FOLIA 376

Annales Universitatis Paedagogicae Cracoviensis

Studia de Securitate 13(1) (2023)

ISSN 2657–8549

DOI 10.24917/26578549.13.1.9

Mateusz Łabuz
Chemnitz University of Technology
ORCID 0000-0002-6065-2188

The Metaverse as a potential threat to democracy: virtual world, real consequences

Metaverse jako potencjalne zagrożenie dla demokracji – świat wirtualny, realne konsekwencje

Abstract

The Metaverse, with its growing popularity, may significantly change the ways in which individuals and institutions use the Internet in the future. Several private companies and public institutions have already decided to open virtual headquarters to respond to the growing demand of customers. However, new opportunities are associated with many legal, social, and psychological challenges, and the problem of the extensive use of virtual reality must be considered in a multidimensional, interconnected way. The development of the Metaverse in the form proposed by the proponents of the new technology might lead to blurring of the boundaries between the real and virtual worlds. The potential transfer of a significant part of life to virtual reality requires pre-emptive actions on the part of legislators and law enforcement authorities to prepare for the inevitable: the use of yet another channel of action for cybercrime. The aim of this article is to draw attention to the threats to democracy, security and privacy that might be associated with the development of the Metaverse and to discuss the ongoing national and international debates regarding the political and legal problems connected to the Metaverse. A careful analysis of both the threats and the debates allows for an informed response to the multidimensional challenges stemming from development of the Metaverse and helps to identify which institutions should play a key role in shaping this response.

Keywords: metaverse, virtual reality, democracy, criminality in the virtual world, policing in metaverse, manipulation in metaverse

Abstrakt

Metaverse cieszy się rosnącą popularnością odbiorców i zainteresowaniem biznesu i może w przyszłości znacząco zmienić formy używania Internetu przez użytkowników indywidualnych i instytucjonalnych. Coraz więcej firm i urzędów decyduje się na otwarcie swoich wirtualnych

siedzib, by odpowiedzieć na zwiększające się zapotrzebowanie ze strony odbiorców. Nowe możliwości wiążą się jednak z licznymi wyzwaniami natury prawnej, społecznej czy psychologicznej, a problem ekstensywnego użycia wirtualnej rzeczywistości musi być rozpatrywany wielowymiarowo i uwzględniać interdyscyplinarność zjawiska. Rozwój metaverse w formie proponowanej przez orędowników nowej technologii może prowadzić do zatarcia granic między światem realnym i wirtualnym. Stąd też potencjalne przeniesienie znacznej części życia do wirtualnej rzeczywistości wymaga wyprzedzających działań ze strony ustawodawcy i organów ścigania, by przygotować się na nieuniknione – wykorzystanie kolejnego kanału działań dla cyberprzestępczości i wyrafinowanej manipulacji. Celem artykułu jest zwrócenie uwagi na wciąż niską świadomość zagrożeń dla demokracji, bezpieczeństwa i prywatności łączących się z dynamicznym rozwojem technologii i samej koncepcji metaverse oraz odnotowanie bieżących debat w przestrzeni międzynarodowej i narodowej dotyczących zagrożeń politycznych i prawnych w metaverse. Umożliwi to odpowiedź na pytanie, w jaki sposób przeciwdziałać wielowymiarowym wyzwaniom związanym z rozwojem metaverse i jakie środowiska powinny uczestniczyć w doborze i kształtowaniu odpowiednich mechanizmów.

Słowa kluczowe: metaverse, metawersum, wirtualna rzeczywistość, demokracja, przestępczość w świecie wirtualnym, polityczne manipulacje w metaverse

Introduction

"The Metaverse" as a concept appeared long ago, but only recently gained popularity and became the subject of mass interest. Touted as the technology of the future,[1] it is supposed to revolutionize the way the Internet will be used. Analysis of the business potential and the social impact of the Metaverse are not unambiguous. Some experts raise concerns over a speculative bubble or "hype"[2] that often accompanies new technology (Anderson & Rainie, 2022: 6). One may underline the sociopsychological aspects of immersion or point out that transferring a significant part of life to the Metaverse evades modern regulatory standards and needs to be thoroughly investigated to assess potential threats to society or democratic systems (Dwivedi, 2022: 43). There is no doubt that the Metaverse provides many positive applications, e.g. in education, leisure, medicine, or sales, and that the protection of democracy should not be a pretext for preventive censorship or overregulation. At the same time, one should not forget that the development of a new technology, which, according to some estimates, might comprise up to 10% of the global economy in the future (Giaglis et al., 2022: 13), requires constant monitoring of trends and threat analysis and necessitates that state authorities to be an active part of that process.

Semantically, the term "Metaverse" is derived from the combination of the notions "meta" (meaning something that is post or beyond) and "universe" (Pimentel et al.,

[1] A helpful definition of the Metaverse is provided by Wang et al. (2022:1): "…the metaverse is regarded as a fully immersive, hyper spatiotemporal, and self-sustaining virtual shared space blending the ternary physical, human, and digital worlds. Metaverse is recognized as an evolving paradigm of the next-generation Internet after the web and the mobile Internet revolutions, where users can live as digital natives and experience an alternative life in virtuality."

[2] Something that gains a lot of interest in relatively short time, mostly exaggerated.

2022: 2) and it was first used by science-fiction novelist N. Stephenson in 1992 in his book "Snow Crash" (Anderson & Rainie, 2022: 5) to depict a specific type of virtual reality (VR). Today, the Metaverse is linked mostly to the technological development of VR or augmented reality (AR), which allows for the generation of three-dimensional mixed reality (MR), where real elements are combined with virtual ones, enabling users equipped with dedicated headsets to "interact in a fully or partially synthetic digital environment constructed by technology" (Mystakidis, 2022: 487). It is possible to describe it as the next stage of the Internet, even if it seems unlikely that the Metaverse will match the Internet's accessibility in the coming years or that it will completely replace the Internet (Xu et al., 2022: 1).

