

## СУЧАСНІ ІНСТРУМЕНТИ ЗАХИСТУ ПРАВ, СВОБОДИ ТА БЕЗПЕКИ ОСОБИСТОСТІ В ЕПОХУ «ЦИФРОВОГО ТОТАЛІТАРИЗМУ»

### MODERN TOOLS FOR PROTECTION OF HUMAN RIGHTS, FREEDOMS AND SECURITY IN THE "DIGITAL TOTALITARIANISM" ERA

Сокоринський В.О.,

*аспірант факультету міжнародних відносин, політології, соціології  
Одеського національного університету імені І.І. Мечникова*

Сучасність, яка обумовлена постійним науково-технічним прогресом та знаходиться в перманентному стані трансформації та розвитку, постійно надає нові можливості для перебудови та оновлення світу. Цим характеризується розвиток та вдосконалення систем політичного урядування, виникнення нових режимів, які досить часто можуть носити ознаки «гібридних». В сучасному політологічному дискурсі прийнято вважати та розглядати систему тоталітарних держав через призму історичного методу дослідження. Перша хвиля тоталітаризму, яка також в науковому дискурсі вважається «Класичним тоталітаризмом» з'явилася в умовах переходу до індустріального суспільства. Після цієї епохи, сучасний світ пережив багато трансформацій, які безпосередньо впливають на форми та структуру сучасних держав та їхніх суспільств. Поява другої хвилі тоталітаризму можлива в рамках переходу суспільства до постіндустріальної або інформаційної системи. Однією з рис інформаційного суспільства є його непереборна тенденція до глобалізації (уніфікації/об'єднання/кооперації) усіх сфер життя. Ця уніфікація веде за собою побудову складних мережево-центричних зв'язків, які можуть пронизувати інформаційні суспільства. У сучасному світі глобалізація проявляється у створенні єдиного економічного простору, єдиної комунікативно-технологічної системи, та соціально-політичної структури. За для забезпечення такої системи, інформаційні технології дають змогу трансформувати сучасні політичні режими. Розвиток е-Демократії логічним способом дав можливість розвитку е-Тоталітаризму, який став логічним продовженням розвитку режимної парадигми осі «Демократія-Тоталітаризм». Держави, країни, суспільства, вбудовуючись у світові відносини підвладні й сучасним політичним віянням, які можуть докорінно змінювати характер та природу влади. Трансформація, адаптація до нових умов світових відносин та їхньої динаміки, пов'язана також з можливим формуванням нової політичної реальності, типу політичної культури, форм та технологій. Вивчення природи тоталітаризму до сьогодні є однією з актуальних політологічних питань, яке надає багато відповідей для упередження розвитку загроз сучасним політичним та соціальним систем.

У статті розглядається новітні прояви та проблеми, який породжує цифровий тоталітаризм. Особлива увага приділяється сучасним системам захисту прав та свобод й безпеки особистості. Аналізуються існуючі форми реакції та відповіді на загрози в умовах «Цифрового тоталітаризму».

**Ключові слова:** тоталітаризм, цифровий тоталітаризм, права людини, захист прав людини.

Modernity, which is due to constant scientific and technological progress and is in a permanent state of transformation and development, constantly provides new opportunities for restructuring and renewal of the world. This characterizes the development and improvement of systems of political governance, the emergence of new regimes, which can often bear the hallmarks of "hybrid". In modern political science discourse, it is customary to consider and consider the system of totalitarian states through the prism of the historical method of research. The first wave of totalitarianism, which is also considered in scientific discourse "Classical totalitarianism" appeared in the transition to industrial society. After this era, the modern world has undergone many transformations that directly affect the forms and structure of modern states and their societies. The emergence of the second wave of totalitarianism is possible in the transition of society to a post-industrial or information system. One of the features of the information society is its irresistible tendency towards globalization (unification / unification / cooperation) of all spheres of life. This unification leads to the construction of complex network-centric connections that can permeate information societies. In today's world, globalization is manifested in the creation of a single economic space, a single communication and technological system, and socio-political structure. To ensure such a system, information technology makes it possible to transform modern political regimes. The development of e-Democracy in a logical way provided opportunities for the development of e-Totalitarianism, which became a logical continuation of the development of the regime paradigm of the axis "Democracy-Totalitarianism". States, countries, societies, integrating into world relations are subject to modern political trends that can radically change the nature and nature of power. Transformation, adaptation to new conditions of world relations and their dynamics, is also associated with the possible formation of a new political reality, such as political culture, forms and technologies. The study of the nature of totalitarianism is still one of the most pressing political issues, which provides many answers to prevent the development of threats to modern political and social systems.

