирович Мязін

аспірант кафедри теоретичної і практичної філософії професора Й. Б. Шада
Харківського національного університету імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
<https://orcid.org/0009-0003-4901-8789>

ЦИФРОВА ВИДИМІСТЬ ТА ПРИВАТНІСТЬ У СУЧАСНОМУ МІСТІ

У представленому дослідженні здійснюється ґрунтовний епістемологічний аналіз феномену тотальної цифрової видимості (total digital visibility) в контексті сучасної урбаністичної парадигми та його імплікацій щодо приватності й суб'єктної автономії міських резидентів. Актуальність проблематики детермінована експоненційною акселерацією цифрової трансформації урбаністичних агломерацій, що супроводжується імплементацією технологій панконтинуального моніторингу, холистичного аналізу великих даних та інтегральної інфраструктури «розумного міста» (smart city). Означені процеси конституують безпрецедентні режими соціотехнічного контролю, де перцептивні, локомоційні та соціальні патерни мешканців підлягають мультимодальній фіксації через гібридні системи сенсорів, відеоаналітики, мобільних інтерфейсів та алгоритмів машинного навчання. Застосовуючи мультиметодологічний підхід, автор експлікує генезу концепту «цифрової видимості» (digital visibility) у інтердисциплінарному полі, простежуючи його семантичні кореляції із соціологією спостереження (surveillance studies) у працях David Lyon та Zygmunt Bauman, критичною аналітикою капіталізму нагляду (surveillance capitalism) у дослідженнях Shoshana Zuboff, експлорацією алгоритмічної суверенності у роботах Taina Bucher та урбаністичними метаморфозами в інтерпретації Rob Kitchin й Sharon Zukin. Особливу аналітичну увагу приділено архітектоніці цифрового спостереження в урбаністичному просторі, що трансформує резидентів у «данізованих суб'єктів» (datafied citizens), позбавлених епістемічного суверенітету над власними даними. У результаті систематизації емпіричних та теоретичних даних виокремлено тріаду фундаментальних загроз приватності в умовах цифрової урбанізації: алгоритмічну редукацію приватності, асиметрію видимості та формування «поведінкового надлишку». Екстраполюючи проблематику на український контекст, автор демонструє дискрепанцію між темпами цифровізації міст та рівнем нормативно-правової регуляції й кібер-освіченості громадян. На основі критичного аналізу робіт вітчизняних дослідників аргументується необхідність конструювання етики цифрової присутності як гібридної нормативної матриці, що інтегрує легальні механізми захисту даних із гуманістичними принципами інтерсуб'єктивної взаємодії у цифровому континуумі. Компаративний аналіз завершується формулюванням тріади аксіологічних принципів цифрової урбаністики: транспарентності алгоритмів, права на цифрову інвизибільність та розвитку цифрової грамотності. Дослідження створює нові епістемологічні перспективи для трансдисциплінарного дискурсу на стику філософської антропології, соціальної теорії, урбаністики та digital studies.

Ключові слова: **цифрова видимість, приватність, розумне місто, капіталізм нагляду, етика даних, цифрова урбаністика.**

Як цитувати: Мязін, М., (2025). Цифрова видимість та приватність у сучасному місті. *Вісник Харківського національного університету імені В.Н. Каразіна, серія «Теорія культури і філософія науки»*, (71), 33-41. <https://doi.org/10.26565/2306-6687-2025-71-04>

In cites: Miazin, M., (2025). Digital visibility and privacy in contemporary urban space. *The Journal of V. N. Karazin Kharkiv National University, Series Theory of Culture and Philosophy of Science*, (71), 33- 41. <https://doi.org/10.26565/2306-6687-2025-71-04> [In Ukrainian]

Актуальність дослідження зумовлена стрімким зростанням процесів цифрової трансформації сучасних міст, що супроводжується впровадженням систем моніторингу, аналітики великих даних та інфраструктури «розумного міста». Ці зміни призводять до формування феномену тотальної цифрової видимості (total digital visibility), що передбачає всепроникне спостереження за діями, переміщенням і поведінкою мешканців через мережу сенсорів, камер, мобільних пристроїв, соціальних мереж і систем штучного інтелекту.

В українському контексті питання приватності та захисту персональних даних у цифровому міському середовищі набуває особливої гостроти через активні процеси цифровізації при недостатньому розвитку відповідних правових механізмів та низькій обізнаності громадян щодо кібербезпеки. Існує нагальна потреба в комплексному дослідженні антропологічних аспектів цифрової тотальності та розробці етики цифрової присутності, яка враховувала б автономію суб'єкта, його право на приватність та відповідальну взаємодію в цифровому просторі.

