



DATA PRIVACY AND SECURITY CHALLENGES IN METAVERSITIES: THE ETHICAL DILEMMAS IN THE FUTURE OF HIGHER EDUCATION

Nurten Gündüz, Mehmet Sincar

Gaziantep University, Türkiye

E-mail: nrtnutar@gmail.com, mehmetinsicar@yahoo.com

Abstract

Without regulations for higher education institutions in the metaverse, ethical transgressions are unavoidable. Educational metaverse systems, which integrate artificial intelligence, essentially depend on big data as their core technology, leading to considerable privacy issues. Therefore, this study examines data privacy and security issues, a sub-dimension of metavethics, and how a healthy, secure, and responsible metaverse can be shaped within higher education. The research group was formed using a maximum diversity and criterion sampling method based on purposive sampling approaches. Semi-structured interviews were conducted with 15 key faculty members who have a voice in the field of educational metaverse. The interview questions were prepared based on the relevant literature and conceptual framework. Some outstanding findings emphasized by the participants on the risks under data privacy and security in higher education are: the challenge of 3-dimensional data such as biological and behavioural data, algorithmic guidance, dependence on private companies in the educational metaverse, wearable technologies, loss of privacy, the danger of the disappearance of free will, loss of autonomy in higher education, personal data becoming a market material, and cyber-attacks on university systems.

Keywords: data privacy, metaverse, metaversity, metavethics, higher education, IPA

Introduction

The metaverse represents the culmination of the Internet's evolutionary trajectory. With the advent of blockchain technology, the Internet has now reached the brink of a digital transformation thanks to Web 3.0 technology, which establishes the framework for the development of three-dimensional virtual simulation environments and multidirectional interaction via avatar representations. Web 3.0 has made all the necessary infrastructure for the metaverse ready for today, as it is a structure that includes many advanced technologies such as mirror world, comprehensive visualisation, augmented reality, virtual reality, mixed reality, cloud application, artificial intelligence, big data, 3D visualisation, and blockchain.

The concept of the metaverse initially emerged in science fiction works such as 'Neuromancer' (Gibson, 1984) and 'Snow Crash' (Stephenson, 1992); hence, the science fiction of three decades ago has evolved into contemporary science. The metaverse has commenced its development of a hybrid universe and, by the 2020s, has prepared the requisite technology. The trials of brain-internet interfaces, regarded as a significant barrier to the transition to a hybrid metaverse, have been under development for numerous years (Dayarathna, 2022). In 2018, researchers at MIT developed a system enabling users to order pizza by transmitting messages to a computer solely through brain impulses, without any physical action. In the forthcoming years, it is projected that substantial information will be transmitted to robots without physical movement; for instance, a chip implanted in the human brain by 2025 is predicted to interpret

all commands processed by the mind (IEEE Standards Association, 2022). Lee, the former head of Google China (Lee & Quifan, 2021), predicted that by the 2030s, individuals who do not utilize XR lenses, which will replace phones and computers, will feel blind. Humanity is gravitating towards a hybrid metaverse encompassing all dimensions. In the imminent future, it could transition all sectors of activity, including education, healthcare, entertainment, and commerce, into the newly accessible metaverse. The metaverse encompasses significantly more than merely a virtual reality or virtual realm.

The term ‘metaversity’ refers to metaverse-based higher education institutions that emulate physical classroom environments and structures, digital campuses, and facilitate the experience of Extended Reality (XR) in educational settings, achieved by constructing digital twins of actual environments within virtual spaces (Hassanzadeh, 2022; Ruwodo et al., 2022; Sun et al., 2021; Sutikno & Aisyahrani, 2022). Sutikno and Aisyahrani (2022) have characterized the metaversity as an initial advancement in higher education towards a comprehensive global metaverse, perceiving it as a novel generation of universities where physical constraints are entirely abolished, instruction is tailored, and students attain more efficient and enduring learning through immersive XR technologies. The metaverse has the potential to immerse students globally in a unified learning environment, effectively converting the entire planet into a singular virtual classroom.

