

Сокоринський Володимир Олегович

«Цифровий Паноптикум» як метод розповсюдження цифрового тоталітаризму та загроза сучасним міжнародним відносинам

УДК 321.8

DOI <https://doi.org/10.24195/2414-9616.2024-2.17>

Сокоринський Володимир Олегович
аспірант факультету міжнародних відносин, політології та соціології
Одеського національного університету імені І. І. Мечникова
вул. Дворянська, 2, Одеса, Україна
ORCID: 0009-0006-1676-5173

У статті розглядається поняття цифрового паноптикуму, як метод розповсюдження цифрового тоталітаризму, який розповсюджуються в еру електронних режимів. Доведено, що цифровий паноптикум є актуальним предметом досліджень для сучасної політологічної науки. Цифровий паноптикум є проявом неконтрольованого та невпинного розвитку інформаційно-технологічних систем сьогодення. Через неконтрольований розвиток ІТ технологій, постає проблема загрози міжнародним відносинам серед головних акторів та суб'єктів міжнародної арени. У статті наводиться історичний опис ідеї Паноптикуму від винаходу до сьогодення. Цей паноптикум відображає необхідність збалансованого підходу до захисту прав та свобод громадян у контексті швидкого розвитку технологій. За допомогою цифрових технологій, особливо соціальних мереж, інтернету та систем зчитування геоданих, суспільство знаходиться під постійним наглядом та контролем. Це викликає питання щодо приватності, соціальної динаміки та особистих свобод. Цифровий Паноптикум є реальним інструментом, який неминуче впливає на сучасне громадянське суспільство. Його розвиток безконтрольний та непередбачуваний, що породжує важливі питання для урядів, держав та громадян. Ця ситуація вимагає уважного розгляду та збалансованого підходу до використання цифрових технологій з метою забезпечення захисту основних прав людини. У цьому контексті особливу увагу слід приділяти розробці та дотриманню етичних і правових норм, що регулюють використання цифрових технологій. Правові рамки повинні гарантувати захист приватності, індивідуальної автономії та конфіденційності громадян. Загальнодоступний рівень усвідомлення цих проблем наразі є недостатнім, тому важливо активізувати дослідження та розгляд цифрового тоталітаризму як загрози сучасному цифровому суспільству. Налагодження балансу між технологічними можливостями та захистом особистих прав і свобод є важливим завданням науковців, правозахисників і суспільства в цілому. У майбутньому, успішний розвиток цифрового суспільства буде залежати від того, наскільки ефективно вдасться забезпечити захист прав і свобод громадян в умовах постійного технологічного прогресу. Тільки такий підхід забезпечить гармонійний розвиток суспільства, в якому технології служитимуть людям, а не обернуться загрозою для їхнього добробуту та свободи.

Ключові слова: цифровий тоталітаризм, споглядання та контроль, системи контролю, системи спостереження, цифрове суспільство, громадське суспільство.

Вступ. У наші часи, коли цифрове оточення та поняття цифрового суспільства стають все більш дедалі комплексними та технологізованими та викликають неабияке замішання в їхньому сприйнятті, взаємодія між країнами та світом продовжує формуватися за допомогою різноманітних досягнень комп'ютеризації суспільства та інформаційних технологій. Використання цих різноманітних технологій, особливо таких як: соціальні мережі, простір Інтернету, технологічні засоби із вбудованими системами зчитування гео-даних – розширює можливості країн у сфері контролю та спостереження за громадянами. Однак, для регламентації та регуляції, цих процесів державам із урахуванням громадських позик доводиться звертати увагу на захист цифрових каналів зв'язку, що, з іншого боку, відкриває шлях для прояву тенденцій цифрового тоталітаризму. Саме сучасні ІТ-технології та їхній неконтрольований розвиток стають ефективним методом для реалізації загрози сучасним цифровим та громадським суспільствам, а ідеї, що сформувалися у філософії минулих століть, починають активно втілюватися в життя. Ідеї утворення

Паноптикуму – не нові, проте завдяки технологізації, комп'ютеризації сучасних стратифіковано-атомізованих суспільств дають можливість створювати більш приховані системи спостереження. Саме «Цифровий Паноптикум» як метод цифрового тоталітаризму, на думку автора, постає реальною загрозою перед міжнародним суспільством. Враховуючи вищевикладене, автор висуває питання про необхідність узгодженого підходу до вивчення цифрового тоталітаризму як потенційної загрози сучасним цифровим суспільствам через аналіз сучасних тенденцій розвитку науково-технічного прогресу та інформаційних технологій.