Мета дослідження полягає в аналізі феномену тотальної цифрової видимості в сучасному місті та визначенні її впливу на приватність і автономію міських мешканців, а також у розробці концептуальних засад етики цифрової присутності як нормативної рамки, що орієнтується на гуманістичні цінності у взаємодії з цифровим середовищем міста.

Завдання дослідження: 1) Проаналізувати еволюцію поняття «цифрова видимість» (digital visibility) у міждисциплінарному контексті, зокрема в соціології спостереження, критиці цифрового капіталізму, дослідженнях алгоритмів і медіа та урбаністиці. 2) Дослідити трансформацію архітектури спостереження в цифровому місті та її вплив на формування парадигми «datafied citizen» (громадянина, перетвореного на дані). 3) Визначити основні загрози приватності, що виникають у процесі цифрової урбанізації, зокрема алгоритмічну редукцію приватності та асиметрію видимості. 4) Проаналізувати сучасний стан правового забезпечення захисту персональних даних в умовах цифровізації українських міст. 5) Обґрунтувати необхідність розробки етики цифрової присутності як нормативної рамки взаємодії в цифровому просторі міста. 6) Сформулювати ключові принципи етики цифрової урбаністики, спрямовані на збереження людської гідності та автономії в умовах тотальної цифрової видимості.

Об'єктом дослідження є процеси цифрової трансформації сучасних міст та пов'язані з ними системи моніторингу й спостереження, що формують режим тотальної цифрової видимості.

Предметом дослідження є вплив тотальної цифрової видимості на приватність та автономію міських мешканців, а також етичні аспекти взаємодії людини з цифровим середовищем міста.

Цифрова трансформація сучасних міст супроводжується впровадженням систем моніторингу, аналітики великих даних та інфраструктури «розумного міста», що значно змінює режим видимості в міському середовищі. Цей процес отримав назву тотальної цифрової видимості (total digital visibility), що означає всепроникне спостереження за діями, переміщенням і поведінкою мешканців через мережу сенсорів, камер, мобільних пристроїв, соціальних мереж і систем штучного інтелекту. Розглядаючи ключові дослідження, які фокусуються на приватності як соціальному та політичному виклику цифрової урбанізації, з поля зору експертів часто зникає антропологічний аспект процесу цифрової тотальності. У добу цифрової урбанізації, де міські простори дедалі більше пронизані сенсорними мережами, системами відеонагляду, алгоритмами розпізнавання облич та аналітикою поведінкових даних, постає критичне питання: якою мірою зростаюча тотальна видимість мешканців міста загрожує їхній приватності?

Звернімося до визначення поняття «цифрова видимість». Поняття «цифрова видимість» (digital visibility) не має однозначного авторства, як, наприклад, класичні теоретичні концепти, і не закріплено за якимось одним ученим чи датою. Воно виникло як частина ширшої дискусії про цифровий контроль, спостереження, прозорість і дані, особливо в контексті цифрових технологій, соціальних мереж, «розумних» міст та великих даних. Спершу воно з'явилося у контексті практичного застосування систем відеонагляду ще наприкінці 1980-х. Це свого часу викликало дебати про прозорість і спостереження (surveillance studies), де обговорювались не тільки технічні та правові аспекти, але й соціальні та психологічні.

Девід Лайон, провідний дослідник у сфері соціології спостереження, використовує терміни, пов'язані з «видимістю» в цифровому середовищі у книзі «Суспільство спостереження: моніторинг повсякденного життя» (Surveillance Society: Monitoring Everyday Life) [Lyon, 2001], яка вважається класичною працею, де цифрова видимість трактується як наслідок збирання даних у повсякденному житті. Дослідник аналізує, як цифрові системи «виводять» суб'єктів у поле видимості. Він описує, як цифрові технології роблять людей «видимими» для держави, корпорацій і один одного. Це змінює патерни поведінки людини, яка відчуває цей тиск спостереження.

Згодом у 2013 році у співавторстві з Зигмундом Бауманом у книжці «Спостереження за

рідиною: розмова» (Liquid Surveillance: A Conversation) [Bauman, Lyon, 2013] Лайон проаналізує ідею нової прозорості й постійної видимості в цифрову епоху. Щодня Google та емітенти кредитних карт відзначають деталі наших звичок, турбот і переваг, тихо підказуючи індивідуальні маркетингові стратегії з нашою активною, надто часто настирливою співпрацею. Сьогодні в світі, де простори можуть бути нефіксованими, а час безмежним, наш вічний рух не залишається непоміченим. Спостереження поширюється неймовірними досі способами, реагуючи на мінливу природу сучасного життя і відтворюючи його, просочуючись в області, де колись воно мало незначний вплив. В суспільстві все частіше використовуються нові форми цифрової прозорості, де кожен стає водночас спостерігачем і спостережуваним. Цифрова прозорість перетворюється в цих умовах на тотальний принцип глобалізованого суспільства. Розвиток такої позиції можна простежити і в концепції цифрової видимості у контексті міського середовища. У сфері урбаністики та медіа, поняття цифрової видимості часто фігурує в дослідженнях міських медіа-інфраструктур, смарт-технологій, цифрової ідентичності та даних. Зокрема, у працях американської дослідниці та соціального психолога Шошани Зубофф (Shoshana Zuboff) в роботі «The Age of Surveillance Capitalism» [Zuboff, 2019], де піднімається питання контролю через «видимість» поведінки в цифровому просторі. Авторка пропонує свій аналіз того, як технологічні гіганти створюють «тотальну видимість» для монетизації поведінки користувачів. Фактично, мова йде не просто про спостереження і захист, а контроль за людиною, який не завжди може бути використано на її благо. Цифровий тоталітаризм переходить межі фантастики і стає побутовим явищем сучасного суспільства.