The metaverse and metaversities are no longer a speculation or a utopian thought; they have become a reality in higher education, with numerous educational institutions taking their first steps towards a global metaversity by creating digital twin campuses and bringing metaverse classrooms to life. The growing prevalence of digital twin campuses indicates that the metaverse is poised to become a mainstream component of higher education within the next decade, thereby integrating seamlessly into the educational experience of university students (Price & Rice, 2023). Numerous universities, including Stanford University, Lindenwood University, Fisk University, Morehouse College, West Virginia University, South Dakota State, the University of Kansas, and York University, are developing their digital twin campuses in the metaverse, while the Adventis Metaverse platform asserts it is the first institution to provide graduate education in the metaverse (Ko, 2021; Price & Price, 2023). The ramifications of this trend, initiated by numerous Western universities, might soon manifest globally and proliferate due to the policies of internationalisation and technological integration in higher education that have been prioritised by many universities worldwide in recent years.

In the near future, virtual reality campuses might supplant physical structures, digital resources could replace traditional books and instructional materials, personalized and application-oriented VR methodologies might replace conventional evaluation techniques, and avatars could take the place of students in classes. Eventually, similar to how the terms academia and madrasa (the term which was used for universities in Muslim countries) were supplanted by university, we might cease to refer to a higher education institution as a university in the metaverse era and might begin to designate it as a metaversity.

As universities progress towards the metaverse, the educational administrators leading this initiative will be the inaugural leaders to confront the potential hazards and vulnerabilities posed by this emerging technology, necessitating the formulation of strategic responses. Consequently, these educational institutions and their administrators must be adequately trained and equipped to confront the problems they will face. Nevertheless, research on the metaverse has predominantly concentrated on its educational benefits (Arbogast, 2019; Karadayı, 2022; Suh & Ahn, 2022) or the ethical dilemmas it poses for humanity (Briggle & Spence, 2008; Dayarathna, 2022; Fernandez & Hui, 2022; Kshetri, 2022; Li et al., 2022), failing to adequately explore the essential ethical challenges arising at the nexus of higher education, the metaverse, and ethics. In this setting, it is essential to undertake comprehensive studies to examine these challenges, cultivate a robust metaverse in education, and foster a forward-thinking perspective.

Research Focus and Aim

Numerous scholars have concurred on the potential devastation that an unregulated metaverse era, devoid of principles, values, and ethical standards, could inflict upon humanity (Dayarathna, 2022; Kaddoura & Al Hussein, 2023; Kshetri, 2022; Li et al., 2022; Zallio & Clarkson, 2022, 2023). Consequent to these deliberations, two researchers from the University of Cambridge, Zallio and Clarkson (2022), have undertaken a novel research to delineate the ethical codes and principles governing the metaverse, following consultations with specialists from leading technology firms including Meta, Google, HTC, and Panasonic, who are proficient in the core technological domains underpinning the metaverse, such as augmented reality (AR), virtual reality (VR), and mixed reality (MR). Following their research, they have introduced the notion of metavethics, defined by the construction of a healthy and responsible metaverse grounded in moral principles, as an innovative and specialized multidisciplinary domain (Zallio & Clarkson, 2023). This study has introduced the term “metavethics” for the first time, establishing a new domain of applied ethics. The authors have asserted that metavethics concentrates on human behaviours associated with the metaverse, highlighting that a primary concern of this emerging discipline is the degree to which the metaverse can establish a dependable, equitable, libertarian, inclusive, accessible, ethical, and transparent virtual environment for individuals.

The ability of higher education institutions to navigate potential crises instigated by the metaverse effectively hinges on their proficiency in assessing prospective threats and ethical dilemmas, as well as their capability to formulate novel regulations and robust policies for the educational metaverse. Consequently, owing to its status as a nascent subject, there exists a pressing demand for metavethics studies in higher education, which are hardly found in the literature. This emerging discipline can furnish essential data and present an innovative perspective in order to enlighten higher education administrators, facilitating the design and management of universities within a healthy, safe, and ethical framework in the metaverse era. Higher education institutions and their leaders must proactively adapt to the swift societal changes and ground their philosophy in the ongoing evolution of the university to fulfil the requirements of the contemporary world (Barnett, 2017). Educational leaders must consistently prioritize the development of higher education through a more ethics-centred framework at every phase of this continuous transformation process. The administrative duties of higher education include the establishment and assessment of ethics-oriented organizational frameworks, along with the identification and resolution of ethical dilemmas and issues (Karsantuk & Çetin, 2020). In this context, higher education administrators must urgently address the ethical risks associated with the emergence of the metaverse in universities globally and the requisite preparations within the realm of metavethics before stepping into an irreversible process.

