DOI: 10.26565/2220-8089-2020-37-12
УДК: 32.019.51

Bohdan Tymchyshyn
Master's graduate,
V.N. Karazin Kharkiv National University,
4, Svoboda Sq., Kharkiv, 61022, Ukraine,
sonicofan@ukr.net,
https://orcid.org/0000-0001-7469-7339

TOTALITARIAN THREATS OF DIGITAL AGE

The growing challenges of the emergence of totalitarianism of a new format generated by the information age are investigated. The features of the new totalitarianism are revealed. Classical totalitarianism manifested itself in the form of a totalitarian state and used measures to ensure control over people, including terror. Today, totalitarianism is much more hidden in nature, because it makes use of modern fashion for the «transparency» of everything (the state, companies, personal life) and the tools for obtaining information about people and events. The trend of the state monopoly leaving the sphere of control, storing personal information, and its manipulation, but it creates conditions for private organizations to initiate their own mechanisms with the same tasks is analyzed. It is explained that these may be algorithms that exploit human behavior for a commercial or political purpose. It turns out that in the context of polarization and politicization, commercial organizations have their own agenda, which allows them to demonstrate themselves as a more significant political actor. As an example, the fact is given that the amount of information and its accuracy that large Internet companies possess about their users is likely to surpass in these indicators the information that the most influential intelligence organizations in the past had. Examples of countries in which mass surveillance of their own citizens on the Internet are openly and implicitly gradually deploying digital totalitarianism are considered. The phenomenon of the global outbreak of the COVID-19 pandemic is analyzed as a factor of an attack on human rights for privacy, including individual digital privacy. We study the trends of how, both democratic and authoritarian states, use resonant events and catastrophes as an opportunity to usurp power and gain more control over their citizens. The assumption is made that the digital era implemented the world of cyberpunk in life. It concludes that escape from the situation of elusive privacy through civic activism, pressure groups, and supranational bodies such as the European Union and competition laws.

***Keywords**: totalitarianism, information age, mass surveillance, privacy, information harvesting, Big Tech, coronavirus, COVID-19, cyberpunk.*

Тимчишин Богдан Володимирович
магістр політології,
Харківський національний
університет імені В.Н. Каразіна,
майдан Свободи, 4, Харків, 61022,
sonicofan@ukr.net,
https://orcid.org/0000-0001-7469-7339

ТОТАЛІТАРНІ ЗАГРОЗИ В ІНФОРМАЦІЙНУ ЕПОХУ

Досліджуються наростаючі виклики виникнення тоталітаризму нового формату, що породжується інформаційної епохою. Розкриваються особливості нового тоталітаризму. Класичний тоталітаризм маніфестував себе в формі тоталітарної держави, використовував заходи, що забезпечували контроль над людьми, включаючи терор. Сьогодні тоталітаризм має куди більш прихований характер, оскільки користується сучасною модою на «прозорість» всього (держави, підприємств, особистого життя) і інструментами

отримання інформації про людей і події. Аналізується тренд виходу державної монополії зі сфери контролю, зберігання персональної інформації та маніпулювання нею, натомість створюються умови для приватних організацій ініціювати власні механізми із такими самими завданнями. Пояснюється, що це можуть бути алгоритми, які експлуатують людську поведінку з комерційною або політичною метою. З'ясовується, що в умовах поляризації та політизації, у комерційних організаціях виникає власний порядок денний, що дозволяє їм демонструвати себе як більш значущого політичного актора. Для прикладу наводиться факт того, що обсяг інформації та її точність, якими володіють великі інтернет-компанії про своїх користувачів, імовірно, перевершує за цими показниками інформацію, яку мали найвпливовіші організації розвідки в минулому. Розглядаються приклади країн, в яких масове стеження за власними громадянами в мережі Інтернет, відкрито і імпліцитно поступово розгортає цифровий тоталітаризм. Аналізується феномен глобального спалаху пандемії COVID-19 як фактор наступу на права людини на приватне життя, в тому числі на індивідуальну цифрову приватність. Вивчаються тенденції як демократичних, так і авторитарних держав, що користуються резонансними подіями і катастрофами як можливістю узурпації влади і отримання більшого контролю над своїми громадянами. Робиться припущення, що, цифрова епоха імплементувала в життя світ кіберпанку. Робиться висновок щодо виходу з ситуації вислизаючої приватності через цивільний активізм, групи тиску і такі наддержавні органи, як Європейський Союз і закони про конкуренцію.