Digital Visibility перетворюється на культурний та соціальний конструкт для позначення того, як тіла, ідентичності або поведінка стають помітними або непомітними в цифровому просторі. На це звертає увагу Таїна Бухер [Bucher, 2012], аналізуючи, як алгоритми визначають, хто та що буде «видимим» у соціальних мережах. Як медіа-дослідник, вона використовує digital visibility для позначення механізмів, через які деякі суб'єкти отримують більше цифрової присутності, ніж інші. Авторка досліджує, як алгоритми Facebook визначають, хто стає видимим у стрічці новин — і яким чином це формує цифрову суб'єктивність.

У більш розгорнутому вигляді ці процеси аналізуються Хосе ван Дейк (José van Dijck) в роботі «Культура зв'язку» [Van Dijck, 2013]. Цей переконливий наратив прокладає шлях для аналізу того, що Реймонд Вільямс називав структурою почуття, а саме те, що наша культура значною мірою характеризується зв'язністю. У той час як інші дослідники все ще розглядають соціальні медіа як нові медіа, намагаючись з'ясувати, що в них такого нового, ван Дейк теоретизує зв'язок, який відрізняється від соціальної цінності зв'язку як основної риси нашої культури. В мережі, на відміну від традиційних систем зв'язку, спрацьовують автоматизовані форми з'єднання, які проєктуються та маніпулюються [Van Dijck, 2013, р. 12] і які швидко перетворилися на монетизований дохід [Van Dijck, 2013, р. 4].

Щоб проаналізувати нашу поточну культуру зв'язку, ван Дейк поєднує два напрямки думки. Поєднуючи політекономічну (так само, як і З. Бауман) перспективу з теорією акторської мережі, ван Дейк прагне «розібрати платформи та знову зібрати соціальність» [Van Dijck, 2013, р. 24]. Таким чином, він розробляє складну структуру для аналізу платформ соціальних мереж. Отриманий аналіз платформи складається з шести компонентів – технології, використання/користувача, контенту, власності, управління та бізнес-моделей – і конфігурує складну мережу для аналізу платформ як посередників. У цій аналітичній структурі технологія розуміється як спосіб, у який платформи є постачальниками «програмного забезпечення, (іноді) апаратного забезпечення та послуг, які допомагають кодувати соціальну діяльність у обчислювальну архітектуру» [Van Dijck, 2013, р. 29]. Отже, це питання про те, як технологічна інфраструктура ((мета)дані, алгоритм, протокол, інтерфейс і за замовчуванням) «формує виконання соціальних дій замість того, щоб просто сприяти їм» [Van Dijck, 2013, р. 29].

Другий вимір – використання/користувачі – розглядає взаємодію з платформою та її технологічними особливостями. Тут автор розглядає як приховані, так і явні форми використання, проводячи різницю між запланованим використанням і фактичним присвоєнням. Виміри вмісту відносяться до об'єктів, які виробляються та циркулюють у поєднанні з технологічними досягненнями платформ. Решта три виміри – власність, управління та бізнес-моделі – виведені з точки зору політичної економії та враховують соціально-економічні структури платформ.

Згодом ми зустрінемо ідею інформаційної платформи і в урбаністичних дослідженнях,

де саме місто постане як тотальна інформаційна платформа, яка містить не тільки загальну інформацію, але й те, що стало відомо завдяки системі цифрової видимості. Аналіз «видимості» в соціальних мережах як елементу публічності, ідентичності та контролю стає одним з елементів урбаністичного дослідження, на що звертають увагу урбаністи Шарон Зукін та Філіп Казініц у книзі 2018 року видання «Джентріфікація та майбутнє міст» (*Gentrification and the Future of Cities*) [Zukin, Kasinitz, 2018]. Видимість у дослідженні розглядається як спосіб, яким цифрові інструменти в міському середовищі створюють нові режими «бачення» міста, конструювання його образу та відображення екзистенційного простору і атмосфери.