However, studies on the metaverse have focused either on the advantages it could provide in the educational dimension or on the ethical challenges it would lead to humanity in general, and have not sufficiently addressed the fundamental ethical problems to be encountered at the intersection of higher education, metaverse, and ethics. In this context, deeper studies are needed to analyze what these problems are, to shape a healthy metaverse, and to develop a future-oriented understanding. This study aimed to examine the aspects of data privacy and security problems and necessary precautions, a sub-dimension of the metavethics, inside higher education.

In line with this purpose, the research sought answers to the following questions. In the data security and privacy dimension of the metaverse in higher education:

- (a) What kind of problems is it deemed to pose?
- (b) How can a healthy metaverse in higher education be constructed in these contexts?

This study, which aimed to obtain the opinions of field experts who are at the forefront

of the process of integrating the metaverse with education, is hoped to make an important contribution to the field in terms of the effectiveness and health of the organisational innovation process, ensuring that our education administrators are not caught off guard in this process. Rather than focusing on merely the opportunities and conveniences offered by the metaverse in educational applications from a utopian perspective, this study targeted to conduct in-depth research on possible digital dystopian scenarios to protect students' digital security and health, to provide a clear picture of the ethical issues that education practitioners and administrators may encounter, and to take the necessary precautions in the new digital formation process. Hence, it is considered to be of critical importance.

Research Methodology

Approach

The interpretive phenomenological design, derived from a cognitive-focused approach and social cognitive paradigm (Brocki & Warden, 2006; Fıncıoğulları, 2016; Smith, 2011), has been determined as a research design. It is believed to be appropriate for searching phenomena that are recognized yet not thoroughly comprehended. In interpretive phenomenology studies, the researcher emphasizes the creation of a comprehensive, inquisitive framework rather than validating or invalidating pre-established hypotheses, thereby facilitating further discourse in subsequent research on the phenomenon (Seggie & Bayyurt, 2015). The interpretive phenomenological design is based on hermeneutics, ideography, and phenomenology, concentrating on how individuals comprehend a phenomenon (Smith, 2011). The aspect that reinforces this pattern, despite contradicting the positivist viewpoint, is its facilitation of flexible research opportunities in emerging fields while allowing for the utilization of existing theoretical frameworks without attempting to prove theories (Brocki & Warden, 2006). Consequently, the interpretive phenomenological design is deemed congruent with the research nature. Within the scope of the research, the views of experts on data privacy and security, which is one of the five basic dimensions of metavethics, were taken, and the perspectives of the competent names that shape the future of the metaverse were reflected.

The Study Group

The research group was established employing maximum diversity and a criterion sampling approach derived from purposive sampling techniques. In this study, to provide various perspectives and a broader, deeper, and richer viewpoint, it was desired that the participants' intersection points are their academic identity and higher education experience, as well as being notable representatives in their respective fields. In both scientific and technological domains, including XR technologies, VR/AR engineering, and artificial intelligence and data engineering, as well as in the humanities, encompassing cyber health specialists from psychology and metaverse and artificial intelligence ethics experts from philosophy, efforts were made to establish an exemplary representative group comprising academics and professionals engaged in metaverse research.

The criterion sampling technique is another method employed in identifying the research group. The criterion established was that faculty members engaged in the study group must possess a minimum of five years of higher education experience and be considered experts in Web 3.0 technologies and the metaverse. The philosophical grounds of the research are grounded in authoritative knowledge (Kivunja & Kuyuni, 2017). The participants in the study, recognized as some of the few proficient individuals in the metaverse domain, constitute an expert team with diverse positions in cyber health, educational metaverse, hybrid learning, cybersecurity, and cyber ethics, alongside their academic identities. Owing to the limited pool

of specialists in this nascent domain and the challenges associated with locating and engaging these individuals, an extensive online search was undertaken to connect with prominent players in the realms of metaverse and ethics. The participants were subsequently contacted through personal email addresses or LinkedIn accounts to ascertain their willingness to engage in the study. The demographic information of the participants is illustrated in Table 1.