***Ключові слова**: тоталітаризм, інформаційна епоха, масове стеження, приватність, збір інформації, Big Tech, коронавірус, COVID-19, кіберпанк.*

Тимчишин Богдан Владимирович
магистр политологии,
Харьковский национальный
университет имени В. Н. Каразина,
площадь Свободы, 4, Харьков, 61022,
sonicofan@ukr.net,
https://orcid.org/0000-0001-7469-7339

ТОТАЛИТАРНЫЕ УГРОЗЫ В ИНФОРМАЦИОННУЮ ЭПОХУ

Исследуются нарастающие вызовы возникновения тоталитаризма нового формата, порождаемого информационной эпохой. Раскрываются особенности нового тоталитаризма. Классический тоталитаризм манифестировал себя в форме тоталитарного государства, использовал меры, обеспечивающие контроль над людьми, включая террор. Сегодня тоталитаризм имеет куда более скрытый характер, поскольку пользуется современной модой на «прозрачность» всего (государства, компаний, личной жизни) и инструментами получения информации о людях и событиях. Анализируется тренд выхода государственной монополии из сферы контроля, хранения персональной информации и манипулирования ею, зато создаются условия для частных организаций инициировать собственные механизмы с такими же задачами. Объясняется, что это могут быть алгоритмы, которые эксплуатируют человеческое поведение с коммерческой или политической целью. Выясняется, что в условиях поляризации и политизации, в коммерческих организациях возникает собственная повестка дня, что позволяет им демонстрировать себя как более значимого политического актора. Для примера приводится факт того, что объем информации и ее точность, которыми обладают крупные интернет-компании о своих пользователях, вероятно, превосходит по этим показателям информацию, которую имели самые влиятельные организации разведки в прошлом. Рассматриваются примеры стран, в которых массовое наблюдение за собственными гражданами в сети Интернет, открыто и имплицитно постепенно разворачивает цифровой тоталитаризм. Анализируется феномен глобального вспышки пандемии COVID-19 как фактор наступления на права человека на частную жизнь, в том числе на индивидуальную цифровую приватность. Изучаются тенденции как демократических, так и авторитарных государств, пользующихся резонансными событиями и катастрофами как возможностью узурпации власти и получения большего контроля над своими гражданами. Делается предположение, что, цифровая эпоха имплементировала в жизни мир киберпанка. Делается вывод о выходе из

ситуации ускользающей приватности через гражданский активизм, группы давления и такие надгосударственные органы, как Европейский Союз и законы о конкуренции.

***Ключевые слова**: тоталитаризм, информационная эпоха, массовая слежка, приватность, сбор информации, Big Tech, коронавирус, COVID-19, киберпанк.*

For a long time, the legal systems of countries lagged behind the pace of development and spread of the Internet, however, many politicians from different countries are beginning to realize the value that can be extracted from the digital space. Therefore, every year we can observe how the state begins to penetrate into the Internet, thereby making it more regulated and less free.

The tragedy of September 11, 2001, which happened in the USA, became a catalyst for the American authorities to start taking measures to prevent terrorism, even at the cost of freedom and privacy of the personal lives of their citizens. These measures have been transformed into the PATRIOT Act, the main framework for the state's mass surveillance (Uniting and Strengthening America 2001).

The revelations of the American whistleblower, Edward Snowden in 2013, revealed the existence of a real program called «PRISM» aimed for mass surveillance of all Internet users utilizing the vast amount of information sources, including the information streams of large computer and Internet corporations of the United States (Greenwald, MacAskill 2013). The information disclosed by Snowden caused an unprecedented scale of attention in the media and led us to discuss mass surveillance in an entirely different way, the consequences could include an increase in tension of relations between the countries of the world and the United States and the fact of knowledge of the existence of a real program for global mass surveillance (Solms, Heerden 2015). No measures were taken to reduce the degree of surveillance by the American state.

The topic of external and internal terrorism has long ceased to be the central narrative of political discussion, which generated public demand for collective security. However, there are no dynamics of weakening surveillance of Americans and we dare to suggest that the means of providing mass surveillance are being improved from year to year.

The country, whose name was recently associated with the value of "«freedom», which gave technology that has connected the whole world, has been going through turbulent times over the past two decades, especially the last 5 years have been distinguished by the intensification of conflicts on domestic policy and ever-increasing polarization of society.