Виділення невирішених раніше частин загальної проблеми. Дана тематика автором вважається актуальною для вивчення з боку країн пострадянського через розвиток ІТ-технологій та безперервного розвитку систем «масового стеження» та «масового контролю» за країнами та іними суспільствами. На сучасному етапі розвитку політичної науки, це питання, автором вважається не розкритим на загально доступному рівні, що доводить про необхідність поступової актуалі-

зації цієї теми через процеси її вивчення та дослідження.

Мета та завдання. Головна мета статті – є вивчення та розкриття сучасних інструментів захисту прав людини, свободи, якими суспільство може керуватись в умовах розвитку нової епохи «Цифрового тоталітаризму» за для забезпечення власної безпеки. За для досягнення були поставлені наступні дослідницькі завдання: 1) Проаналізувати актуальні наукові дослідження в проблематиці статті. 2) Визначити основні тенденції формування сучасних систем захисту прав людини. 3) Сформулювати та проаналізувати сучасний стан суспільств на нормативно-правових актів, які стоять актуальної проблематики. 4) Надати новий науковий підхід до вивчення актуальної теми.

Методи дослідження. У роботі, автором були використані загальнонаукові, а також спеціальні методи дослідження, такі як: аналізу та синтезу. При дослідженні поняття цифрового тоталітаризму, цифрового паноптикуму використовувався системний метод дослідження, тощо. Також були використані методи наукового абстрагування та узагальнення, а також науково-аналітичний метод дослідження.

Результати. Поняття Паноптикон. «Дослівно «паноптикон» з грецької означає – простір, у якому видно все» [6, с. 133] Саме така ідея була покладена братами Бенетами у створенні системи тюрем, шкіл, училищ чи заводів. «Паноптикон, описаний Дж. Бенетом у листах 1786–1787 рр., являв собою круглу чотириповерхову будівлю діаметром 100 футів з 48 одиночними камерами по периметру на кожному поверсі. Загалом Паноптикон був розрахований на 192 особи. Ширина камери по зовнішній стіні складала 6 футів. Замість дверей – решітки з тонкими прутами. У кожній камері мало бути досить велике вікно й завдяки сонячному світлу, а у вечірній час спеціальним ліхтарям все, що відбувалося всередині, повинно було добре видно з центральної точки Паноптикону» [6, с. 135]. За Бенетами популяризував ідею відомий французький філософ Мішель Фуко, який у власному творі «Наглядати і карати» розвинув ідею нагляду за людьми використовуючи напрацювання минулих авторів. «Роздуми Мішеля Фуко про локалізацію, протяжність, місцеположення відтворили послідовні зміни уявлення про простір, які панували послідовно в традиційному доіндустріальному місті, сучасному або модерному індустріальному метрополісі, постмодерному постіндустріальному мегалополісі» [3]. Поєднуючи думку про дисциплінарність владних та протовладних інституцій разом із ідеями Паноптикону, сутність системи організації роботи таких закладів, як школи, бібліотеки, інтернати, лікарні, навіть торгові універмаги стають дедалі більш зро-

зумілими. Проте цифровізація та комп'ютеризація дають змогу не тільки удосконалити ці ідеї у реальність але ще й спростити механізми створення та впровадження в усіх сферах життєдіяльності суспільств. Так що таке Цифровий Паноптикон? Виходячи із розвитку технологій, автор розуміє цей термін, як – всеохоплюючу та всепронизуючу систему спостереження за цифровим суспільством із використанням центричної системи споглядання та контролем. В сучасних технологічних містах, споглядання та контроль не є новиною «Масова комп'ютеризація сприяє посиленню процедур контролю, нагляду, реєстрації, категоризації та обліку життєдіяльності індивідів, що встановлює влади цілком нового типу» [3] Розповсюдження пандемії Covid-19, нетипові обмеження в пересуванні та оновлені системи контролю та ідентифікації, загострення міжнародних взаємовідносин останні роки, війни, тільки прискорюють неконтрольований процес розповсюдження та створення нових систем споглядання та контролю. Кожний веб-сайт, кожна сторінка, кожний клік – це окреме віконце технічних кодів, які створюють умови для користування технологіями. Ці технології, з самого початку роботи безперервно кешуються, тобто зберігають інформацію про користувачів та їхні дії та оновлюються. Саме такі дії, такі технології дають змогу стверджувати, що цифровий паноптикон – це дієвий метод завдяки, якому зчитується будь-яка інформація користувачів мережі Інтернет.