Metaverse users navigate MR worlds[3] using virtual alter-egos called "avatars." Both the Metaverse and avatars realistically reflect the real world, mirroring real places and activities and even reproducing an individual's personal characteristics in the form of their avatar-representations (Park & Kim, 2022: 4211). The key element of interaction is the so-called "immersion," in which the boundaries between the real and virtual worlds are gradually blurred (Büchel & Klös, 2022: 5), and consequently, the perception of reality might be distorted. Visions of multidimensional Metaverses have been presented through literature and cinematography; one of the most prominent examples is the movie adaptation of the science-fiction novel by E. Cline entitled "Ready Player One." In another example, filmmaker Steven Spielberg portrayed a rather grim, dystopic future in which VR offers an escape from the real world to the Metaverse in a movie called Oasis.

Perhaps the most important sign of the Metaverse's growing importance as the "technology of tomorrow" was Facebook's decision to rebrand as "Meta" in 2021 (Chohan, 2022). This decision underlined Facebook's global aspirations to shape the Metaverse environment and invest in that technology (Dwivedi et al., 2022: 2). Experts estimate that the Metaverse market might be worth billions of dollars, and its potential is quickly growing. It is estimated that by the end of 2026, 25% of people will spend at least one hour a day interacting via the Metaverse (European Parliament, 2022: 2). Research conducted by the Fraunhofer Institute (2022) shows that 58% of respondents from the United States, Germany, and China could imagine transferring part of their life activity to the Metaverse, and 22% would be willing to accept a complete transfer of their life to the Metaverse (Duwe et al., 2022: 5). On the other hand, some companies have already decided to reduce expenditures on research related to the Metaverse due to cost and uncertain business prospects (Whelan & Flint, 2023). What is more, some experts have pointed out that the Metaverse might already be dead as it "lacked a coherent vision," and the tech industry has already "turned to a new, more promising trend – generative AI" (Zitron, 2023). Interest in Meta seems to be diminishing. One may plausibly argue that the aspirations failed to meet the challenge, at least at this stage of technological development. This does not mean, however, that the Metaverse should

[3] There is no one universal Metaverse, though it has already been noted that the interoperability of different platforms may occur in the future. The most significant examples of Metaverses today are Meta's Horizon Worlds, Decentraland, Roblox, and The Sandbox.

be seen as completely buried. It might return in another incarnation, as an improved version of what engineers had managed to achieve in the first phase of development.

These issues should draw the attention of lawmakers, law enforcement agencies, and experts in social interaction. The European Union devotes an increasing number of documents to the Metaverse. It has already launched a "Virtual and Augmented Reality Industrial Coalition" to connect stakeholders engaged in developing Metaverse technologies (Kabelka, 2022). In December 2022, the Digital Committee of the German Bundestag held a special meeting dedicated to Web 3.0 and the Metaverse, which raised serious concerns over social aspects of the new technology (Digital Committee of Bundestag, 2022). In the United States, the issue of the Metaverse has been addressed by the Congressional Research Service (Zhu, 2022).

Some countries have gone even further. The United Arab Emirates established a virtual ministry, Barbados opened the first digital embassy using the Metaverse, while Singapore funded the "Centre for Strategic Futures" (Vishnoi, 2021), which will concentrate on "building capacities, mindsets, expertise and tools for strategic anticipation and risk management which would shape policy making decisions" (Centre for Strategic Futures, 2022). The World Economic Forum in Davos launched the initiative, "Defining and Building the Metaverse," comprised of stakeholders motivated to "develop and share actionable strategies for creating and governing the Metaverse" (World Economic Forum, 2022).

While the debate is ongoing, there is a significant gap in public discussion of new threats to democracy, security and privacy brought on by the Metaverse. Considering this gap, this study takes up the threats to democracy stemming from the development of the Metaverse and, specifically, the use of MR in political campaigns. The list presented in this study is not exhaustive, and the catalog of threats and harmful forms of using MR will presumably increase with the development of the Metaverse. It should be assumed that MR, with its potential to monitor users' interactions and behavior, will become a valuable field for collecting data and generating highly personalized content, which in turn may increase the potential for the manipulation of private user information. The Metaverse will also affect the security environment as crime patterns will potentially be replicated there and will dynamically adjust to new tools and opportunities. A detailed description of these potential problems will help to identify the best countermeasures and the institutions most appropriate to shape them. This description will, in turn, provide answers to the question of how to prepare for the challenges related to the development of the Metaverse. In sum, the aim of this study is to highlight the risks associated with the expansion of the Metaverse and to encourage debate on social, legislative, and political levels.

Methods

The study used the methods of scientific inference and analysis. The study drew on secondary sources of information (source literature), legal acts and statistical data.

The focus of the study is threats to democracy generated by the Metaverse, meaning the personalization of the political content based on data analysis. Its aim is to develop

a set of recommendations for state authorities, including law enforcement agencies, regarding the potential development of the Metaverse and threats stemming from its use on a large scale.

Potential threats – cybercrime

Cybercrime is an extremely complex phenomenon, the detailed description of which goes beyond the scope of this study. The Metaverse is widely considered to be one of the arenas of cybercriminal activity. Some countries, including Estonia, Denmark, and Norway, have already invested in online policing that, in the future, might possibly be extended to the Metaverse. "Nettpatrulje" (Norwegian Internet Patrols) or experiences of cooperation among law enforcement agencies (Europol, 2022: 24) are good examples of proactive approaches, even if they are not aimed directly at the Metaverse. In 2022 Interpol launched its own Metaverse that would allow for training and capacity building. Interpol's Executive Director of Technology and Innovation commented that "[i]n order for police to understand the Metaverse, we need to experience it" (Interpol, 2022). Some countries have set up new units within police forces to concentrate on cybercrime exclusively. All these activities are steps in the right direction and can be a prelude to capacity building measures.