У дослідженні Аші Крішнан та Лілі Іріані підкреслюється, що сучасне місто є простором безперервного спостереження, де кожна дія — від використання транспортної карти до пересування тротуаром — залишає цифровий слід [Krishnan, Irani, 2014]. Концепт «цифрової видимості» (*digital visibility*) відображає ступінь, у якому цифрові технології фіксують, аналізують і використовують поведінку людей у міському просторі.

Інфраструктура так званих «розумних міст» (*smart city*) перетворює міста на простори паноптичного контролю [Kitchin, 2016]. У цьому контексті цифрова видимість вже не є інструментом безпеки чи ефективності, а радше — механізмом вбудованого контролю. Д. Бойд (Boyd) та К. Кроуфорд (Crawford) наголошують на зсуві у розумінні приватності: від індивідуального вибору до структурної уразливості перед державними та корпоративними системами збору даних [Boyd, Crawford, 2012]. Згідно з згаданим вже дослідженням Д. Лайона, цифрові системи спостереження створюють нові форми нагляду, які більше не обмежуються конкретними об'єктами чи подіями, а функціонують як розсіяна, всюдисуща інфраструктура [Lyon, 2018]. Такий характер спостереження ускладнює контроль над тим, хто, коли і як бачить або використовує наші дані. У цифровому місті не існує стабільної межі між приватним і публічним простором.

Таким чином, поняття «цифрова видимість» виникло як міждисциплінарна метафора і концепт, а не як термін, уведений конкретним автором. Його формування пов'язане з чотирма аспектами: соціологією спостереження (Lyon, Bauman); критикою цифрового капіталізму (Zuboff); дослідженнями алгоритмів і медіа (Bucher, José van Dijck); урбаністикою в контексті даних про міста, цифрові інтерфейси (Zukin, Kasinitz).

Розгляд проблеми «цифрової видимості» підводить нас до розуміння нової парадигми «datafied citizen» (громадянина, перетвореного на дані), що виникає в умовах діджиталізованого міста. Створюється «архітектура спостереження» в цифровому місті не тільки як інфраструктура «розумного міста», але й як форма постпаноптизму [Zuboff, 2019; Kitchin, 2016], де класичні архітектурні моделі нагляду трансформуються в алгоритмічні мережі. Як стверджує Р. Кітчін: «Розумні міста — це не лише інструментальне середовище, але й системи спостереження, які роблять міське життя більш прозорим, зрозумілим і керованим за допомогою даних» [Kitchin, 2016, р. 8]. На відміну від паноптикуму Мішеля Фуко, сучасне цифрове місто створює умови для розсіяного, децентралізованого і невидимого спостереження, що не завжди усвідомлюється мешканцями [Graham, Wood, 2003].

Житель цифрового міста поступово трансформується у «datafied subject» — суб'єкт, чие існування фрагментується у вигляді даних, придатних для аналізу, передбачення та управління [Van Dijck, 2014]. Це створює структурну асиметрію між тими, хто виробляє дані (мешканці міста), і тими, хто має до них доступ (корпорації, держава, платформи). Впровадження технологій розпізнавання обличчя, систем біометричної ідентифікації та аналізу поведінки в публічних просторах є предметом особливої критики. Ці технології, хоч і декларуються як безпекові, можуть спричинити ущільнення контролю та зміну характеру публічності в місті [Harvey, 2020; Vanolo, 2014].

Отже, цифрова урбаністика створює асиметрію видимості, коли громадяни дедалі більше піддаються нагляду, водночас як алгоритми, власники платформ і муніципальні контракти залишаються закритими до публічного огляду [Pasquale, 2015]. Це породжує кризу довіри і нові форми політичного спротиву — від криптоактивізму до «аналогових бунтів» проти камер спостереження.

Як наслідок, відбувається не лише підриг приватності, але й втрата автономії у процесі самопрезентації. Однією з головних загроз, які вирізняються в літературі, є алгоритмічна редукція приватності, коли приватна інформація не просто збирається, але й обробляється алгоритмами, які формують припущення, категорії та профілі для індивідів [Eubanks, 2018]. У міському контексті це проявляється в цифрових паспортах, системах соціального кредиту (як у

Китаї), персоналізованій рекламі або в управлінні мобільністю.

Загроза приватності в цифровому місті — не лише технічна чи етична дилема, а радше соціальна проблема, що стосується розподілу влади, довіри та участі громадян. Як зазначає американська соціальна психологиня Ш. Зубофф, цифрове місто часто функціонує у логіці поведінкового надлишку («behavioural surplus» — надлишок поведінкових даних), де всі форми людської активності перетворюються на товар [Zuboff, 2019]. Цей феномен отримав нове теоретичне осмислення у працях Ш. Зубофф, яка описала «капіталізм нагляду» — економіку, що базується на монетизації людської поведінки через аналіз даних [Zuboff, 2019]. Цифрова видимість у такому вимірі стає інструментом не лише соціального, а й ринкового контролю.