Отже, Цифровий тоталітаризм із урахуванням сучасних тенденцій розвитку цифрових суспільств – постає системою тотального контролю за всіма сферами життя суспільства, використовуючи електронні технічні засоби, які в свою чергу дозволяють лімітувати чи корегувати діяльність людини в Інтернеті. Дірк Хелбінг – німецький професор обчислювальної соціології факультету гуманітарних, соціальних і політичних наук, член факультету комп'ютерних наук ETH Zurich – виділяє наступні риси сучасних цифрових тоталітарних суспільств, а саме: (1) масове стеження; 2) неетичні експерименти з людьми в рамках існування соціальної інженерії; 4) примусове підпорядкування людей; 5) пропаганда та цензура; 6) існування «доброзичливої» диктатури; 7) поліцейська діяльність, тобто наявність «поліцейської держави»; 8) виборче застосування забезпечення прав людини) [8]. Такого роду риси притаманні наступним системам споглядання та контролю за населеннями, як PRISM, Smart-city, Системи соціального кредитування, котрі увібрали у себе новітні технології спостереження та останні операційні оновлення, що дозволяють найшвидшими шляхами збирати необхідну інформацію з боку розробників. Перша система, яку треба охарактеризувати, це «PRISM» – це програма підрозділу

Special Source Operations (SSO) АНБ США, яку було викрито у фактах шпіонажу за насленнями, країнами, мережами, урядами у 2013 р., колишнім амереканськими співробітником АНБ Джоном Сноуденом. Ця програма має єдину мережеву систему, яка сполучає її з більш ніж 100 відомими амереканськими компаніями [5]. Під підпорядкуванням цієї системи спостереження знаходяться такі компанії, як Google, Microsoft, Yahoo!, Facebook, Facetalk, PalTalk, Youtube, Skype, Apple тощо. Масштаби та контент усіх зібраних даних може різнитись. «Згідно з американським законодавством, вони зобов'язані виконувати запити про надання інформації про користувачів. Однак програма PRISM надає спецслужбам прямий доступ до серверів компаній. У документі АНБ наголошується, що її здійсненню «сприяють провайдери комунікацій у США» [4]. Ситуація навколо системи PRISM дуже швидко сколихнула різні групи населення, як в США, так і в інших країнах світу. Низка Сенаторів США, таких, як Рон Вайден (Дем. Партія), Крістофер Кунс (Дем.Партія) висловили максимальне занепокоєння та почали одразу заявляти про небезпеку існування такої технологічної програми. Washington Post у своїх аналізах дійшли висновку існування додаткових систем стеження, а саме: MAINWAY – це база даних АНБ, що містить метадані про сотні мільярдів телефонних дзвінків, здійснених через чотири найбільших телефонних компаній США: AT & T, SBC, BellSouth і Verizon.

MARINA – Метадані Інтернету (логи доступу в Інтернет окремих користувачів, логи серверів та інша інформація, що дозволяє відстежувати роботу конкретних людей в Мережі). NUCLEON- це голосові записи (телефонні розмови та ін). Разом програми можуть охоплювати, так звані «величезні території», у склад яких входять метадані телекомунікацій та інтернет-потоків, що проходять безпосередньо у США. КНР використовує такі системи, як: *Золотий щит* (неофіційна назва – «Великий китайський файрвол») – програма Інтернет-цензури та комп'ютерного стеження, реалізована Міністерством громадської безпеки КНР. Проєкт був ініційований у 1998 році та почав діяти у листопаді 2003 року, додатково існують також інформаційна мережа громадської безпеки та Бюро з нагляду. [2]

Російська федерація використовує такі системи, як СОРМ, СОРМ-1, СОРМ-2, СОРМ-3 (скорочення від рос. Система технических средств для обеспечения функций оперативно-розыскных мероприятий) – комплекс технічних засобів та заходів, призначених для проведення оперативно-розшукових заходів у мережах телефонного, рухомого та бездротового зв'язку та радіозв'язку (згідно із Законом «Про зв'язок» та наказом Міністерства зв'язку № 2339 від 9 серпня 2000).

Завдяки системі «СОРМ-1» – ведеться активне прослуховування телефонних переговорів абонентів, котра була створена у 1996 році. Завдяки «СОРМ-2» – ведеться протоколювання звернень до мережі Інтернет від користувачів.