It should not be expected that the reality created within the Metaverse will be significantly different from the one we already know. Rather, it should be assumed that already existing crime patterns will be replicated in the Metaverse. Moreover, users of the Metaverse will gain new opportunities to commit crimes, some of which will likely be initially observed and penalized as responses to reported cases (Qin, Wang, Hui, 2022: 1). The reactive approach, though conventional on legal grounds, might be insufficient to prepare for what is yet to come.

As mentioned above, it should be assumed that already codified types of crime will also appear in the Metaverse, albeit in a slightly modified form. This entails the need to determine to what extent current regulations will apply to the Metaverse, which in practice should result in extending the existing jurisdiction to virtual worlds. As a result, some experts (Jaursch, 2022) claim that it is not the right moment to regulate the Metaverse with new laws specific to it, but instead to enforce already existing applicable regulations, including the European Union Digital Services Act.[4] They need to be effective, and for that, they need to be supported. This point of view assumes that regulators should be proactive, set the tone of the discussion, and unequivocally favor a rational approach to the use of current measures instead of getting into protracted theoretical or semantic debates.

Lawmakers should also respond to the growing demand to penalize digital acts of violence, including the rape or murder of an avatar. The "crude delineation between physical and virtual will become increasingly problematic. As these experiences become more embodied, start to feel more real, we will have to decide at which point virtual experiences will be equally impactful as those of the physical realm" (Europol, 2022: 17).

[4] A legal act adopted by the EU in 2022 to ensure a safe and accountable environment online.

That might naturally lead to a discussion on the liability of avatars and their owners. The creation of a digital identity or even a "digital body" would require protection within civil law but also a closer look at liability issues. It would also be necessary to find the proper legal mechanisms to address avatar-to-avatar interactions of a criminal nature. According to some researchers, one next step might even be granting rights to avatars if they possess consciousness (Cheong, 2022: 470–472), although this attribute should not overshadow the more central debate about human beings' rights in the Metaverse.

The next iteration of the Internet might further hinder the identification of cybercrime and make it even harder to secure digital evidence, particularly in cases involving decentralization and anonymity (Europol, 2022: 11). It has already been a difficult task under the current conditions, and the Metaverse will increase the problems of law enforcement in that aspect. The basic threats have been recognized by international law enforcement organizations. Interpol (2022) points out that the Metaverse can be used for criminal purposes such as money laundering, data theft, child grooming and child sexual exploitation, harassment, sexual assault, stalking, cyberattacks, cyber-physical attacks, financial fraud, social engineering, scams, counterfeiting and copyright infringements, and terrorism recruitment and training. Studies have already identified potential threats to data security and identity theft. They have also found a detrimental sociopsychological impact, at least to some parts of society (Dwivedi et al., 2022: 3). That might pave the way for further harmful effects. In addition, cyberbullying, and a variety of negative phenomena regarding surveillance (government and corporate ones), espionage, or disinformation on an unprecedented scale (Jaursch, 2022) should be taken into account.

Europol (2022) warns that "criminals have already been selling digital fingerprints, which imitate the user's device's characteristics and behavior" and speculates that in the future, criminals may generate synthetic identities and add behavioral layers to fakes. Potential threats, in this case, are associated not only with the classical sphere of criminal law (identity theft, extortion, phishing), but also with the creation of a powerful field for abuse in the areas of message personalization, manipulation, and propaganda.

There might be serious reasons for concern regarding children's safety. The Metaverse could amplify negative outcomes such as grooming or sexual abuse, while the use of haptics and sensory devices prevalent in the Metaverse may pave the way for online sensual harassment (Europol, 2022: 18). According to Europol (2022) in 2020 58% of girls experienced online harassment. The Metaverse opens up even greater opportunities for the perpetrators of crimes. Their effects can be more severe than in the real world due to immersion.

This is just a sample list that contains the types of crimes that appear in the classic version of the Internet. Unfortunately, the Metaverse can become a platform where negative processes are amplified and challenging to investigate.

Potential threats to democracy

There are many possible applications of the Metaverse in the context of politics: conducting remote meetings with stakeholders, conducting trainings for civil servants,

and organizing election rallies within MR (Dunn, 2022). Politicians could merchandise and raise funds for political campaigns while saving costs for townhalls and debates in the real world (Choudhary, 2022). This might facilitate participation, bring some citizens who have not been interested in traditional means of communication with authorities closer, and at the same time save time and to reduce the carbon footprint. But this is just one side of the coin.

There is a reason why some researchers describe the Metaverse as "the most dangerous tool of persuasion ever created" (Rosenberg, 2022: 2) or call it a "world of expanded surveillance" that is "more powerful than a lie detector" (Wheeler, 2022: 8). Politicians have been using emerging technologies for some time to increase their chances for election. It might be the case that political parties would use the Metaverse to reach a wider audience, especially in the age, ethnic, or minority groups where they underperform.

The Metaverse might be one of the first places where data analysis and biometric identification play a prevailing role in crafting tailor-made political messages. R. Waltzman (2022) offers a fictitious example of a campaign reaching out to millions of users with the presentation of personalized versions of a candidate based on their physical resemblance to the viewers. Mimicry might be used to manipulate audiences who are unaware of this type of process, giving them a false impression of a resemblance, and increasing the chances for identification and thus for a vote. That very idea was studied in 2008 by researchers at Stanford University, who assessed the outcome of facial resemblance between candidates and voters. They concluded that "given the revolution in information technology […] political strategists will increasingly resort to transformed facial similarity as a form of campaign advertising" (Bailenson et al., 2008: 954). The question arises of whether the Metaverse will offer the technical feasibility for such a far-reaching manipulation.