За Ж. Делезом (Deleuze), ми вступаємо в добу «суспільств контролю», де влада діє не через інститути, а через цифрові середовища, що формують поведінку індивіда [Deleuze, 1992]. У філософському аспекті тотальна видимість трансформує уявлення про суб'єкта, оскільки цифрове середовище продукує «прозору людину», яка втрачає глибину й автономність через постійну вимогу до самопрезентації [Nap, 2012]. Цей суб'єкт існує в логіці візуальної експозиції, а не в межах внутрішнього, приватного буття. У такому суспільстві цифрова видимість стає простором нових ієрархій, що поглиблюють соціальну фрагментацію [Кисельов, 2021, с. 139–141].

Таким чином, цифрова тотальна видимість у місті є результатом інтеграції технологій у публічний простір, яка загрожує фундаментальним принципам приватності та автономії особи. Вона формує нові архітектури нагляду, що діють не лише як технічні, але й соціальні та культурні структури. В умовах цифрової урбанізації важливо поставити під сумнів нейтральність технологій та вимагати прозорості, відповідальності і права на анонімність у публічному просторі.

У контексті цифрової трансформації українських міст питання приватності та захисту персональних даних набувають особливої актуальності. Слід відмітити, що правовий аспект проблеми цифрової тотальної видимості у місті набув найбільш активного обговорення в українському науковому товаристві.

Так, Олег Гиляка у своїй статті «Право на приватність та захист персональних даних в умовах цифровізації» [Hylyaka, 2022] підкреслює, що збереження персональних даних на цифрових платформах робить їх потенційною мішенню для шахраїв та злочинців. Він наголошує на необхідності оновлення законодавства та впровадження сучасних механізмів захисту для забезпечення безпеки персональних даних громадян. Слід зазначити, що в українських розвідках проблеми цифровізації міста правовий аспект переважає. На що вказує і В.М. Брижка у роботі «Приватність даних у хмарних технологіях» [Bryzhko, 2021]. Автор аналізує проблеми, пов'язані із захистом персональних даних у контексті використання хмарних сервісів. Він пропонує впровадження в Україні інституту права приватної власності на персональні дані як засобу підвищення рівня їхнього захисту.

А.Г. Бірюкова та Г.В. Колісникова [Biryukova, Kolisnykova, 2023] розглядають цивільно-правові аспекти цифрової конфіденційності в Україні. Вони аналізують нормативно-правову базу, що регулює захист персональних даних, та підкреслюють важливість оптимізації законодавства для забезпечення балансу між правом на приватність і потребами державної безпеки та економічного розвитку.

Тема інформаційної безпеки продовжується у спільній праці В.Г. Пилипчука та В.М. Брижка «Інформаційна безпека та приватність у сфері захисту персональних даних» [Pylypchuk, Bryzhko, 2020], де розглядаються питання правового забезпечення інформаційної безпеки та приватності. Автори акцентують увагу на необхідності вдосконалення законодавства для ефективного захисту персональних даних в умовах цифровізації.

Такої ж позиції дотримується і В.В. Аніщук в статті «Захист персональних даних у кіберпросторі» [Anishchuk, 2022], де висвітлюються типові загрози, з якими стикається користувач у віртуальному просторі, а також пропонуються шляхи вдосконалення національної політики з кібербезпеки.

У свою чергу це питання розглядає Р.А. Пристай [Prystay, 2021] в межах концепції «приватності за замовчуванням» та пропонує користувацьку модель даних як основу захисту приватності та персональних даних у соціальних мережах. Автор аналізує підходи до забезпечення конфіденційності у цифрових сервісах та соціальних мережах, зокрема через запровадження механізмів «privacy by default». Дослідник акцентує увагу на необхідності впровадження механізмів, що забезпечують автоматичний захист даних користувачів без

потреби в додаткових налаштуваннях.

У сучасних українських містах процеси цифровізації набирають обертів, що сприяє підвищенню ефективності управління міськими ресурсами та покращенню якості життя громадян. Слід зауважити, що проблема цифровізації міста викликає не тільки науковий, але й практичний інтерес. Так, Міністерство цифрової трансформації України спільно з Інститутом Маліка (Швейцарія) дослідили фактори розвитку Smart City в Україні. Метою було зрозуміти, як швидко та ефективно перетворити великі міста на «розумні». Дослідження підкреслює важливість врахування аспектів приватності та безпеки даних при впровадженні технологій Smart City.