Table 1
Demographic Information of the Experts Participating in the Study

Code	Expertise	Role	Experience (Years)	Sex	Country
p1	Electronic & communication technologies, 3D modelling	Technology entrepreneur / Metaverse consultant	15	Male	Türkiye
p2	Software, 3D modelling,	Metaverse platform project manager	9	Male	Türkiye
p3	Educational metaverse & AI	Educational metaverse trainer/ consultant / Educational metaverse platform manager	18	Female	USA
p4	Virtual reality, blockchain & NFT	Metaverse, blockchain and NFT consultant	8	Male	Türkiye
p5	VR & AI	VR technology entrepreneur/ consultant	10	Male	USA
p6	Software, 3D modelling, VR & AR	Metaverse platform project manager	10	Male	Türkiye
p7	Computer ethics & moral philosophy & Artificial intelligence and metaverse ethics	Metaverse and AI ethics trainer/ consultant	12	Female	Spain
p8	Data visualization, data & metaverse ethics	Data visualization trainer/ consultant in AR/VR, metaverse	8	Female	France
p9	Digital health & bioethics	Metaverse entrepreneur/ Founding director of digital health company	9	Male	USA
p10	Health metaverse & artificial intelligence, humanism and futurism in the metaverse	Founding director of a digital health company/ Digital health consultant/trainer at Metaverse/ Digitalisation humanist and activist	30	Male	Sweden
p11	Cyber health & cyber psychology	Cyber psychology trainer/ counsellor	28	Male	Türkiye
p12	Distance education & metaverse technologies	Metaverse consultant/ Commercial metaverse platform developer	32	Male	Türkiye
p13	Educational metaverse, game design, AI & XR	Artificial intelligence integration project consultant / Campus XR lab founder	23	Male	USA
p14	Post-humanism, context engineering, embodied consciousness & hybrid technologies	Trainer/consultant on post-humanism and hybrid technologies	19	Male	England
p15	Cyber security and privacy, metaverse law & corporate information technology management	Metaverse law trainer/consultant	21	Male	Sri Lanka

Data Collection Tools and Procedure

This study developed a semi-structured interview technique addressing data privacy and security, a critical component of the five fundamental characteristics of metavethics, based on the conceptual framework established by Zallio and Clarkson (2022; 2023). The interview questions were written and subsequently given to four professionals for review and guidance, including two XR specialists, a higher education authority, and a language expert.

The interview instrument consists of 37 questions in total, 12 main questions and 25 probes. The questions in the interview protocol were centred on topics such as the challenges of 3D data, the avatar crisis, private life, algorithmic manipulations, cyber-attacks, and data security, drawing on relevant literature. Interviews were conducted to explore the expected problems and potential solutions for higher education.

Throughout the data gathering process, the date, time, and location of the interviews were coordinated with the voluntary participants, and the interviews were recorded to prevent any loss of data following the participants' consent. The collection of all data was conducted over a relatively long period of 6-7 months in the years 2023-2024, especially as some participants were difficult to reach and appointments were difficult to make. The majority of the interviews were performed by Zoom, typically lasting one to two hours. The total length of data obtained from the video interviews with 15 participants was calculated as 203 pages and 1143 minutes in total.

Data Analysis

The NVivo14 qualitative data analysis software was employed for descriptive frame coding and thematic content analysis of the data. In the initial stages, deductive descriptive analysis was applied because a conceptual framework for the metavethic codes and the main categories was already in place. Meta-theoretical codes served as the conceptual framework and primary categories. In this deductive analysis phase, the data was segmented into sentences and paragraphs exhibiting semantic coherence, based on similarities and differences, and it was subsequently organized under the principal themes and categories outlined at the study's inception.

Following deductive frame coding, inductive thematic analysis was applied to the coded data for content analysis, and illustrative quotes were selected (Kynge, 2020; Mayring, 2014). Thematic content analysis was shaped by reviewing the relationships and causal links between the codes formed under the main categories and by creating subcategories and codes based on the scope of the relevant literature. During both descriptive and content analysis, the analyst persistently poses various generating inquiries, continually engages in theoretical comparisons, and systematically conceptualises existing codes utilising analytical instruments (Moghaddam, 2006; Williams & Moser, 2019). The content analysis approach in the study was informed by a thorough examination of the links and causal connections among codes, with the development of subcategories and codes grounded in the pertinent literature. The thematic encoding procedure resulted in the creation of themes by basing the relationships between the codes in a dynamic, cyclical, and non-linear process, on the extent of pertinent material (Williams & Moser, 2019). Applying thematic content analysis facilitated the creation of new categories and themes, thereby establishing new theoretical underpinnings in metavethics because while the deductive reasoning approach is considered an important strategy for testing the accuracy and validity of existing theories and categories, and for continuously reviewing and re-evaluating them, the inductive approach is important for explaining research findings, establishing causal relationships and forming new theoretical foundations (Williams & Moser, 2019).