The ruling party of China, enriched by the profit from the country's production, is beginning to actively develop and implement information technologies as tools of total control over their citizens. China has already tried with its project «Golden Shield» to isolate its citizens from the «external network» and this project has some success, but the ongoing development of new information technologies is aimed at eliminating the concept of «privacy» and implementing full transparency of citizen data for the authorities. This is a centralized collection of information about each person that goes beyond the digital space, where each action is evaluated by computer systems in real-time, which subsequently make adjustments to the «social rating», which sounds like another horror story from dystopian novels, but this is already a reality for over a billion Chinese citizens (Mosher 2019).

The current government of the Russian Federation is working on its own version of restricting digital freedom, more control over the actions of Russian users, collecting data about them and isolating them from the rest of the Internet, calling it «sovereign Internet», motivating that this project will help in increasing level of national security (Давлашян 2019).

Roskomnadzor, the Russian agency responsible for regulating information channels that block access to certain websites and network services, has become notorious for its incompetence in the events of the Telegram ban, a messenger created by Pavel Durov. Incompetence was shown by blocking the IP addresses belonging to the hosting provider Amazon Web Services, which created the problem of access to many large Internet resources that were not the target of blocking, no actions made towards desirable change and Telegram itself remained available. Roskomnadzor had to roll back blockings to restore access to resources blocked by mistake. In the end, Telegram is formally banned, but millions of Russian users continue to use it (Барышева 2018).

We assume that the implementation of the «sovereign Internet» project will not bring the desired results, that is, the isolation of the Russian part of the Internet from the global

network if the personnel policy of this agency will not change.

It is worth mentioning that the prerequisites for the creation of the Telegram arose with Pavel, when in 2011 «special forces» began to make visits to him. A little after, in 2013, «Putin's people» forced Durov to sell them VKontakte, making the social network informally state-owned, penetrated with various monitoring and intelligence services (Hakim 2014).

Citizens who are critical of the «sovereign Internet" concept often call it «Cheburnet».

The government's application «Diia», implementing the concept of «a state in a smartphone», proposed in its program by President Vladimir Zelensky is a double-edged sword (Передвиборча програма кандидата 2019). The transfer of public services online allows acceleration and optimization of their use, reduce the volume of red tape, and the risks of corruption. Digitization of documents and their legitimate power equal to the existing physical originals make Ukraine a real pioneer in this direction of e-government. However, despite the obvious advantages like ease of use, the destruction of space for corruption and falsification of documents, there are significant risks for Ukrainians in the form of direct state surveillance of the app users, collection of various data from the device. Also, external threats, which are rogue states, will do their best to crack the application's security system in order to disrupt government processes and steal vital data about citizens.

This concept certainly deserves the right for full implementation but requires a wide public discussion about data privacy, the involvement of experts in the field of digital privacy and security.

In the light of recent global events, the outbreak of COVID-19 will force some states to take new measures to monitor and prevent infectious diseases that will trample on such terms as «confidentiality of personal data» and «privacy» as a price for public health. The argument for this trend will be - China. The leading party, the CCP, whose negligence and fear of losing a positive image among its citizens, have just become a catalyst for a global pandemic, are now trying to capitalize on the current catastrophe. Manipulating the statistics of infection and recovery rates, (Wadhams, Jacobs 2020) lying to the world community through WHO (Weissmueller 2020) and organizing the delivery of humanitarian aid to the most affected countries, all these actions are aimed at creating the image of China as a leader in the fight against a pandemic and the superiority of authoritarian methods of managing the state in a catastrophe and general insurance of safety of its own citizens (Barbaccia 2020). In such difficult times, people are inclined to meet their main need - security, and it is likely for many citizens of the democratic world that China will become an example to be followed, especially in the context of the failure of the United States, the longest-living and one of the largest democracies of the world, in providing an adequate response to the outbreak of the pandemic.

National authorities around the world have set about developing their own mobile application. This created a situation of heterogeneity and wide diversity in the choice of approach.

Installing the application as an option raises doubts about the effectiveness and general feasibility of this path, but there are still not enough studies at the moment that confirm or disprove these doubts. So far, the only successful voluntary application is «TraceTogether», created by the Singaporean government. The application has more than a million installations, collects information about people with COVID-19 and their movement through the exchange of encrypted Bluetooth-handshake, which is one of the best ways to transfer information in terms of security and privacy. Singapore has a very low COVID-19 morbidity rate and has the lowest mortality rate from this disease, which allows us to assume that the application allows Singaporeans to detect the presence of coronavirus infection in the very early stages, receive treatment as early as possible, greatly reducing damage to the health (Coronavirus (COVID-19) death rate in countries with confirmed deaths and over 1,000 reported cases as of June 5, 2020, by country).