The article examines the latest manifestations and problems posed by digital totalitarianism. Particular attention is paid to modern systems of protection of human rights and freedoms and security. Existing forms of reaction and response to threats in the conditions of "Digital Totalitarianism" are analyzed.

**Key words:** totalitarianism, digital totalitarianism, human rights, protection of human rights.

**Постановка проблеми.** В сучасному суспільстві, є очевидним думки, що інформаційні технології (ІТ) на зорі свого зародження були покликани за для емансипації людини та надавали новий спосіб для розвитку свободи серед людей. Глобальна мережа «Інтернет» сьогодні нівелює не тільки

кордони але й надає змогу реалізовувати будь-які політичні проекти, які дуже важко здійснити за межами Інтернет-зв'язку, тобто «офлайн». Парадоксально, проте, нові можливості дуже швидко отримали і інші оцінки та стали розглядатися, як загроза демократичній стабільності та свободи людини. З огляду на таку парадоксальність впливу інформаційних технологій на сучасні суспільства, актуальність захисту прав, свобод та безпеки особистості в епоху «Цифрового тоталітаризму» постає очевидною.

Це питання постійно продовжує набирати характер «особливого» через постійний розвиток ІТ-сфери та постійного втручання державних структур в процеси розповсюдження та вдосконалення засобів комунікацій.

#### **Аналіз останніх досліджень і публікацій.**

Характеризуючи *ступінь наукової розробки* проблеми слід відзначити прогностичне значення наукового доробку відомих зарубіжних дослідників, таких як Д. Белл [3], З. Бжезинський [4], А. Бюль [22], М. Вейнстейн [27], П. Дракер [7], А. Крокер [27], М. Паєтау [21], А. Турен [18], Е. Тоффлер [16], Х. Аренд [19] в аналізі проблем розвитку демократії, природи тоталітаризму та значення інформаційних технологій в цих процесах.

Не можна не відзначити практичне значення доробку сучасних дослідників, які першими почали дослідження феномену саме «цифрового тоталітаризму», і серед них Джон Барлоу [20], Вінсент Ф. Хендрікс і Мадс Вестергоард [24], Сімона Янковські [25], Бюнг-Чул Хань [23], Хусейн Пусат Кілдіг [26].

Серед вітчизняних вчених слід назвати таких дослідників як А. Баранов [2], Г. Атаманов [1], В. Богуш [5], В. Лопатін [12], О. Додонов [6], Б. Кормич [8], О. Литвиненко [10], Г. Смолян [13], О. Соснін [14], О. Юдін [5], які досліджували питання кібербезпеки в країнах СНД та України.

**Виділення невирішених раніше частин загальної проблеми.** Дана тематика автором вважається актуальною для вивчення з боку країн пострадянського простору виходячи з набуття поступової актуальності через питання розповсюдження проблем «масового стеження» та «масового контролю» за суспільствами через активну науково-технічну революцію у світі. На сучасному етапі розвитку політичної науки, це питання вважається не розкритим на належному рівні, що доводить про необхідність актуалізації цієї теми дослідження.

**Формулювання цілей статті (постановка 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 без-

пеки. 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) Сформувати та проаналізувати сучасний стан суспільств на нормативно-правових актів, які стуються актуальної проблематики. 4) Надати новий науковий підхід до вивчення актуальної теми.

**Виклад основного матеріалу дослідження.** З появою цифрових технологій виникла серйозна потреба у розвитку захисту абсолютно нової форми «прав людини», таких як – цифрових прав (digital rights).