Thus far, yes, and it may go even further. Researchers are already warning against the potential misuse of private data, including the tracking of physical reactions such as pupil dilation, heart rate, eyes movement, and skin moisture. The use of data emerging from the sphere of intimacy that cannot consciously be controlled might be a biggest threat to individuals and their rights within the Metaverse (Heller & Bar-Zeev, 2021: 10; Wheeler, 2022: 8). Meta's headsets allow for tracking facial expressions and eye movement, detecting reactions which are too subtle for human beings to be aware of consciously (Rosenberg, 2022: 3). Some researchers warn against "a business model that is based on reselling user data to advertisers or reusing it for other commercial purposes, while access, functionality and algorithms are designed in such a way that people produce as much data as possible" (Hermann, 2022: 3).

What distinguishes the old-fashioned patterns of manipulation from sophisticated, technologically advanced solutions introduced within the Metaverse is "the ability to create high-speed feedback loops in which user behaviors and emotions are continuously fed into a controller that can adapt its influence in real-time to optimize persuasion" (Rosenberg, 2022: 5). Real-world politicians are not able to process data in this way themselves. Politicians boosted by artificial intelligence (AI) will be able to. One may wonder if these capacities are just a new type of marketing or if they are

better described as direct manipulation based on the unconditioned reactions of the body measured by sophisticated hardware and software; "the real harm to consumers comes from ongoing manipulation by unaccountable forces that knowingly use people's private sensitivities against them" (Heller & Bar-Zeev, 2021: 10).

The activity of political campaigns is one of many arenas that AI experts might follow. One may assume that data analysis could lead to the personalization of political messages adjusted to specific characteristics of voters. Such analysis could be based on algorithms measuring interactions, emotions, and interests in the virtual world(s). Such a scheme has already been used in marketing. The Metaverse, with its potential to gather information, could allow for "psychological and emotional manipulation of its users at a level unimaginable in today's media" (Waltzman, 2022). Eventually, two realities will become further intertwined in the Metaverse, "allowing for new organizational tactics and PsyOps campaigns" (Richardson, 2021) and for the exploitation of emotional weaknesses, including temporary mood swings of users that would increase susceptibility to specific messages.

The potential of the Metaverse can possibly complement other opportunities stemming from the use of AI in a political context. In 2022, during the presidential election in South Korea, one of the candidates decided to create his digital copy, altered by AI to increase his attractiveness among the young voters. The so called "deep fake" avatar might have been one of the reasons for his victory, which was achieved by a small margin (Shin & Yi, 2022). In one sense, the use of AI to increase the chance of winning an election is a brilliant idea, especially since such activities are not prohibited by law. The problem was the manipulation behind the election process. AI-generated videos presented a distorted picture of reality, giving a false perception of the candidate's abilities and performance to recipients. And that might be just the beginning, as the Metaverse would create more opportunities for these actions.

It should not be forgotten that many of the solutions presented here have positive applications, e.g., mimicry can be used to amplify messages while learning in VR. A simple procedure of focusing the teacher's avatar's gaze on a specific student was sufficient to improve attention and learning outcomes (Bailenson & Blascovich, 2011). However, democratic processes are based on equality, transparency, and participation. The potential for manipulation described above, and specifically the micro-targeting of voters (Hermann, 2022: 5), undermines the idea of democracy.

The Metaverse could also have an indirect impact on democratic processes through the gradual change of society and of social interactions. So-called cyberdemocracy has a range of possible dimensions, such as the transfer of some part of decision-making processes to cyberspace, the formation of new political movements within cyberspace, and pressure on authorities to allow cybervoting (Filipova, 2023: 10). It should not be assumed that MR will completely supplant the competition for votes in the real world, but the Metaverse should be considered a new forum for the struggle for electorate.

The democratization and decentralization of platforms that support the Metaverse represent both a new opportunity and a new challenge. The egalitarian nature of the system will lead to the emergence of new social and political movements, as well as changes in the form of existing ones and the creation of new leaders. Decentralized

digital societies would put more pressure on the importance of online identification, which might, in turn, lead to the emergence of new needs (e.g., purchasing virtual objects), the problem of verifying individual identity, increased health issues, and the degradation of moral values (Filipova, 2023: 9).

At the same time, presence in seemingly open environments, where the influx of information from the outside may be limited, can lead to the radicalization of the social masses. It is not difficult to foresee that the Metaverse will be an excellent platform for extremist movements, state and non-state actors, cybercrime, or terrorist organizations who may fully exploit the potential for disinformation, radicalization, or recruitment. On the other hand, the Metaverse might also be a form of escapism from the political problems of the real world, including climate change, air pollution, and the degradation of resources (Richardson, 2022). Looking for one's own identity outside of the unacceptable real world will inevitably lead to stronger immersion or a disruption of the capacity to assess conditions realistically, which in turn may result in attempts to look for a new group identity in the virtual world.

Information bubbles or echo chambers have negative consequences, which will themselves result in social polarization; immersion will play the role of a catalyst. In extreme cases, the complete blurring of boundaries in perceiving the real and semi-real worlds will make it impossible to distinguish political reality from the one created by MR. This phenomenon is nothing new. The aforementioned information bubbles and echo chambers are a significant social problem of contemporary social media (Cinelli, 2021: 1). The Metaverse, based on immersion, will be an even more effective source of manipulation in this regard, one resulting from being locked in a specific, often hermetic environment where the stimuli will be felt even more strongly due to sensory transmitters.

Social media is already described as "an effective amplifier to attract naïve youth to extremism" and to serve as a tool for radicalization (Liang, 2022: 74). Paradoxically, the decentralization of the Metaverse, which would allow for greater democratization of services and ensure increased anonymity of users, may lead to the mass dissemination of content that in a moderated environment could be caught and defined as inconsistent with regulations.