Таким чином, українські дослідження підтверджують, що цифрова трансформація міст супроводжується значними викликами у сфері приватності та захисту персональних даних. Низький рівень обізнаності громадян щодо кібербезпеки та недостатня правова база підкреслюють необхідність комплексного підходу до вирішення цих питань. Впровадження інноваційних технологій у міське середовище має супроводжуватися розробкою та впровадженням ефективних механізмів захисту приватності, а також підвищенням рівня цифрової грамотності населення. Українські дослідники також акцентують увагу на необхідності підвищення обізнаності громадян щодо ризиків, пов'язаних із цифровою видимістю, та розробки ефективних механізмів захисту в цифровому середовищі.

У цьому контексті виникає потреба в етиці цифрової присутності — новій нормативній рамці, що орієнтується на гуманістичні цінності у взаємодії з цифровим середовищем міста. Йдеться не лише про правові регуляції чи технічний захист даних, а про культуру відповідальної взаємодії в цифровому просторі, яка враховує автономію суб'єкта, його право на невидимість, мовчання, помилку. Етика цифрової присутності має сприяти формуванню критичного ставлення до цифрових практик, розвитку цифрової емпатії та усвідомленому співіснуванню в урбанізованому світі, де кордони між технічним і людським дедалі більше розмиваються.

Висновки. Сучасна урбаністика дедалі більше визначається цифровими технологіями, які змінюють функціональність та соціокультурну динаміку міста. У цьому контексті концепція «цифрового міста» (як Smart city) фокусується не лише на підвищенні ефективності міського управління, але й на трансформації способів життя, форм взаємодії та ідентичності мешканців [Batty et al., 2012; Townsend, 2013]. Зрештою, місто перетворюється на складну інформаційну екосистему, де потоки даних стають таким самим базовим ресурсом, як інфраструктура чи енергетика.

Одним із ключових наслідків цифрової трансформації міського середовища є зростання цифрової видимості. Мешканці сучасних міст постійно продукують цифрові сліди — через смартфони, камери спостереження, сенсори, банківські та навігаційні системи. Усе це формує ситуацію тотального нагляду, яку Д. Лайон описує як «суспільство спостереження» [Lyон, 2003].

Видимість, що зумовлюється цифровою інфраструктурою, часто позиціонується як позитив — механізм забезпечення безпеки, комфорту, прозорості. Проте водночас вона спричиняє ерозію особистого простору, формує нові механізми самоконтролю та дисциплінування.

Розвиток цифрової урбаністики є неоднозначним процесом: з одного боку, він відкриває нові можливості для покращення життя у місті, з іншого — породжує радикальні виклики для автономії індивіда. Тотальна цифрова видимість демонструє, наскільки технологічний прогрес може втручатися в онтологію суб'єкта, порушуючи баланс між відкритістю та захищеністю, між участю та контролем.

Отже, постає нагальна потреба формування етики цифрової урбаністики, яка має ґрунтуватися на принципах прозорості алгоритмів, права на приватність, критичної цифрової грамотності та публічного контролю над обігом даних [Kitchin, Dodge, 2011]. Така етика повинна бути не лише техніко-юридичною, а й філософсько-антропологічною, зосередженою на збереженні людської гідності у цифровому просторі міста..

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Анішук В. В. (2022). Захист персональних даних у кіберпросторі. *Правова інформатика*, 73(1), 44-52.
2. Бірюкова А. Г., Колісникова Г. В. (2023). Цивільно-правові аспекти цифрової

конфіденційності в Україні. Вісник НУЛП, серія "Юридичні науки", 10(2), 54-63.