Validity and Reliability

In this study, interviews were conducted with participants for an average of 1 to 2 hours, while some interviews were conducted over a longer period, such as 2.5-3 hours. The fact that the total duration of the interviews conducted throughout the research was 1143 minutes is among the indicators that strengthen the credibility of the study. Starting from the development of the data collection tool, expert opinions were used intermittently during the data analysis and interpretation of the findings to strengthen the credibility of the study.

Although a completely objective perspective is neither realistic nor possible in qualitative research, a research process in which the researcher's own assumptions and perspectives are minimized is considered important in terms of the confirmability and validity of the study (Fraenkel & Wallen, 2008; Glesne, 2015; Miles & Huberman, 1994; Patton, 2014). Therefore, during the interviews with the participants, the researcher took care not to reflect their own thoughts in the process, to be a good listener, and to ensure that the flow of the interviews was controlled by the participants and that they could express their thoughts freely, without hindrance or guidance.

The factors that strengthen the transferability and external validity of this study include the fact that a sample group that serves the purpose of the research was determined by using maximum variation and criterion sampling methods among purposive sampling methods, the opinions of competent names representing authoritative knowledge in the context of the subject (Kivunja & Kuyuni, 2017), and the diversification of the sample group in order to reveal different perspectives and avoiding a uniform perspective (Hammarberg et al., 2016; Lincoln & Guba, 1986). As proof that qualitative studies are reliable and consistent, the relevant statements of the participants were directly quoted in the findings section to increase consistency and trustworthiness (Lincoln & Guba, 1986; Miles & Huberman, 1994; Polit & Beck, 2012; Sandelowski, 1995). Concurrently, inter-coder reliability studies (Silverman, 2009) were conducted throughout the research by consistently comparing the acquired data with one another dynamically and clinically.

Research Results

Participants emphasized that, without necessary precautions within an ethical framework, metaverse applications in higher education could pose serious risks and threats to data privacy and big data. The results, covering the risks to data privacy and security in higher education derived from the research, along with the essential actions to cultivate a healthy and responsible educational metaverse, are illustrated in Table 2.

Table 2
Risks & Precautions for Data Privacy and Security in Higher Education Institutions

Risks	Precautions
Biological data and behavioural data problem	Double-factor encryption system
Threat to the assessment and management system	Establishment of pilot universities and error detection
Domestic cyber-attacks	Distinguishing between biometric data for authentication and identification
Environmental data problem	Virtual footprint tracking
Metaverse and artificial intelligence's power to transform into gods	Legislation for the students to protect themselves
Employees of private companies can use the data	Avoiding monolithization in educational metaverse platforms
The mechanization/slavery of man	Enclosed platforms
Possible attacks on servers	Modified data privacy statements in the law
Inadequacy of state institutions and dependence on private companies	High-level security measures for servers
Mentality for humans, despite humans	Preference for more secure equipment
Forged / fake data	Choosing the platforms that guarantee data privacy
The possibility of universities selling the data	Avoiding intermediary companies
Personal data being market material	Physical servers instead of virtual servers
Tracking thoughts and feelings	Use of blockchain technology
	Metaverse regulation at universities
	Data control to platforms
	More qualified white hat software developers
	Strong contracts to be made with hardware service providers on data privacy
	Qualified software, modelling and IT support team for universities
	Web 3.0 piracy defence training in legal education
	High biological encryption techniques such as palm identification, retinal reading
	Training of system operators and managers
	Platforms with transparent data processing and storage policies
	Supporting metaverse security experts

The findings suggested that the Web 3.0 technology underlying the metaverse, along with the necessary hardware, would exacerbate data security and privacy vulnerabilities. As some participants asserted:

Imagine that all of these things — pads, helmets, wearable clothes that can control you down to your nerve cells — are worn by your students. How can you prevent the identity, the personal data, and habits of these students from becoming a global market material? (p1).

It will track your body movements and head movements and record your behavioural data when you turn your head left or right. It will also track your biometric data with the VR headset. No privacy, no private life (p. 13).

When you have data, it always means information, especially personal data, which is considered high-level. (...) We are discussing a system that allows you to record your preferences, habits, feelings, and emotions. Imagine an academician collecting the data of thousands of students for 10 years and then using it for marketing (p. 14).

Accordingly, P3 expressed the drawbacks of VR headsets for data collection as follows.