Recent progress in neuroscience would also have a direct impact on the Metaverse users. "Metaverses could substantially contribute to cognitive warfare aimed at leveraging, disrupting or influencing basic belief structures in adversaries (both civilian and military) in ways that digitally influence their physical behaviors." (Rickli & Mantellassi, 2022: 10–11). The idea of using the Metaverse as a cognitive warfare should be a source of interest to military experts. It has already been established that subliminal advertising and propaganda would contribute to disturbance of the sense of moral or political values since users might have a false impression that their identity is built on their beliefs, whereas, in fact, it has been gradually replaced by the algorithm's choices or manipulated content (Henz, 2022: 4).

Considering the above, the Metaverse could also create fertile ground for terrorism and extremism, allowing for selection and recruitment. Europol (2022) warns against imagined fictions of theoretically free worlds that do not comply with the basic rules

of democracy or the rule of law. Examples of Nazi gas chambers found in the quickly growing Metaverse called Roblox are extremely worrisome (Europol, 2022: 19). Two phenomena may possibly occur. The uncontrolled development of the decentralized Metaverse can lead to the undermining of basic democratic principles, whereas massive surveillance, intended to serve the business purposes of the platforms, could lead to the de-democratization of the Metaverse since such surveillance is inherently anti-democratic. "Centralized" democracy might be "subordinated to the governmental and corporate elites who control smart technologies and govern 'by code'. Outsourcing democratic resilience increases the power of the powerful elites, raising further concerns over accountability, representation, and transparency" (Bibri, 2022: 855).

Recommendations

1. Introducing the problem to lawmakers. Finding solutions requires first understanding the problem and its consequences. In some countries, the topic of the Metaverse has already appeared at the level of the parliamentary debate. This is a step in the right direction. Technological innovations require appropriate expertise, and parliamentary committees for digitization seem to be the adequate forum to discuss that subject.

The task of the experts is to create appropriate conditions for a professional debate, devoid of prejudices and excessive emotions. The Metaverse should not only be seen as a potential tool of manipulation or a source of cybercrime, although these threats must be fully acknowledged. Its basic applications need to be clearly identified to avoid a biased debate that would not serve a productive purpose. The familiarization of policy makers with the issues of the Metaverse is required for rational legislation. In sum, there is a need to "intellectually domesticate" the Metaverse.

2. Using already existing provisions. The emergence of new phenomena may trigger a natural desire to regulate them. This, in turn, may raise legitimate concerns about overregulation, which itself results in a fear of the new rather than a thorough discussion. However, before a new legal framework is created, it is necessary to verify to what extent existing solutions can be applied to the Metaverse. Many of the problems associated with the widespread use of the Metaverse have already appeared in social media. The list of potential crimes indicated in this study does not differ significantly from the current activities of cybercriminals. However, the Metaverse has the potential to multiply negative phenomena.

The opinion that the Metaverse in its current form is not fundamentally different from other existing forms of VR seems right, which in turn requires the authors of relevant laws to adjust the regulations. Lawmakers should take a proactive approach. They can directly and explicitly include the Metaverse within the scope of existing regulations. J. Jaursch (2022) rightly pointed out that the EU has already introduced the regulatory measures that should apply to the Metaverse. The Digital Services Act would have the potential to at least reduce the negative consequences of the Metaverses to minors or oblige the platforms to be more transparent with targeting, though it is still unknown how the rules would apply to all the Metaverses, especially in the case of decentralization.

3. Preparing long-term strategy and using strategic foresight. The debate on the application of regulations currently in existence is a precondition to concretizing legal provisions and directing them to cover the Metaverse. The possibility that they would take the form of a targeted legal act cannot be ruled out, although this is not an optimal solution for the next few years. However, if the Metaverse reaches the size some experts predict it will, it may require dedicated *lex specialis*. Thus, it is necessary to use strategic precautionary tools for the "anticipatory governance" of the Metaverse (Peters et al., 2022: 12). These tools would allow for the testing of existing regulations and their applicability to the Metaverse and the analysis of the scope of possible future legislation. The Metaverse might have a moment of weakness due to changing economic conditions or the potential financial problems of companies, but this does not necessarily mean that the idea of immersive reality will be completely abandoned by the tech industry. The Metaverse might return in a different incarnation.

In this context, the announcement of the European Commission to launch "a creative and interdisciplinary movement, aiming to develop standards, increase interoperability, maximizing impact with the help of IT experts, regulatory experts, citizens' organizations and youth" (European Commission, 2022) should be more than welcomed. These activities are complemented by the founding of the Virtual and Augmented Reality Industrial Coalition and the launching of the VR Media Lab through Horizon Europe.

R. Waltzman (2022) correctly points out the necessity of considering appropriate guardrails for new technologies to minimize potential harm. The comprehensive study and evaluation of psychological aspects of immersion, supplemented by the analysis of the potential use of malicious or manipulative tools, seem to be mandatory. They need to be merged with a thorough evaluation of the technological characteristics of the Metaverse. Waltzman's idea of developing a technology to detect when manipulation techniques are used—for example, by introducing "emotional canary" that would send warning signals to users once it detects the attempt at emotional manipulation-- seems to be hardly realistic, as the technical feasibility of this solution is arguable and might lead to preventive censorship or damage to the business dimension of the Metaverse.

4. A dual-track approach to cybercrime and manipulation. It is necessary to counteract cybercrime in the classical sense. This is a task not only for law enforcement authorities, but also for lawmakers, who should pass specific regulations regarding the activity of criminals in cyberspace. On the other hand, it is necessary to pay attention to the problem of how the collection and processing of data are used to manipulate users. In any case, it will be extremely difficult to draw the line between what is acceptable for marketing purposes and what constitutes illegal manipulation. Experts should focus on introducing clear and transparent rules for data processing. L. Rosenberg (2022) suggests restrictions regarding the monitoring of users, the emotional analysis of users, and product placement within the Metaverse, and even considers banning simulated personas (photorealistic human representations), although this type of regulation would need very specific, detailed provisions of law.