3. Брижко В. М. (2021). Приватність даних у хмарних технологіях. Інформація і право, 37(2), 80-95.
4. Гиляка О. (2022). Право на приватність та захист персональних даних в умовах цифровізації. Право та інновації, 28(2), 78-89.
5. Кисельов, О. С. (2021) Цифрова трансформація публічного простору та її соціальні наслідки. Соціальна філософія. № 15 (2). С. 136–148.
6. Міністерство цифрової трансформації України, Інститут Маліка (2023). Дослідження факторів розвитку Smart City в Україні. Київ: Мінцифра. Доступно за посиланням: <https://thedigital.gov.ua/regions/news/prezentatsiya-doslidzhennya-institutu-malika-pro-rozvitok-smart-city-v-ukraini>
7. Пилипчук В. Г., Брижко В. М. (2020). Інформаційна безпека та приватність у сфері захисту персональних даних. Інформація і право, 33(2), 86-103.
8. Пристай Р. А. (2021). Приватність за замовчуванням: користувацька модель даних як основа захисту приватності та персональних даних у соціальних мережах. Інформаційне право, 14(3), 112-124.
9. Batti, M., Axhausen, K., Giannattasio, F. et al. (2012) Smart cities of the future. European Physical Journal. Vol. 214. P. 481–518.
10. Bauman, Z., & Lyon, D. (2013) Liquid Surveillance: A Conversation. Cambridge: Polity Press. 180 p.
11. Boyd, D., & Crawford, K. (2012) Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. Information, Communication & Society. Vol. 15, No. 5. P. 662–679.
12. Bucher, T. (2012) Want to be on the top? Algorithmic power and the threat of invisibility on Facebook. New Media & Society. Vol. 14, No. 7. P. 1164–1180.
13. Deleuze, G. (1992) Postscript on the Societies of Control. October. No. 59. P. 3–7.
14. Eubanks, V. (2018) Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. New York: St. Martin's Press. 288 p.
15. Graham, S., & Wood, D. (2003) Digitizing surveillance: categorization, space, inequality. Critical Social Policy. Vol. 23, No. 2. P. 227–248.
16. Han, B.-C. (2012) The Transparency Society. Stanford: Stanford University Press. 120 p.
17. Harvey, D. (2020) The Right to the City. New Left Review. No. 53. P. 23–40.
18. Kitchin, R. (2016) The ethics of smart cities and urban science. Philosophical Transactions of the Royal Society A. Vol. 374, No. 2083. P. 20160115.
19. Kitchin, R., & Dodge, M. (2011) Code/Space: Software and Everyday Life. Cambridge: MIT Press. 320 p.
20. Krishnan, A., & Irani, L. (2014) Social visibility in digital cities. Digital Cities. Vol. 12, No. 1. P. 87–102.
21. Lyon, D. (2003) Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination. London: Routledge. 210 p.
22. Lyon, D. (2001) Surveillance Society: Monitoring Everyday Life. Milton Keynes: Open University Press. 240 p.
23. Lyon, D. (2018) The Culture of Surveillance: Watching as a Way of Life. Cambridge: Polity Press. 200 p.
24. Pasquale, F. (2015) The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge: Harvard University Press. 320 p.
25. Townsend, A. M. (2013) Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia. New York: W. W. Norton & Company. 400 p.
26. Van Dijck, J. (2014) Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. Surveillance & Society. Vol. 12, No. 2. P. 197–208.
27. Van Dijck, J. (2013) The Culture of Connectivity: A Critical History of Social Media. Oxford: Oxford University Press. 250 p.

28. Vanolo, A. (2014) Smartmentality: The Smart City as Disciplinary Strategy. *Urban Studies*. Vol. 51, No. 5. P. 883–898.

29. Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books. 450 p.

30. Zukin, S., Kasinitz, P. (2018) *Gentrification and the Future of Cities*. London: Routledge. 280 p.

Стаття надійшла до редакції 01.04.2025

Стаття рекомендована до друку 21.05.2025

Mykyta V. Miazin, PhD Student of the Department of Theoretical and Practical Philosophy named after Professor Y. B. Shad, V. N. Karazin Kharkiv National University, Svobody sq. 4, Kharkiv, 61022, Ukraine, <https://orcid.org/0009-0003-4901-8789>

DIGITAL VISIBILITY AND PRIVACY IN CONTEMPORARY URBAN SPACES

The presented research conducts a thorough epistemological analysis of the total digital visibility phenomenon in the context of the modern urban paradigm and its implications for privacy and subjective autonomy of urban residents. The relevance of this problematic is determined by the exponential acceleration of digital transformation in urban agglomerations, accompanied by the implementation of pan-continual monitoring technologies, holistic big data analytics, and integrated smart city infrastructure. These processes constitute unprecedented regimes of socio-technical control, where perceptive, locomotor, and social patterns of residents are subject to multimodal fixation through hybrid systems of sensors, video analytics, mobile interfaces, and machine learning algorithms.

Applying a multi-methodological approach, the author explicates the genesis of the "digital visibility" concept in the interdisciplinary field, tracing its semantic correlations with surveillance studies in the works of David Lyon and Zygmunt Bauman, critical analytics of surveillance capitalism in Shoshana Zuboff's research, exploration of algorithmic sovereignty in Taina Bucher's works, and urban metamorphoses in the interpretation of Rob Kitchin and Sharon Zukin. Special analytical attention is paid to the architectonics of digital surveillance in urban space, which transforms residents into "datafied citizens" deprived of epistemic sovereignty over their own data.

Through systematization of empirical and theoretical data, a triad of fundamental privacy threats in the conditions of digital urbanization is identified: algorithmic reduction of privacy, asymmetry of visibility, and formation of "behavioral surplus." Extrapolating these issues to the Ukrainian context, the author demonstrates the discrepancy between the pace of urban digitalization and the level of regulatory framework and cyber literacy of citizens. Based on a critical analysis of domestic researchers' works, the necessity of constructing a digital presence ethics as a hybrid normative matrix is argued, integrating legal mechanisms of data protection with humanistic principles of intersubjective interaction in the digital continuum.