However, a number of countries, in their strategy for the contamination of coronavirus infection, have taken measures mandatory installation of the application. A case in point is India, where, depending on the region or city, a person can get a fine or a ticket to jail for not having the «Aarogya Setu» app on their phone. The opacity of data streams and the lack of legislation regarding the protection of data and privacy on the Internet, this tool to combat coronavirus poses a threat to the privacy of Indian citizens in both short and long term (Howell O'Neill 2020).

The previously mentioned polarization of society in the United States echoes far beyond the borders of this country. The unprecedented

consequences for the Internet caused by the split in American society quickly poured into the private enterprise.

For a long time, most of the public discussion went online because of the convenience, the presence of a wide audience and the speed of receiving feedback. Despite the benefits of discussing various political issues on the Internet, there is the problem of freedom of speech. Although states can constitutionally guarantee the right of people to freedom of speech and public discussion, private companies that own digital spaces for meetings and discussions are not required to comply with the rights of clients to freedom of speech and have their own policies regarding the rules for publishing information and censorship (Keller 2019).

Also, one of the indirect, nevertheless unpleasant consequences is the arbitrary creation of echo-chambers. Attention economies, which are social networks, large platforms for public discussion and media hosting have specific algorithms aimed at providing users content that matches their likings and preferences. Thus, many people consuming political content fall into the trap of one-sided perception of information, because the algorithms take into account preferences and try not to give any uninteresting information to them but potentially could allow users to learn about alternative or opposing points of view. Unfortunately, algorithms do not include diversification of suggested info and form a distorted idea of real political life.

Mark Zuckerberg's testimony before the U.S. Congress in 2018 provided information that his website collects almost all data possible about their online activity from users' computers without the consent of the users themselves. The data collected is not directly sold to third parties, however, according to Zuckerberg himself, this data is a source of company profit (Anderson, Jesdanun 2018).

The amount of information that Facebook has about its users is of interest not only to parties who want to advertise products and services. Facebook's policy includes providing access to the collection of data to various types of scientific organizations for conducting social research. In 2018, whistleblower and a former Cambridge Analytica employee disclosed information about the fact that information received from «Your Digital Life» was processed and then used its results in facilitating the election campaigns of Ted Cruz and Donald Trump. The application «Your Digital Life», developed by the British researcher Aleksandr Kogan for scientific purposes. The application got access to personal information of the users and the information of the “friends” of the users, even those who did not install this application. People's profiles were created from the information collected and transferred to «Cambridge Analytica», a UK-based private political consultancy organization (Wylie 2018). Facebook has vulnerabilities for abuse of personal information by third parties. The consequence was Facebook's ban on publishing personality quizzes, the company's loss in share prices and public trust (Kastrenakes 2019). This scandal provoked an acute negative reaction from users and the spontaneous campaign «#DeleteFacebook», which urged users to delete their Facebook accounts because of the danger of various kinds of manipulation, but this initiative caused difficulties for some people, since erasing an individual digital footprint was a difficult task due to the entanglement of information in a broad scale (Griffin 2018).

It is worth mentioning that, based on more than 250 «likes», a social network can know more about a person than a spouse (Youyou, Kosinski, Stillwell 2015) and with a 90% probability to predict the gender and race of a person (Kosinski, Stillwell, Graepel 2013). The early Facebook investor, Sean Parker in his interview for Axios gave insight that the site is designed exploiting «vulnerabilities» of human psychology (Allen 2017).

We believe that cyberpunk has already arrived, not as beautiful and attractive as many writers and artists have imagined, but its manifestation in the real world is no less horrifying.

All the worst cyberpunk tropes described in many works of this genre begin to find a place in our real daily life. If the pictures drawn by cyberpunk look frightening, then the reality is terrifying since these most terrible options of our future do not just become reality, but become reality at a pace that attention cannot be paid enough to it. Cyberpunk has already come, we just haven't noticed it.