It is difficult to say unequivocally whether personalization and manipulation of a political nature should be regulated separately. Undoubtedly, the political dimension of the Metaverse should be the subject of careful analysis. Under certain conditions,

as indicated in this study, it poses a significant threat to democratic systems. At the same time, one should remember the positive political applications of the Metaverse, which, in the right form, could increase social participation and social interest in political matters.

Thus, the issue of using the Metaverse should be combined with the broader issue of using AI for political campaigns. Although, at first glance, political manipulation may seem more harmful to democracy than manipulation resulting directly from private corporate activity, the qualitative difference will be difficult to grasp. Experts in the field of electoral law should subject the use of new technologies and the implementation of far-reaching policies involving the personalization of political messages created by algorithms with limited human intervention to careful analysis. Even at this stage, determining the limit of what level of interference should be permitted will be extremely difficult, if not impossible.

The question of inter-connections between the Metaverse worlds and those of data migration has not yet been fully answered (Anderson, 2022). There is a need to better understand the interoperability processes to assess the capabilities of the platforms responsible for collecting and using personal data. In this context, close cooperation with the platforms themselves is necessary to propose appropriate countermeasures at early stages, including self-regulation, transparency regarding algorithms, the introduction of codes of conduct, and rules for the responsible use of AI.

5. Raising awareness, strengthening cyberliteracy, and contributing to online democracy. One of the reasons for the current state of unpreparedness is the lack of expertise. Apparently, "there are not enough qualified people to deal with the complexity of the architecture" of the Metaverse, which makes it even harder to develop security solutions (Dwivedi et al., 2022: 10). That lack of expertise covers diverse fields, from lawmakers, administration, law enforcement, sociologists, psychologists, to society itself.

In December 2022, experts invited by the Bundestag emphasized the need to raise awareness and intensify the debate on what the digital economy might look like in the future, the threats to fundamental rights and personal data associated with the expansion of VR, and how to counteract the expansion of cybercrime (Digital Committee of Bundestag, 2022). This type of parliamentary debate serves as an important tool for capacity building in the public sector. It is also a chance to flag significant social issues. Society must be included in the discussion about the threats stemming from the intensive use of the Metaverse and education on this topic should primarily be addressed to the younger generations, which in the future will be a key target for Metaverse platforms. Strengthening cyberliteracy is a comprehensive task for the modern education system.

Some proponents of the Metaverse argue that Web 3.0 will be based on decentralization and that the Metaverse should be democratically owned and controlled by global users (Grider & Maximo, 2021: 4). If such a scenario were to materialize – which seems unlikely at this stage, given the business potential of the Metaverse and the influence of powerful stakeholders – raising user awareness will be one of the key mechanisms to protect virtual communities from the erosion of democratic standards.

Education systems, universities, non-governmental organizations, and independent experts can all contribute to building social awareness and resilience, strengthening not only cyberliteracy but also the democratic values that should be introduced to the Metaverse communities.

6. A pro-active approach of law enforcement agencies and close cooperation with stakeholders. Law enforcement agencies and organizations can play a huge role in shaping the environment around and within the Metaverse. "Law enforcement needs to build experience in the Metaverse and should find a way to make use of these private experiences, as they provide invaluable insight to make sense of what is happening and accurately assess new developments" (Europol, 2022: 26). Thus, it is necessary to engage with users, the private sector, and developers of the Metaverse to truly understand the nature of this phenomenon.

Such involvement of law enforcement authorities is also in the interest of the stakeholders, including platforms, as they should care about the appropriate enforcement of regulations. If not, the uncontrolled development of the Metaverse might force the introduction of far-reaching countermeasures, resulting in overregulation.

Law enforcement agencies should enhance existing solutions, including capacity building through training and online activities, experience and intelligence sharing, investigative support, and the establishment of partnerships (Interpol, 2022). At the same time, a properly designed international framework "would promote inter-nation collaboration, facilitate crime investigation, and support democratic governance" (Qin, Wang, Hui, 2022: 2). Moreover, law enforcement agencies need to establish their permanent presence in the Metaverse to familiarize users with the very concept of online policing, while also counteracting the damaging perception of the apparent impunity of online activities.

The threats of radicalization, extremism and terrorism indicated in this study should become key elements of law enforcement activities in the Metaverse. It is essential to penetrate potentially anti-democratic and criminal communities, understand the mechanisms of interactions, and prevent the influx of new recruits. This work will require extensive energy, financial, and personal resources, but it must be a constant process of adapting to the growing environment of the virtual world.

7. Enhancing research in the fields of sociology and psychology. The negative trends presented in this study regarding the development of the Metaverse included sociological and psychological aspects. While one should not forget the positive applications of the Metaverse, such as those that contribute to medical treatment or education, experts express warnings about the detrimental effects of extensive use of the Metaverse and excessive immersion. These can result in the disruption of boundaries between the virtual and real world or addictions (Bojis, 2022: 4).

One may assume that "escapes in the Metaverse will affect social interactions as well as consumers' physical and psychological well-being. Inevitably, it will affect people's ability to cope and function in life" (Han et al., 2022: 1455). The list of harmful effects should be supplemented with Fear of Missing Out (FOMO), mood disorders, depression, or traumatization. Some researchers predict that the Metaverse would increase the number of mental health disorders, an outcome that "might even lead

to the identification and classification of new mental health illnesses" (Usmani et al., 2022: 4–5).

There is a need for further, thorough research with the goals of estimating risks and building a system to prevent the negative effects of immersion. As with the other recommendations, capacity building, raising awareness, and strengthening expertise are greatly needed. Immersion is not a new phenomenon. It has already been studied in the context of gaming, but the Metaverse seems to offer a new dimension of immersion. Its promised change in the form of social interactions will likely pose completely new challenges to sociology and psychology and may even require enforcing and strengthening existing standards.