The data problem is more of a problem with VR headsets. (...) So identification should be for authentication, not identification. After 5 minutes, it becomes clear that Meta can identify your

personality using the biometric data and other information it collects. And we know that when you wear VR headsets, Meta also collects information about your environment. What else, though, does Meta collect? (P3)

Participants in the study stated that it is up to us humans to create a good or bad metaverse in higher education and that it is possible to create a metaverse that is more secure than Web 2.0 technologies, where privacy is more prominent and personal data can be better protected. P5 emphasized that with Web 3.0 technology, it is easier to track people's digital footprints, and so even simple security problems can be easily prevented.

In the metaverse environment, you have a digital footprint that is tracked. A user can be blocked at any time. So we are actually under more control there. (...) In the Metaverse, there will be monitoring mechanisms that control the digital footprints of such people (P5).

P4 suggested that universities draw inspiration from high-security institutions, such as banks, when establishing the metaverse's security system. This could include applications like double-layer verification and sending a confirmation code to the mobile phone.

In the context of cybersecurity, you can attack from so many places, but at the same time, the system needs to protect itself. Just as white hat security experts now protect banking systems, universities also need to develop similar measures (P4).

Similarly, P2 and P12 stated that biological encryption methods, such as palm scanning and retina reading, are a necessary method for secure access to the metaverse.

To be able to read the eye retina of the person and log in by getting the password from there. If the system is accessed without doing this, the system should immediately recognize this as a threat. (...) The person who commits the theft inevitably wears those glasses (P2).

There will be security problems, but unlike the current 2D Internet, features such as palm identification and retina reading can be added to reduce security problems (P12).

P3, P9, and P12 stated that the selected platforms, service provider companies, and the agreements made with these companies are important for ensuring security and emphasized that agreements should be made with transparent companies with strict security measures. Besides, all participants strongly supported that the metaverse infrastructure used in higher education institutions has to be based on blockchain. Some of the participant statements in this context are as follows.

It must ensure this through contracts with private companies and service providers. If they process data outside of this, the same penalties are imposed on them. (...) It puts its entire infrastructure in front of them. (...) Confidentiality must be ensured to the fullest extent (P9).

In the metaverse, the blockchain is an application that is currently quite costly, but it will become cheaper. Once it becomes cheaper, it will be able to transform the Internet into secure environments that are potentially 1000 to 10,000 times more secure than the current 2-dimensional Internet (P3).

In the Metaverse, there are safeguards against data theft. We call it blockchain technology. In the blockchain, the data is very robust. The data is stored in pieces, divided into parts. (...) It will make it extremely difficult for attackers. (...) (P12).

Discussion

The research findings have raised some concerns regarding data privacy and confidentiality in higher education. Among these, the most prominent risks include the recording of behavioural

data, character traits, cognitive data, interests, identification information, and even conversations and body movements of students and faculty members by AI-based metaverse platforms to provide personalized education and training scenarios. Moreover, wearable technologies like VR headsets and haptic sensors which are essential for engaging with the metaverse, can gather biological data including heart rates, brain waves, retinal information, blood pressure, and hormone levels (Dayarathna, 2022; Smith et al., 2023), in addition to environmental data about the surroundings, encompassing details about nearby objects and individuals. The challenge of big data generated from the sensitive information collected by the metaverse has been a central focus of metaverse research in recent years, with scholars investigating potential risks and alternative solutions (Datta et al., 2018; Dayarathna, 2022; Park & Kim, 2022; Rawal et al., 2022; Rich et al., 2019). Park and Kim (2022) are critical of metaverse platforms because they track users' behaviour, conversations, and movements, often without individuals even realising they are being monitored. Likewise, wearable technology provides specific risks to the privacy and security of students and faculty in higher education. Embedded sensors in VR headsets provide direct internet connectivity, enabling access to diverse biological data, including individuals' location, brain waves, mental health, heart rate, and physical activity (Datta et al., 2018; Rich et al., 2019). This circumstance indicates that in higher education, any malicious individual with easy access to this data could endanger students or faculty members. To put the matter much more simply, even ordinary conflicts between students and lecturers can have disastrous consequences if one side obtains the location, identity, and biological data of the other.

The foundational technology of the metaverse relies on the perpetual record-keeping of all actions, personal information, social interactions, biometric data, and behavioural metrics occurring within these digital environments, regardless of location, time, or social standing; in essence, educational metaverse platforms depend on big data for their technologies, and these platforms will acquire a volume and diversity of data unprecedented in prior technologies, facilitated by the core Web 3.0 technology of the metaverse (Joye, 2016; Li et al., 2022; Zallio & Clarkson, 2023).