А система «СОРМ-3» – забезпечує збирання інформації з усіх видів зв'язку та її довготривале зберігання. [2] Існування цих систем доводять реальну загрозу громадським правам на приватне життя та ставить під загрозу процеси збору та обробки персональних даних користувачів мережі Internet, а отже і всього цифрового простору в цілому. Інший технологічний прорив було розроблено за рахунок створення Технології «Smart City» – це це один винахід сучасного науково-технологічного прогресу, який покликаний поліпшити життя у великих містах, мегаполісах тощо. Мета цього глобального проєкту це «... максимізувати ефективність міських операцій та послуг та встановити зв'язок із жителями, ...поєднуючи в собі інформаційні та комунікаційні технології, або «ІКТ», з різними фізичними пристроями, підключеними до Інтернету.» [4] Таким чином, використовуючи дану технологію представники місцевих органів самоврядування можуть з легкістю стежити за діяльністю та змінами у місті та тримати прямий зв'язок із службами пенітенціарного характеру.

Непрогнозований порядок впровадження, відсутність єдиного погляду розвитку цієї технології серед держав також може переформатовати цю технологію у метод та інструмент розповсюдження цифрового тоталітаризму. Система соціального кредиту – це система завдяки якій влада може збирати інформацію щодо відповідності громадянина усім «соціальним» та «громадським» стандартам. Ця система почала розробляти у КНР ще з 2010-х рр., її спіткають різні невдачі із повноцінним впровадженням, проте на сьогодні за рахунок цієї системи держава регулює взаємодію із бізнес компаніями та громадянами власного суспільства. [1] Існування та можливий «експорт» такого винаходу у світовий ринок може спричинити тотальний контроль серед держав та урядів за всіма сферами життєдіяльності громадськості.

Висновки. Отже, цифровий паноптикон взаємопов'язаний із цифровим тоталітаризмом, виступаючи, як метод та інструмент досягнення контролю та влади над цифровими суспільствами та населенням у цифрову епоху. Багаторазове дослідження проблематики цифрового тоталітаризму, доводять ті припущення, що Цифрового Паноптикуму, як метод та інструмент дійсний та цілком реальний. Його неминучий та неконтрольований розвиток, кожний день стикає сучасні громадські суспільства, уряди та держави з важливими питаннями щодо приватності, соціальної динаміки та особистих свобод громадян та суспільств. Завдання науковців полягає у ретельному

пошуку та винаходом балансу між незаперечними перевагами технологічного прогресу та невпинною повагою до фундаментальних прав зі сторони урядів, держав та підконтрольних їми наказами комерційних компаній. Порушуючи цю проблематику ми створюємо прецедент для звернення уваги щодо траєкторій розвитку світового та вітчизняного цифрового майбутнього. Особливу увагу слід приділяти дотриманню та відповідності етичних та правових рамок, що регулюють розширення впливу цифрових технологій. У нашому прагненні до суспільства, повністю інтегрованого з цифровими технологіями, захист індивідуальної автономії та конфіденційності повинно стати пріоритетним завданням, яке має бути також на передніх планах технологічного ландшафту, що так стрімко розвивається.

ЛІТЕРАТУРА:

1. Кащавцева К. Не виплатив кредит – відключили інтернет: як працює соціальний рейтинг у Китаї. URL: <https://www.unian.ua/curiosities/chto-takoe-socialnyy-reyting-v-kitae-pravda-i-mify-12443769.html>
2. Кібершпигунство. URL: <https://www.psdinfo.pro/post/%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D1%88%D0%BF%D0%B8%D0%B3%D1%83%D0%BD%D1%81%D1%82%D0%B2%D0%BE>
3. Лозинський Р. Простір, влада і дисципліна у творах Мішеля Фуко. URL: <http://dspace.tnpu.edu.ua/bitstream/123456789/17260/1/Lozunckuu.pdf>
4. Сидорук А. Через PRISMy спецслужб. URL: <https://ms.detector.media/kiberbezpeka/post/3798/2013-06-13-cherez-prismu-spetssluzhb/>
5. Сноуден розповів, для чого спецслужби стежили за мільйонами у соцмережах. URL: <https://web.archive.org/web/20131001214703/http://www.pravda.com.ua/news/2013/09/29/6998918/>
6. Сокальська О.В. Пенітенціарна система Джеремі Бентама: нереалізований проєкт «ідеальної в'язниці». Питання боротьби зі злочинністю: зб. наук. пр. / редкол.: В. І. Борисов та ін. Харків: Право, 2020. Вип. 40. 132-146 с.
7. Gade D. (2024) Top 10 Smart Services of Smart Cities. URL : <https://medium.com/@drdgade/top-smart-services-of-smart-cities-a5f31a412844>
8. Helbing D. (2017) Digital fascism rising? URL: <https://www.theglobalist.com/fascism-big-data-artificial-intelligence-surveillance-democracy/>