Conclusions

The potential development of the Metaverse requires the interest and activity of state authorities on many levels, even if it does not reach the level expected by its proponents. The list of threats presented in this study is not exhaustive. Due to the limited scope of this research, this study focused on the most important issues regarding democratic processes, how they might be undermined through manipulation and how political campaigns may become based on excessive data gathering in the Metaverse. Documented patterns of cybercrime in the Metaverse replicate existing threats, whereas manipulation can take new, more dangerous forms.

Difficulties in foreseeing the potential range of the Metaverse prevent the prediction of the actual scale of threats to democracy. Therefore, threat assessment requires constant analysis, the observation of trends, and the establishment of a presence as preparation for understanding how the Metaverse works and how interactions inside the Metaverse are shaped. The activity, consistency, and creativity of lawmakers and law enforcement agencies are needed to constantly monitor the development of the Metaverse and its other incarnations and to respond adequately to new forms of crime and manipulation.

References

Anderson J., Rainie L. (2022). *The Metaverse in 2040*. Retrieved from: https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2022/06/PI_2022.06.30_Metaverse-Predictions_FINAL.pdf.

Anderson P. (2022). *How to let a metaverse die*. Retrieved from: https://www.polygon.com/23025632/metaverse-mmo-ending (28.01.2023).

Bailenson J.N. (2008). Facial similarity between voters and candidates caused influence. *Public Opinion Quarterly*, No 72(5). p. 935–961, doi.org/10.1093/poq/nfn064.

Bailenson J.N., Blascovich J. (2011). *Virtual Reality and Social Networks Will Be a Powerful Combination*. Retrieved from: https://stanfordvr.com/mm/2011/bailenson-ieee-vr-social.pdf (01.02.2023).

Bojis L. (2022). Metaverse through the prism of power and addiction: what will happen when the virtual world becomes more attractive than reality? *European Journal of Futures Research*, No 10(1), doi.org/10.1186/s40309-022-00208-4.

Büchel J., Klös H.-P. (2022). Metaverse: Hype oder "next big thing"? Potenziale und Erfolgsbedingungen. *IW-Report*, No 42.

Bundestag (2022). *Anhörung zum Web 3.0 und Metaverse*. Retrieved from: https://www.bundestag.de/ausschuesse/a23_digitales/Anhoerungen/921548–921548 (28.01.2023).

Center for Strategic Futures (2022). *Who We Are*. Retrieved from: https://www.csf.gov.sg/who-we-are (28.01.2023).

Cinelli M., Morales G.D.F., Galeazzi A., et al. (2021). The echo chamber effect on social media. *The Proceedings of the National Academy of Sciences*, No 118(9), doi.org/10.1073/pnas.202330111.

Cheong B.C. (2022). Avatars in the metaverse: potential legal issues and remedies. *International Cybersecurity Law Review,* No 3, p. 467–494., doi.org/10.1365/s43439-022-00056-9.

Chohan U.W. (2022). *Metaverse or Metacurse?* doi.org/10.2139/ssrn.4038770.

Choudhary L. (2022). *Why this Poll Strategist Thinks Metaverse can Change Political Campaigns*. Retrieved from: https://analyticsindiamag.com/why-this-political-strategist-thinks-metaverse-can-change-political-campaigns (28.01.2023).

Digital Committee of the Bundestag (Die 24. Sitzung des Ausschusses für Digitales) on 14.12.2022. *Web 3.0 und Metaverse*.

Dunn J. (2022). *Five ways the metaverse could transform British politics over the next five years*. Retrieved from: https://www.newstatesman.com/spotlight/public-sector-tech/2022/12/five-ways-metaverse-transform-british-politics-next-five-years (28.01.2023).

Duwe D., Busch M., Weissenberger-Eibl M.A. (2022). *Enabling the Metaverse. Whitepaper on international user preferences, business models and innovation processes in the metaverse*, Fraunhofer Institute for Systems and Innovation Research ISI, doi:10.24406/publica-220.

Dwivedi Y.K., Hughes L., Baabdullah A.M. et al. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, No 66, doi.org/10.1016/j.ijinfomgt.2022.102542.

European Commission (2022). *People, technologies & infrastructure – Europe's plan to thrive in the metaverse*. Statement/22/5525.

European Parliament (2022). *Metaverse. Opportunities, risks and policy implications*. European Parliamentary Research Service.

Europol (2022). *Policing in the metaverse: what law enforcement needs to know, an observatory report from the Europol Innovation Lab*. Publications Office of the European Union.

Filipova A.I. (2023). Creating the Metaverse: Consequences for Economy, Society, and Law. *Journal of Digital Technologies and Law*, No. 1(1), p. 7–32.

Giaglis G. et al. (2022). *Metaverse*. The European Union Blockchain Observatory & Forum.

Grider D., Maximo M. (2021). *The Metaverse*. Grayscale. Retrieved from: https://www.grayscale.com/research/reports/the-metaverse.

Han D.-I. D., Bergs Y., Moorhouse N. (2022). Virtual reality consumer experience escapes: preparing for the metaverse. *Virtual Reality*, No. 26, 1443–1458. doi.org/10.1007/s10055-022-00641-7.

Heller B., Bar-Zeev A. (2021). The Problems with Immersive Advertising: In AR/VR Nobody Knows You Are an Ad. *Journal of Online Trust and Safety*, Vol. 1 No. 1, doi.org/10.54501/jots.v1i1.21.

Henz P. (2022). The societal impact of the metaverse. *Discover Artificial Intelligence*, No. 2(19). doi.org/10.1007/s44163-022-00032-6.

Interpol (2022). *Technology Assessment Report on Metaverse*.

Interpol (2022). *INTERPOL launches first global police Metaverse*. Retrieved from: https://www.interpol.int/News-and-Events/News/2022/INTERPOL-launches-first-global-police-Metaverse (28.01.2023).