The comparative analysis concludes with the formulation of a triad of axiological principles for digital urban studies: algorithmic transparency, the right to digital invisibility, and the development of digital literacy. The research creates new epistemological perspectives for transdisciplinary discourse at the intersection of philosophical anthropology, social theory, urban studies, and digital studies.

Keywords: **digital visibility, privacy, smart city, surveillance capitalism, data ethics, digital urban studies.**

REFERENCES

1. Anishchuk, V. V. (2022). Protection of personal data in cyberspace. *Legal Informatics*, 73(1), 44–52. (in Ukraine)
2. Biryukova, A. H., & Kolisnykova, H. V. (2023). Civil-Law Aspects of Digital Privacy in Ukraine. *Bulletin of NULP, Series "Legal Sciences"*, 10(2), 54–63. (in Ukraine)
3. Bryzhko, V. M. (2021). Data Privacy in Cloud Technologies. *Information and Law*, 37(2), 80–95. (in Ukraine)
4. Hiliaka, O. (2022). The Right to Privacy and Protection of Personal Data in the Context of Digitalization. *Law and Innovations*, 28(2), 78–89. (in Ukraine)
5. Kyselov, O. S. Tsyfrova transformatsiia publichnoho prostoru ta yii sotsialni naslidky [Digital transformation of public space and its social consequences]. *Sotsialna filosofiia*. 2021. No. 15 (2). P. 136–148. (In Ukrainian)
6. Ministry of Digital Transformation of Ukraine, Malik Institute. (2023). *Research on the Development Factors of Smart Cities in Ukraine*. Kyiv: Ministry of Digital Transformation. Available

at: <https://thedigital.gov.ua/regions/news/prezentatsiya-doslidzhennya-institutu-malika-pro-rozvitok-smart-city-v-ukraini> (in Ukraine)

7. Pylypchuk, V. H., & Bryzhko, V. M. (2020). Information Security and Privacy in the Field of Personal Data Protection. *Information and Law*, 33(2), 86–103. (in Ukraine)
8. Prystai, R. A. (2021). Privacy by Default: The User Data Model as a Basis for Privacy and Personal Data Protection in Social Networks. *Information Law*, 14(3), 112–124. (in Ukraine)
9. Batti, M., Axhausen, K., Giannattasio, F. et al. (2012) Smart cities of the future. *European Physical Journal*. Vol. 214. P. 481–518.
10. Bauman, Z., & Lyon, D. (2013) *Liquid Surveillance: A Conversation*. Cambridge: Polity Press. 180 p.
11. Boyd, D., & Crawford, K. (2012) Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society*. Vol. 15, No. 5. P. 662–679.
12. Bucher, T. (2012) Want to be on the top? Algorithmic power and the threat of invisibility on Facebook. *New Media & Society*. Vol. 14, No. 7. P. 1164–1180.
13. Deleuze, G. (1992) Postscript on the Societies of Control. *October*. No. 59. P. 3–7.
14. Eubanks, V. (2018) *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press. 288 p.
15. Graham, S., & Wood, D. (2003) Digitizing surveillance: categorization, space, inequality. *Critical Social Policy*. Vol. 23, No. 2. P. 227–248.
16. Han, B.-C. (2012) *The Transparency Society*. Stanford: Stanford University Press. 120 p.
17. Harvey, D. (2020) The Right to the City. *New Left Review*. No. 53. P. 23–40.
18. Kitchin, R. (2016) The ethics of smart cities and urban science. *Philosophical Transactions of the Royal Society A*. Vol. 374, No. 2083. P. 20160115.
19. Kitchin, R., & Dodge, M. (2011) *Code/Space: Software and Everyday Life*. Cambridge: MIT Press. 320 p.
20. Krishnan, A., Irani, L. (2014) Social visibility in digital cities. *Digital Cities*. Vol. 12, No. 1. P. 87–102.
21. Lyon, D. (2003) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London: Routledge. 210 p.
22. Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life*. Milton Keynes: Open University Press. 240 p.
23. Lyon, D. (2018) *The Culture of Surveillance: Watching as a Way of Life*. Cambridge: Polity Press. 200 p.
24. Pasquale, F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press. 320 p.
25. Townsend, A. M. (2013) *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia*. New York: W. W. Norton & Company. 400 p.
26. Van Dijck, J. (2014) Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*. Vol. 12, No. 2. P. 197–208.
27. Van Dijck, J. (2013) *The Culture of Connectivity: A Critical History of Social Media*. Oxford: Oxford University Press. 250 p.
28. Vanolo, A. (2014) Smartmentality: The Smart City as Disciplinary Strategy. *Urban Studies*. Vol. 51, No. 5. P. 883–898.
29. Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books. 450 p.
30. Zukin, S., Kasinitz, P. (2018) *Gentrification and the Future of Cities*. London: Routledge. 280 p.

The article was received by the editors 01.04.2025

The article is recommended for printing 21.05.2025