REFERENCES:

1. Kashhavceva K. (2023) Ne vyplatyv kredyt – vidkljuchyly internet: jak pracjuje socialnyj rejtyng u Kytaji. UNIAN. Retrieved from: <https://www.unian.ua/curiosities/chto-takoe-socialnyy-reyting-v-kitae-pravda-i-mify-12443769.html>
2. Kibershpyghunstvo (2023, February 9). Retrieved from: <https://www.psdinfo.pro/post/%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D1%88%D0%BF%D0%B8%D0%B3%D1%83%D0%BD%D1%81%D1%82%D0%B2%D0%BE>
3. Lozynskij R. Prostir, vlada i dycyplina u tvorakh Mishelja Fuko. Retrieved from: <http://dspace.tnpu.edu.ua/bitstream/123456789/17260/1/Lozunckuu.pdf>
4. Sydoruk A. (2013, June 13) Cherez PRISMy specsluzhb. Retrieved from: <https://ms.detector.media/kiberbezpeka/post/3798/2013-06-13-cherez-prismu-spetssluzhb/>
5. Snouden rozpoviv, dlja chogho specsluzhby stezhyly za milijonamy u socmerezhakh (2013, September 29) Ukrainskya Pravda. Retrieved from: <https://web.archive.org/web/20131001214703/http://www.pravda.com.ua/news/2013/09/29/6998918/>
6. Sokaljska O.V. (2020) Penitenciarna sistema Dzeremi Bentama: nerealizovanyj projekt «idealnoji v'jaznyci». Kharkiv: Pravo, Vol. 40, pp. 132-146.
7. Gade D. (2024) Top 10 Smart Services of Smart Cities. Retrieved from: <https://medium.com/@drdgade/top-smart-services-of-smart-cities-a5f31a412844>
8. Helbing D. (2017) Digital fascism rising? Retrieved from: <https://www.theglobalist.com/fascism-big-data-artificial-intelligence-surveillance-democracy/>

«Digital Panopticon» as a method of spreading digital totalitarianism and a threat to modern international relations

Sokorinskiy Vladimir Olegovich

Postgraduate Student of the Faculty
of International Relations,
Political Science
and Sociology
Odesa National I.I. Mechnikov University
Dvorianska str., 2, Odesa, Ukraine
ORCID: 0009-0006-1676-5173

The article examines the concept of a digital panopticon, a method of spreading digital totalitarianism as a political regime that spreads in the era of electronic regimes. It has been proven that the digital panopticon is a relevant subject of research for modern political science. The digital panopticon is a manifestation of the uncontrolled and relentless development of today's information technology systems. Due to the uncontrolled development of IT technologies, there is a problem of threats to international relations among the main actors and subjects of the international arena. The article provides a historical description of the idea of the Panopticon to the present day. This panopticon reflects the need for a balanced approach to protecting the rights and freedoms of citizens in the context of rapid technological development. With the help of digital technologies, especially social networks, the Internet and geodata reading systems, society is under constant surveillance and control. However, this raises questions about privacy, social dynamics and personal freedoms. The Digital Panopticon is a real tool that inevitably affects modern civil society. Its development is uncontrolled and unpredictable, which raises important questions for governments, states and citizens. This situation requires careful consideration and a balanced approach to the use of digital technologies in order to ensure the protection of basic human rights. In this context, special attention should be paid to the development and observance of ethical and legal norms governing the use of digital technologies. The legal framework must guarantee the protection of privacy, individual autonomy and confidentiality of citizens. The public awareness of these problems is currently insufficient, therefore it is important to intensify the research and consideration of digital totalitarianism as a threat to the modern digital society. Establishing a balance between technological opportunities and the protection of personal rights and freedoms is an important task for scientists, human rights defenders and society as a whole. In the future, the successful development of the digital society will depend on how effectively it will be possible to ensure the protection of the rights and freedoms of citizens in conditions of constant technological progress. Only such an approach will ensure the harmonious development of a society in which technology will serve people and not become a threat to their well-being and freedom.

Key words: digital totalitarianism, surveillance and control, control systems, surveillance systems, digital society, public society.