Jaursch J. (2022). *Der DSA wirkt auch "im Metaverse" – wenn es mit der Rechtsdurchsetzung klappt*. Stiftung Neue Verantwortung. Retrieved from: https://www.stiftung-nv.de/de/ publikation/gastbeitrag-der-dsa-wirkt-auch-im-metaverse-wenn-es-mit-der-rechtsdurchsetzung-klappt (28.01.2023).

Kabelka L. (2022). *European Commission turns its gaze towards the metaverse*. Retrieved from: https://www.euractiv.com/section/digital/news/european-commission-turns-its-gaze-towards-the-metaverse/ (28.01.2023).

Liang C.S. (2022). The Technology of Terror: from Dynamite to the Metaverse. *Global Terrorism Index*. Institute for Economics & Peace, p. 73–76.

Mystakidis S. (2022). Metaverse. *Encyclopedia*, No. 2(1). p. 486–497. doi.org/10.3390/encyclopedia2010031.

Park S.-M., Kim Y.-G. (2022). A Metaverse: Taxonomy, Components, Applications, and Open Challenges. *IEEE Access*, No. 10, p. 4209–4251, doi:10.1109/access.2021.3140175.

Peters R., Schmietow B., Krieger B. (2022). Zwischen Hype und Zukunftsthema: Auf dem Weg ins Metaverse? *iit-perspektive*, No. 62.

Pimentel D., Fauville G., Frazier K., et al. (2022). *An introduction to learning in the Metaverse*. Meridian Treehouse.

Qin H.X., Wang Y., Hui P. (2022). *Identity, Crimes, and Law Enforcement in the Metaverse*. doi.org/10.48550/arXiv.2210.06134.

Richardson D. (2021). *What will the Metaverse mean for political movements?* Retrieved from: https://paradoxpolitics.com/2021/12/what-will-the-metaverse-mean-for-political-movements (28.01.2023).

Rickli J.-M., Mantellassi F. (2022). Our Digital Future: The Security Implications of Metaverses. *Geneva Center for Security Policy*, Is. 24, p. 2–13.

Rosenberg L. (2022). *The Metaverse: from Marketing to Mind Control*. Future of Marketing Institute. Retrieved from: https://futureofmarketinginstitute.com/the-metaverse-from-marketing-to-mind-control (28.01.2023).

Rosenberg L. (2022). Regulation of the Metaverse: A Roadmap. *6th International Conference on Virtual and Augmented Reality Simulations (ICVARS 2022).* March 25–27, 2022 – Brisbane, Australia, p. 21–26, doi.org/10.1145/3546607.3546611.

Shin H., Yi H.Y. (2022). *South Korea candidates woo young voters with 'deepfakes', hair insurance*. Reuters. Retrieved from: https://www.reuters.com/world/asia-pacific/skorea-candidates-woo-young-voters-with-deepfakes-hair-insurance-2022-03-03/ (28.01.2023).

Usmani S.S., Sharath M., Mehendale M. (2022). Future of mental health in the metaverse. *General Psychiatry*, Vol. 35, Is. 4, doi.org/10.1136/gpsych-2022-100825.

Vishnoi S. (2021). *How the Metaverse Will Redefine Politics and Governments*. Retrieved from: https://www.thequint.com/voices/opinion/metaverse-and-politics#read-more (28.01.2023).

Waltzman R. (2022). *Facebook Misinformation Is Bad Enough. The Metaverse Will Be Worse*. Retrieved from: https://www.rand.org/blog/2022/08/facebook-misinformation-is-bad-enough-the-metaverse.html (28.01.2023).

Wang Y., Su Z., Zhang N., et al. (2022). A Survey on Metaverse: Fundamentals, Security, and Privacy. *IEEE Communications Surveys & Tutorials*, Vol. 25, Is. 1, doi.org/10.48550/arXiv.2203.02662.

Wheeler T. (2022). Who Will Make the Rules for the Metaverse? *Mossavar-Rahmani Center for Business & Government Associate Working Paper Series*, No. 195.

Whelan R., Flint J. (2023). *Disney Eliminates Its Metaverse Division as Part of Company's Layoffs Plan*. Retrieved from: https://www.wsj.com/articles/disney-eliminates-its-metaverse-division-as-part-of-companys-layoffs-plan-94b03650 (15.04.2023).

World Economic Forum (2022). *Defining and Building the Metaverse*. Retrieved from: https://initiatives.weforum.org/defining-and-building-the-metaverse/home (28.01.2023).

Xu M. Ng W.C., Lim W.Y.B., et al. (2022). *A Full Dive into Realizing the Edge-enabled Metaverse: Visions, Enabling Technologies, and Challenges*, doi.org/10.48550/arXiv.2203.05471.

Zhu L. (2022). *The Metaverse: Concepts and Issues for Congress*. Congressional Research Service (R47224).

Zitron E. (2022). *RIP Metaverse. An obituary for the latest fad to join the tech graveyard*. Retrieved from: https://www.businessinsider.com/metaverse-dead-obituary-facebook-mark-zuckerberg-tech-fad-ai-chatgpt-2023-5 (15.05.2023).

Author's bionote

Mateusz Łabuz – Career diplomat working for the Polish Ministry of Foreign Affairs; PhD candidate at the Chemnitz University of Technology (Germany); Lecturer of Cybersecurity at the University of the National Education Commission in Kraków (Poland). Member of numerous high-level delegations, representing Poland during international conferences and summits. Alumni of Körber Netzwerk Außenpolitik aimed for young foreign policymakers. Graduate of Law, Administration and English Philology faculties at the Jagiellonian University and the Pedagogical University of Cracow; graduate of the Diplomatic Academy of the Polish MFA. His research interests include modern technologies and their impact on security and democracy. Author of one of the biggest websites on the history of World War II (WarHist.pl).