Так за словами Е. Талапіної: «Під цифровими правами (digital rights) у всьому світі розуміються специфічні права людини, які мають публічно-правове походження» [15]. Коли кажуть про цифрові права людини, то першочерговим вважаються реальні гарантії отримання права на підключення до Інтернет мережі. В свою чергу, це право розподіляється на дві суттєві категорії:

а) право на користування послугою у виді «Інтернету»;

б) право на отримання інформації через Інтернет;

Методом забезпечення гарантій прав людини на думку, А. Тулікова є своєчасне виявлення фактів невідповідності обмежень прав людини загрозам інформаційної безпеки і наслідків їх прояву, превентивні дії спеціалізованих державних органів, омбудсмена, створення незалежних інституцій цифрової безпеки, які будуть мати контрольні функції, спрямовані на стримування недемократичних зазіхань з боку цифрових структур державної влади [17].

Право на доступ до Інтернету розглядають, як частину права на свободу від блокування, яке визнається втручанням у власне життя. Дослідники бачать проблему не тільки, коли використання Інтернету для політичної критики стикається з репресіями (як в Китаї, Північній Африці, на Близькому Сході), але і коли відключення від Інтернету відбувається як санкція за повторне порушення авторських прав (Франція та Великобританія) [15]. Ст. 10 Конвенції прав людини гарантує право на свободу вираження поглядів та право на доступ до інформації, але виходячи з процесу цифрової трансформації, ця стаття доповнюється правом доступу до Інтернету. В світовій практиці таке визнання відбувається за трьома варіантами: визнання Інтернету універсальною і загальнодоступною послугою (Естонія, Іспанія); закріплення права на доступ до Інтернету в якості конституційного права (Греція, Португалія); визнання цього права вищими судами (Франція, Коста-Ріка) [15]. Виходячи з того, що стан цифрових технологій переважає існування індивіда в мережі,

то людина, яка виключена з доступу до користування Інтернетом втрачає можливість брати пряму участь в соціально-політичному житті країни. Ця проблема ставить в цікаве положення держави, які повинні надавати доступ до Інтернету громадянам, щоб забезпечувати право «право на комунікацію» (right to communicate). Звісно, вільність тлумачення забезпечення «права на комунікацію» надає урядам право вказувати, що таке право існує, головне забезпечувати себе можливостями користуватися цим правом. Так, цікавий приклад тлумачення «права на комунікацію» можемо побачити в Конституції Непалу 2015 р. у ст. 19, яке визначається як: «введення обмежень на цензурування інформації, поширюваної різними способами, в тому числі шляхом розміщення електронних публікацій» у ч. 1 ст. 19; «заборона на закриття, арешт або анулювання реєстрації будь-яких засобів масової інформації, включаючи цифрові та електронні» у ч. 2 ст. 19, а також «заборона на закриття будь-яких засобів зв'язку, включаючи пресу, електронні засоби зв'язку та телефонію» у ч. 3 ст. 19 [9].

Поняття «безпека», «інформаційна безпека» розкриваються через поняття «стан захищеності життєво важливих інтересів особистості, суспільства і держави». Інформаційна безпека в даному випадку визначається як стан захищеності національних інтересів в інформаційній сфері, що складається з сукупності збалансованих інтересів особистості, суспільства і держави від внутрішніх і зовнішніх загроз» [17]. Особливо, проблематика загострюється навколо «права на публічність» та «права на конфіденційність» (або «права на повагу до приватного життя»), як і навколо «права на збереження репутації», «права на цифрову ідентичність» [15].

Держава, яка все обирає шлях забезпечення цифрових прав звела свою участь у вирішенні лише незначних завдань, а саме : 1) не перешкоджати здійсненню прав людини через Інтернет і не обмежувати їх (наприклад, не здійснювати цензуру); 2) захищати законне використання інформаційно-комунікаційних технологій від кібератак з боку третіх осіб; 3) гарантувати та полегшувати законне використання інформаційно-комунікаційних технологій (доступ малозабезпечених осіб до Інтернету) [15]. Ця проблема, досліджувалась такими дослідниками, як Г. Алмонд, Р. Арон, К. Баймьо, Б. Барбер, Є. Вятр, А. Лейпхарт, А. Пшеворський, Дж. Цімерман. Так наприклад, Р. Арон, Х. Арендт, К. Гаджієв, Р. Даль, Р. Дарендорф, К. Попер, Дж. Сарторі в контексті захисту демократії і протистояння встановленню «тоталітарній демократії» при зовнішньому демократичному фасаді. Наприклад, у книзі «Vita Activa, або про активне життя» Х Арендт вперше поставила проблему *стирання межі між приватним та публічним*, порівняла політичний простір, що