The poor visibility of the advent of the cyberpunk era is due to the gradual introduction of technology into our everyday lives, and we get used to them without much deliberation. Fictional worlds 20-30 years ago, cyberpunk seemed to us very far from reality and it was easy to distinguish the real world of that time from the world of cyberpunk. Today, when technological development is becoming close to cyberpunk levels and how these technologies have changed the socio-political structure of

societies. The only thing that distinguishes the current real world from the world of cyberpunk is the attractive aesthetics of the latter, which our meatspace did not inherit. Cyberpunk dystopia, in which we all ended up today, came out extremely dull (Cuck Philosophy 2019).

The optimism of various futurologists who anticipated the development of the Internet and means of mass communication as an amplification of democracy and people's freedom turned out to be unjustified. We are witnessing the exact opposite picture, people have become victims of manipulations by large computer corporations and political forces that study the Internet and weaponize the Internet for their propaganda.

We believe that privacy on- and off-line is becoming an increasingly expensive luxury. In the case of using VPN services, this can be taken literally, but in this context, the time and effort taken to search for information on means to minimize monitoring and tracking are understood.

Is liberalism, in particular economic liberalism, which gave a possibility for the birth of large corporations, will be destroyed by its own creation? Those who call themselves liberals today should redefine the individual-state-business relationship because large businesses with great power and control can pose an unobvious threat to democracy and human rights. The laissez-faire concept turns into a farce and ceases to serve the interests of the whole society when large companies do not have accountability to society and social responsibility.

Big players are gaining strength every year, introducing their lobbyists into political systems and this is only a matter of time when exclusively representatives of corporate interests will remain in parliaments. At least some opposition to the growing hegemony of large Internet corporations is being provided by the European Union, accusing in abusing user's data and exercising monopoly power. EU completion law commissioners charge multi-billion fines for data misuse (Hamilton 2018) creates a working system for protecting personal information on the Internet such as GDPR (General Data Protection Regulation 2016), albeit with incidents like Article 13, which caused massive public outrage, interpreting it as a meme ban on the Internet, the European Parliament later reassured people, saying that the memes would not be touched (Kleinman 2019).

The desire of the European Union to fight for the freedom of the Internet and respect for the rights of people online only proves the need for this entity and the need for its development.

Given the dependence on the Internet of the economy and society, we, as citizens and users, should be civic in every way so that digital space meets the interests of not only large corporations and intelligence services.

We believe that strengthening the human rights movement for digital privacy could put pressure on national authorities in countries with large information sectors to make Internet corporations more privacy-oriented and government agencies more transparent digitally.

The topic of privacy in the digital space, the collection of information for the purpose of implicit mass manipulation of people's opinions and behavior, will acquire more and more significance and not only deserves but requires even more attention and research.

REFERENCES

"Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (Usa Patriot Act) Act of 2001", *Govinfo.* URL: https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

Greenwald, G., MacAskill, E. 2013. "NSA Prism program taps in to user data of Apple, Google and others". *The Guardian.* URL: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

von Solms, Sune. van Heerden, R. 2015. "The Consequences of Edward Snowden NSA Related Information Disclosures" *Research Gate.* URL: https://www.researchgate.net/publication/275019554

Mosher, S. 2019. "China's new 'social credit system' is a dystopian nightmare", *New York Post.* URL: https://nypost.com/2019/05/18/chinas-new-social-credit-system-turns-orwells-1984-into-reality/

Давлашян, Н. 2019. "Что такое "суверенный интернет" и чем он грозит пользователям?", *Euronews.* URL: https://ru.euronews.com/2019/02/13/ru-russia-sovereign-internet-explainer

Барышева, Е. 2018. "Роскомнадзор против Telegram: как блокировки повлияли на сервис Дурова", *Deutsche Welle.* URL: https://p.dw.com/p/30vRX

Hakim, D. 2014. "Once Celebrated in Russia, the Programmer Pavel Durov Chooses Exile" *The New York Times.* URL: https://www.nytimes.com/2014/12/03/technology/once-celebrated-in-russia-programmer-pavel-durov-chooses-exile.html

"Передвиборча програма кандидата на пост Президента України Володимира Зеленського". 2019. *Зе! Команда.* URL: https://program.ze2019.com

Wadhams, N., Jacobs, J. 2020. "China

Intentionally Under-reported Total Coronavirus Cases and Deaths, U.S. Intelligence Says" *Fortune*. URL: https://fortune.com/2020/04/01/china-coronavirus-cases-deaths-total-under-report-cover-up-covid-19/