Certain commercial enterprises developing educational metaverse platforms lack safeguards to prevent employees from exploiting or selling this data, which poses a serious risk. In line with this argument, academic institutions in the metaverse era should consider intellectual property and privacy issues as critical concerns. In the foreseeable future, data security and privacy may significantly influence even individuals' university choices.

From the perspective of higher education, the metadata problem can fundamentally be analyzed under two risk categories. The first issue is the privacy and confidentiality of personalized data in higher education, and the second is the issue of data security. The main corridor that gives rise to both problems is the delivery of dangerously large amounts of data obtained through Web 3.0 to artificial intelligence and AI-supported platforms.

The necessity of a metavethics framework in the context of data privacy and security in higher education might be felt even more acutely with the widespread use of educational metaverse platforms. It is necessary to follow not only which data is collected through these metaverse systems but also where this data goes and how it is used. The collection of biometric and physiological data generates information about user neural activity, which requires a framework of rights to support ethical use and prevent abuse (Smith et al., 2023). Suppose we lack mental privacy and biological privacy. In that case, some of the new technologies can essentially read our minds, model our identities, reach contextually relevant conclusions, and then nudge our behaviours to the point of undermining our intentional actions (Takahashi, 2021).

Since the metaverse offers advanced and personalized experiences, the necessity of using private data arises, and users are generally unaware of the types of data they provide to

the system; for example, a twenty-minute virtual reality headset experience is considered to provide approximately 2 million data points from a person's body language, head and hand movements, facial expressions, and behavioural characteristics related to both mental and physical health (Saraçoğlu, 2022). However, there are no security or privacy policies for the metaverse in higher education.

Understanding how big data is commonly used to guide individuals and organize crowds through algorithms in our daily lives will allow us to see its impact on shaping our existence and the potential risks if the metaverse is seized by biased channels more clearly. The function of the metaverse is primarily to calculate, maintain, and regulate, to record users' footprints, to determine directions, to specify time and space, and to create data indices (Rawal et al., 2022). According to Rawal et al., the ubiquitous smart algorithms in the metaverse possess simplified autonomy, that is, action autonomy, while designers overlook ethical autonomy during the program design process. In complex events, algorithms weaken causal thinking, and excessive correlation thinking is adopted. This raises the question of whether individuals and, subsequently, institutions will have free will and ethical autonomy in the era of the metaverse shaping higher education.

Research findings also suggest that the metaverse could make higher education institutions vulnerable to data attacks and data theft. Cyber-attacks on data in the metaverse can take many forms, such as malware, ransomware, identity fraud, copyright infringement, and data theft or breaches (Saraçoğlu, 2022). In the 2020s, as we transitioned to Web 3.0, the scale of cyber-attacks began to increase significantly; for example, the rate of attacks on corporate networks in 2021 was recorded to have increased by 50% compared to 2020. If this trend continues, it is expected that the financial damage caused by ransomware to institutions will reach 265 billion dollars by 2031, and it is anticipated that ransomware attacks, which occurred every 10 seconds in 2021, will happen every 2 seconds by 2031 (Check Point, 2022). How higher education institutions can protect their structures and manage potential financial damages against the intensity of ransomware attacks, which even affect large-scale private institutions with high budgets and high security, is another topic of discussion.

In the current situation, many world universities lack the necessary infrastructure, equipment, knowledge, experts, technical staff, and, most critically, the budget to maintain control over data security and provide a strong defence and safety environment against cyber-attacks. This could make metaverse universities vulnerable to various data attacks such as phishing, ransomware, and avatar hacking. Higher education institutions affected by these attacks may suffer not only financial losses but also damage to their reputation.

As technology steps forward, it not only makes the work of white-hat software developers easier, but also black-hat, malicious software developers are now developing more sophisticated cyber-attack methods, which increases concerns about data security. While the cost of data breaches in 2021 alone was 4.24 million dollars, the total cost of data breach incidents worldwide has exceeded 40 billion dollars; on the other hand, the expenses incurred by institutions for data security and risk management, which reached 133 billion dollars as of 2021, are expected to reach 223 billion by 2026 (Saraçoğlu, 2022). In the Metaverse era, higher education institutions might also need Web 3.0 data security experts and high-cost security software to protect the data that has dramatically increased both qualitatively and quantitatively. In this period, the importance of data security might increase compared to the Web 1.0 and Web 2.0 periods of the Internet, and it might be necessary to employ more qualified cybersecurity experts in universities. Surveys on the future of cybersecurity show that as public and private organisations adopt new technologies based on XR and artificial intelligence, the most important competencies for organisations in the years following 2021 are enhanced enterprise cybersecurity and data privacy (Deloitte, 2022).