формується при тоталітарному режимі як «порядок домогосподарства», який спирається на нерівність, нерозмежування приватного та публічного, тиск з боку більшості, відсутність індивідуальної свободи. У роботі «Джерела тоталітаризму» вона ж вказала, що основою тоталітаризму є деперсоналізація людини, що вказує на мобілізацію активності за рахунок маніпуляції влади. Усвідомлений прояв політичної активності в цій системі неможливий, оскільки «декласований натовп» втрачає самостійність, а індивід будь-яку дію здійснює за сценарієм. Отже, відбувається *поглинання приватного – публічним*.

Погоджуючись із Х. Арендт, Сергій Пролєєв звернув увагу на те, що в модерну епоху відбувається руйнування класичних «політичної», «громадської, «публічної» сфер через їх поглинання сферою «приватних відносин». Спираючись на критику виявлення «єдиних рис тоталітарної моделі» Г. Гласнером, А. Куном, Т. Джонсом та прихильниками Франкфуртської школи – Т. Адорно, Г. Маркузе, Ю. Габермаса, Е. Фрома – Пролєєв зазначив, що ознаки тоталітаризму є і у розвинутій ринковій системі, де існує *практика стирання межі між приватним і публічним* через *поглинання приватним – публічного*.

Таким чином, «систематичний збір відомостей секретними службами є втручання в приватне життя, навіть якщо ці відомості одержано в громадських місцях і якщо містять інформацію виключно про професійної або громадської діяльності особи. Ті ж дії, здійснювані за допомогою застосування GPS-технологій, і зберігання даних про місцезнаходження особи і його пересування також представляють собою втручання в приватне життя» [15].

В цьому відношенні, на думку Е. Талапіної суди повинні знаходити баланс між приватними та публічними інтересами. Авторка приводить справу, яка викликала масу контрверсійних оцінок через постанову Європейського суду з прав людини у справі «Біг Бразер Вотч та інші проти Сполученого Королівства». Рішення Суду наполягало: «...що масове стеження «per se» – не порушує Конвенцію. Європейський суд визнав, що рішення про введення режиму масового перехоплення діяло для того, щоб ідентифікувати невідомі загрози національній безпеці, і що це є правом держави при виборі того, яким чином краще забезпечити досягнення легітимної мети захисту безпеки» [15]. Отже, в питанні перехоплення даних, стеження за людьми було визнано правом держави, яка фактично порушила право на конфіденційність.

Якщо розглянути правові доктрини США і ЄС, то «інформаційна безпека» за цими доктринами здійснюється через конкретні заходи забезпечення безпеки та пов'язується з принци-

пами та правами конфіденційності, цілісності та доступності інформації та інформаційних систем. За доктринами, ці права та принципи, забезпечують баланс інтересів між усіма сторонами правовідносин, а отже, виступають гарантіями прав людини в державній сфері забезпечення «інформаційної безпеки». Але на практиці, дія державних органів не завжди рахується з правами людини і фактично користувач поступово втрачає контроль над використанням своїх персональних даних, і, нерідко, на добровільній основі [17]. Наприклад, у Швейцарії питання про розширення можливостей щодо встановлення масового стеження вирішувалося референдумом і рішення було прийнято на його користь, що продемонструвало і довіру державі [9].

Отже, людина з традиційним «приватним світом» поступається людині – публічній, приватність якої оцифрована та у будь-яку мить, помилково чи навмисно, може стати публічним надбанням, хоча в самому Європейському Союзі право на недоторканність приватного життя є фундаментальним правом, захист якого гарантується ст. 8 Європейської конвенції про захист прав людини і основних свобод 1950 р. і конституціями держав-членів ЄС.