Weissmueller, Z. 2020. "How China Corrupted the World Health Organization's Response to COVID-19", *Reason.* URL: https://reason.com/video/how-china-corrupted-the-world-health-organizations-response-to-covid-19/

Barbaccia, G. 2020. "Could China's Coronavirus Surveillance Come to the US?", *China Uncensored.* URL: https://youtu.be/qvOctm0R8P0?t=199

"Coronavirus (COVID-19) Death Rate in Countries With Confirmed Deaths and Over 1,000 Reported Cases as of June 5, 2020, by country". 2020. *Statista.* URL: https://www.statista.com/statistics/1105914/coronavirus-death-rates-worldwide/

Howell, P. 2020. "India is Forcing People to Use its Covid App, Unlike any Other Democracy" *MIT Technology Review*. URL: https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-covid-app-mandatory/

Keller, D. 2019. "Facebook Restricts Speech by Popular Demand", *The Atlantic.* URL: https://www.theatlantic.com/ideas/archive/2019/09/facebook-restricts-free-speech-popular-demand/598462/

Anderson, M., Jesdanun, A. 2018. "Factcheck: Facebook Doesn't Sell Data But Profits off it", *WHYY.* URL: https://whyy.org/articles/watch-facebooks-zuckerberg-senate-testimony/

Wylie, C. 2018. "Cambridge Analytica Whistleblower: 'We Spent $1m Harvesting Millions of Facebook Profiles'", *The Guardian.* URL: https://youtu.be/FXdYSQ6nu-M

Kastrenakes, J. 2019. "Facebook Bans Personality Quizzes After Cambridge Analytica Scandal", *The Verge.* URL: https://www.theverge.com/2019/4/25/18516608/facebook-personality-quiz-ban-cambridge-analytica

Griffin, A. 2018. "Delete Facebook Campaign Takes Off – But Actually Removing Your Data Might Prove More Difficult Than It Seems", *The Independent.* URL: https://www.independent.co.uk/life-style/gadgets-and-tech/news/delete-facebook-cambridge-analytica-campaign-deactivate-data-remove-hide-privacy-a8266671.html

Youyou, W., Kosinski, M., Stillwell, D. 2015. "Computer-based Personality Judgments are More Accurate Than Those Made by Humans", *PNAS.* URL: https://doi.org/10.1073/PNAS.1418680112

Kosinski, M., Stillwell, D., Graepel, T. 2013. "Private traits and attributes are predictable from digital records of human behavior", *PNAS*. URL: https://doi.org/10.1073/pnas.1218772110

Allen, M. 2017. "Sean Parker: Facebook was designed to exploit human "vulnerability"", *Axios.* URL: https://www.axios.com/sean-parker-unloads-on-facebook-god-only-knows-what-its-doing-to-our-childrens-brains-1513306792-f855e7b4-4e99-4d60-8d51-2775559c2671.html

Cuck Philosophy. 2019. "The Cultural Significance of Cyberpunk" *Cuck Philosophy*. URL: https://youtu.be/Nvor7hhDKTs?t=1024

Hamilton, I. 2018. "The EU is now Going After Amazon After Slapping Google and Apple With Giant Fines" *Business Insider.* URL: https://www.businessinsider.com/amazon-investigated-by-eu-commissioner-margrethe-vestager-2018-9?r=US&IR=T

"General Data Protection Regulation". 2016. *Official Journal of the European Union.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Kleinman, Z. 2019. "Article 13: Memes Exempt as EU Backs Controversial Copyright Law", *BBC.* URL: https://www.bbc.com/news/technology-47708144

REFERENCES

"Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act Of 2001". 2001. *Govinfo.* URL: https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

Greenwald, G., MacAskill, E. 2013. "NSA Prism program taps in to user data of Apple, Google and others". *The Guardian.* URL: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

von Solms, Sune. van Heerden, R. 2015. "The Consequences of Edward Snowden NSA Related Information Disclosures" *Research Gate.* URL: https://www.researchgate.net/publication/275019554

Mosher, S. 2019. "China's new 'social credit system' is a dystopian nightmare", *New York Post.* URL: https://nypost.com/2019/05/18/chinas-new-social-credit-system-turns-orwells-1984-into-reality/

Davlashyan, N. 2019. "What is the "sovereign Internet" and what does it threaten users with?", *Euronews* .URL: https://ru.euronews.com/2019/02/13/ru-russia-sovereign-internet-explainer (in Russian)

Barysheva, E. 2018. "Roskomnadzor vs Telegram: how locks affected Durov's service" *Deutsche Welle*. URL: https://p.dw.com/p/30vRX (in Russian)

Hakim, D. 2014. "Once Celebrated in Russia, the Programmer Pavel Durov Chooses Exile" *The New York Times.* URL: https://www.nytimes.com/2014/12/03/technology/once-celebrated-in-russia-programmer-pavel-durov-chooses-exile.html

"Volodymyr Zelensky's Election program of the candidate for President of Ukraine". 2019. *Ze! Komanda.* URL: https://program.ze2019.com (in Ukrainian)

Barbaccia, G. 2020. "Could China's Coronavirus Surveillance Come to the US?", *China Uncensored.* URL: https://youtu.be/qvOctm0R8P0?t=199

Wadhams, N., Jacobs, J. 2020. "China intentionally under-reported total coronavirus cases

and deaths, U.S. intelligence says" *Fortune*. URL: https://fortune.com/2020/04/01/china-coronavirus-cases-deaths-total-under-report-cover-up-covid-19/

Weissmueller, Z. 2020. "How China Corrupted the World Health Organization's Response to COVID-19", *Reason.* URL: https://reason.com/video/how-china-corrupted-the-world-health-organizations-response-to-covid-19/

"Coronavirus (COVID-19) death rate in countries with confirmed deaths and over 1,000 reported cases as of June 5, 2020, by country". 2020. *Statista* URL: https://www.statista.com/statistics/1105914/coronavirus-death-rates-worldwide/

Howell, P. 2020. "India is forcing people to use its covid app, unlike any other democracy" *MIT Technology Review* URL: https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-covid-app-mandatory/

Keller, D. 2019. "Facebook Restricts Speech by Popular Demand", *The Atlantic* URL: https://www.theatlantic.com/ideas/archive/2019/09/facebook-restricts-free-speech-popular-demand/598462/

Anderson, M., Jesdanun, A. 2018. "Factcheck: Facebook doesn't sell data but profits off it", *WHYY* URL: https://whyy.org/articles/watch-facebooks-zuckerberg-senate-testimony/

Wylie, C. 2018. "Cambridge Analytica whistleblower: 'We spent $1m harvesting millions of Facebook profiles'", *The Guardian* URL: https://youtu.be/FXdYSQ6nu-M

Kastrenakes, J. 2019. "Facebook bans personality quizzes after Cambridge Analytica scandal", *The Verge*. URL: https://www.theverge.com/2019/4/25/18516608/facebook-personality-quiz-ban-cambridge-analytica

Griffin, A. 2018. "Delete Facebook Campaign Takes Off – But Actually Removing Your Data Might Prove More Difficult Than It Seems", *The Independent.* URL: https://www.independent.co.uk/life-style/gadgets-and-tech/news/delete-facebook-cambridge-analytica-campaign-deactivate-data-remove-hide-privacy-a8266671.html

Youyou, W., Kosinski, M., Stillwell, D. 2015. "Computer-based personality judgments are more accurate than those made by humans", *PNAS.* URL: https://doi.org/10.1073/PNAS.1418680112

Kosinski, M., Stillwell, D., Graepel, T. 2013. "Private traits and attributes are predictable from digital records of human behavior", *PNAS.* URL: https://doi.org/10.1073/pnas.1218772110

Allen, M. 2017. "Sean Parker: Facebook was designed to exploit human "vulnerability"", *Axios.* URL: https://www.axios.com/sean-parker-unloads-on-facebook-god-only-knows-what-its-doing-to-our-childrens-brains-1513306792-f855e7b4-4e99-4d60-8d51-2775559c2671.html

Cuck Philosophy. 2019. "The Cultural Significance of Cyberpunk", *Cuck Philosophy*. URL: https://youtu.be/Nvor7hhDKTs?t=1024

Hamilton, I. 2018. "The EU is now going after Amazon after slapping Google and Apple with giant fines" *Business Insider*. URL: https://www.businessinsider.com/amazon-investigated-by-eu-commissioner-margrethe-vestager-2018-9?r=US&IR=T

"General Data Protection Regulation". 2016. *Official Journal of the European Union.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Kleinman, Z. 2019. "Article 13: Memes exempt as EU backs controversial copyright law", *BBC*. URL: https://www.bbc.com/news/technology-47708144