Методом забезпечення гарантій прав людини на думку, А. Тулікова є своєчасне виявлення фактів невідповідності обмежень прав людини загрозам інформаційної безпеки і наслідків їх прояву, превентивні дії спеціалізованих державних органів, омбудсмена, створення незалежних інституцій цифрової безпеки, які будуть мати контрольні функції, спрямовані на стримування недемократичних зазіхань з боку цифрових структур державної влади [171]. Пригадуючи «залізний закон бюрократизації» Роберта Міхельса, слід пам'ятати, що цифрова грамотність та своєчасна дія громадянських структур, в тому числі і протестна, має бути спрямована на захист цифрових прав громадянина та на опір неототалітаризму «старшого брата» у державі [11]. Видимість протестних інтервенцій, як у фізичному, так і цифровому просторі, лежить в основі успішного вису-

вання вимог, впливає на процес прийняття рішень і формування політики щодо важливих для громадянського суспільства питань, будь то міське планування, права людини, рівноправність або турбота про навколишнє середовище [11]. Поява таких технологій, як стрімінг, суспільно-громадське мовлення, отримання фото – та відео – зображень з дронів, технології розширеної та доповненої реальності, тобто – VR(virtual reality)/(віртуальна реальність), AR(augmented reality)/(доповнена реальність) та цифрові голограми, мають потенціал як форми цифрових форм опору. До того ж, обізнаність громадянських структур в цій галузі забезпечить розвиток цифрових форм демократії. Загальноприйнятним має стати рішення Європейського суду з прав людини, вираженого в справі «Класс та інші проти Німеччини», за яким «право таємного спостереження за громадянами, яке характерне для поліцейської держави, прийнятне відповідно до Конвенції тільки тоді, коли воно строго необхідно для збереження демократії» [17].

**Висновки та перспективи подальших розвідок у цьому напрямі.** Визначено, що розвиток технологій призводить до появи загроз національній безпеці держави. Необхідність захисту даних цінностей стає підставою для обмеження права на недоторканність приватного життя. Відповідність обмежень цілям їх встановлення виступає гарантією прав людини і інформаційної безпеки особистості. Держава завжди більш оперативно реагує на можливості, які надають нові інформаційно-комунікаційні технології для захисту публічних, ніж приватних інтересів. Це обумовлено тим, що стійкість функціонування інститутів публічної влади, збереження правопорядку є необхідною передумовою дотримання прав людини. Але, цифрова грамотність, консолідована громадська дія, розвиток Інтернет права постають умовами захисту прав людини та громадянина в системі е-урядування та в умовах неототалітарних форм контролю з боку держави та наднаціональних корпоративних структур.

#### СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Атаманов Г. А. Інформаційна безпека в сучасному російському суспільстві (соціально-філософський аспект): дис. ... канд. філос. наук: 09.00.11 Волгоград.2006.168 с.
2. Баранов А. Інформаційний суверенітет або інформаційна безпека. Національна безпека і оборона. 2001. № 1. С. 70-76
3. Белл Д. Майбутнє постіндустріальне суспільство. Досвід соціального прогнозування. М.: Academia, 2004. 788с. URL: <https://www.twirpx.com/file/682165/>
4. Бжезинський З. Велика шахівниця (Панування Америки і його геостратегічні імперативи). пер. з англ. Е. А. Нарочницької, Ю. Н. Кобякова. – М.: Міжнародні відносини, 2004. 287 с. URL: <http://www.lib.ru/POLITOLOG/AMERICA/bzhezinskij.txt>
5. Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. – К. : МК-Прес, 2005. – 432 с.
6. Додонов О. Г. Системи організаційного управління: інформаційні технології та безпека / О. Г. Додонов, О. С. Горбачик, М. Г. Кузнецова. Матеріали междунар. науч. конф. ИТБ-2013 «Информационные технологии и безопасность: оценка состояния». Вып. 13. С. 5.

7. Дракер П. Посткапиталистическое общество // Новая постиндустриальная волна на Западе. Антология / Под ред. В. Л. Иноземцева. М.: Academia. 1999. С. 71.
8. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України: дис. ... д-ра юрид. наук : спец. 12.00.07. – Одеса, 2004. – 427 с.
9. Коротич Р.А. Особливості розвитку прав і свобод людини в умовах цифрового суспільства. Вчені записки Тамбовського відділення. Росмен. 2020. № 17. URL: <https://cyberleninka.ru/article/n/osobennosti-razvitiya-prav-i-svobod-cheloveka-v-usloviyah-tsifrovogo-obschestva>
10. Литвиненко О.В. Проблеми забезпечення інформаційної безпеки у пострадянських країнах (на прикладі України та Росії) : Автореф. дис. ... канд. політ. наук : 23.00.04. – К., 1997. – 18 с  
Литвиненко О.В. Проблеми забезпечення інформаційної безпеки у пострадянських країнах (на прикладі України та Росії) : Автореф. дис. ... канд. політ. наук : 23.00.04. – К., 1997. – 18 с
11. Локоть Т. Майбутнє видимості: можливості мережевих технологій для громадянського невдоволення. Сканування горизонтів: роль інформаційних технологій в майбутньому цивільного суспільства. 2020. № 1. URL: <https://cyberleninka.ru/article/n/budushee-vidimosti-vozmozhnosti-setevyh-tehnologiy-dlya-grazhdanskogo-needovolstva>
12. Лопатин В.Н. Информационная безопасность России: дис... д-ра юрид. наук. М., 2003. 433 с.
13. Смолян Г.Л. Новини інформаційної війни./ Г. Л. Смолян, В Цигічко, Д. Черешкін. Захист інформації. «Конфідент». № 6. 1996 г.
14. Соснін О. Інформаційні ризики в державному управлінні / О. Соснін, С. Яременко. Віче. – 2011. – № 8. – С. 24-27. URL: [http://nbuv.gov.ua/UJRN/viche\\_2011\\_8\\_10](http://nbuv.gov.ua/UJRN/viche_2011_8_10)
15. Талапіна Е. В. Еволюція прав людини в цифрову епоху. Праці Інституту держави і права РАН. 2019. № 3. URL: <https://cyberleninka.ru/article/n/evolyutsiya-prav-cheloveka-v-tsifrovuyu-epohu>
16. Тоффлер, Елвін. Третя хвиля. Переклад на російську мову: А. Мірер, І. Москвіна-Тарханова, В. Кулагіна-Ярцева, Л. Бурмістрова, К. Бурмістров, Е. Комарова, А. Мікіша, Е. Руднева, Н. Хмелько. М. 2004. Центр гуманітарних технологій. 27.01.2011. URL: <https://gtmarket.ru/laboratory/basis/4821>
17. Туліков А.В. Забезпечення інформаційної безпеки як гарантія прав людини. Право. Журнал Вищої школи економіки. 2015. № 2. URL: <https://cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-kak-garantiya-prav-cheloveka>
18. Турен А. Повернення людини чинної. Нарис соціології. М., 1998.
19. Arendt H. *The origins of totalitarianism*. New York: Harcourt Brace & Company, 1951.
20. Barlow J. A declaration of the independence of cyberspace. 1996. URL: <https://www.eff.org/cyberspace-independence>
21. Becker B., Paetau M. Virtualisierung des Sozialen. Die Informationsgesellschaft zwischen Fragmentierung und Globalisierung. Frankfurt a. M. 1997.
22. Bühl A. The virtual society: Economy, politics and culture under the sign of cyberspace. Opladen, 1997.
23. Han B. C. Digital Totalitarianism: How Big Data Is Killing Free Will.
24. WorldCrunch. 07.05.2016. URL: <https://www.worldcrunch.com/culture-society/digital-totalitarianism-how-big-data-is-killing-free-will>
24. Hendricks V. F, Vestergaard M. Epilogue: Digital Roads to Totalitarianism. In 'Reality Lost: Markets of Attention, Misinformation and Manipulation'. 2018. P. 119-199. URL: [https://link.springer.com/chapter/10.1007/978-3-030-00813-0\\_7](https://link.springer.com/chapter/10.1007/978-3-030-00813-0_7)
25. Jankowski S. The Sectors Where the Internet of Things Really Matters, *Harvard Business Review*. 2014. 22.09.2014. URL: <https://hbr.org/2014/10/the-sectors-where-the-internet-of-things-really-matters>
26. Koldis H. P. Digital Totalitarianism: China's Social Credit System. Ankasam. 27. 04.2019. URL: <https://ankasam.org/en/digital-totalitarianism-chinas-social-credit-system/>
27. Kroker A., Weinstein M. Data Trash. The Theory of the Virtual Class. Montreal, 1994. URL: <http://www.thing.net/~rdom/ucsd/posthuman/DATATRASH.pdf>