The invisible widening of the digital competence gap between students and teachers may also cause many problems in the teaching process, such as distortion of data, intrusion of strangers, and spread of violence, illegal information, and teachers' great difficulty in classroom management. Predicting the winner of the data management race between the younger generation, which has been introduced to Web 3.0 through games since infancy, and a generation that is likely to be involved in the metaverse and Web 3.0 in adulthood or maturity is not tricky. Lecturers need to be trained in both the educational metaverse and data security in order to protect their own data and the data of their students in the classroom. However, universities lack even the technical staff to provide Web 3.0-based data security in their institutions and to train their lecturers.

All participants in the study agreed that a higher education institution in the metaverse should be based on blockchain and decentralized internet infrastructure. They noted that the attempt to continue the Web 2.0-based centralized internet structure would carry many issues to the metaverse, as data stored on fixed servers is vulnerable to cyber-attacks and cannot ensure data privacy and confidentiality. However, under current conditions, some platforms established under the name of the metaverse, including applications like Meta's Horizon, continue their attempts to keep data on their centralized servers, and it is believed that these efforts are a result of their attempts to hold onto big data, which is considered the new oil, in other words, capital (Kaya, 2022). These large-budget companies can make massive investments in educational metaverse platforms to retain data and ensure that the services they offer are of higher quality than those of other low-budget platforms. This situation could also influence universities' preferences for platforms, leading them to adopt the products of these giant companies for better services. This poses a significant risk to higher education, as the popularity of these companies in the educational metaverse means they will hold the data of all students, educators, and staff participating in this system worldwide. This also raises concerns about concepts such as privacy, security, transparency, free will, and autonomy.

Despite these increasing cyber threats, research findings suggest that the metaverse could rapidly gain popularity as a specialized and safe place for the digital world, as the use of blockchain and decentralized internet makes fraud and other concerns much more difficult to establish and spread (Clemens, 2022). Blockchain technology is defined as a decentralized, immutable, highly secure, and transparent ledger where data is encrypted in real-time over the internet in a distributed structure and stored in blocks, with each block forming a chain structure with the previous and the following data (Kim et al., 2020; Kahraman, 2022). In the blockchain architecture, each user is part of a network node, data is encrypted in a distributed manner, and verified by every user participating in the system (Kahraman, 2022). In this way, a more secure and transparent internet is provided, and since the data is not stored in a single place, on a single server, measures are taken not only against cyber attacks that may come from outside, but also against data theft that may occur from within. In other words, the ethical risk of a private company holding all your data and selling it to an advertising company at will, as seen in the examples of Facebook and Instagram, is eliminated, resulting in a decentralized and robust internet environment.

A direr scenario is that the institutions steering the metaverse in higher education will not be leading educational organizations but giant technology companies driven by capital, posing a threat that could plunge the entire higher education system into chaos. Therefore, it is an ethical imperative for higher education organizations to be at the command centre and steer the ship of the educational metaverse. The most important element that should not be ignored at every stage of this continuous transformation process is to move higher education to a more humanistic and more ethical position at every step and to be shaped in this manner. The formation and analysis of ethics-centred organizational structures in higher education, and the identification of problems and solutions to ethical contradictions and difficulties, are considered

within the scope of the administrative tasks of higher education (Karsantık & Çetin, 2020). In this context, the ethical discussions and analyses of the educational metaverse structures that are being shaped in universities should be included in the agendas and focus of interest of higher education administrators before entering a process that cannot be changed or reversed.

Digital capitalism might create a more pronounced divide between the affluent and the impoverished in the metaverse. In other words, in virtual reality, the inequality in reality will expand infinitely (Kaddoura & Al Hussein, 2023). If we allow digital capitalism to permeate education, considering its historical success and undeniable influence on contemporary educational institutions, it is highly possible that its offspring, digital capitalism, will do the same; the metaverse will inevitably permeate the hypothetical inequalities and injustices of the physical world into higher education as more profound human crises.

For all these reasons, universities seeking to integrate into the metaverse should prioritize data security and privacy for their students and faculty, and opt for metaverse platforms that utilize decentralized Internet and blockchain technologies. Blockchain is particularly essential for institutions and organizations with high data density, such as universities, because even if they are subjected to cyber-attacks, the data on the blockchain network will never be lost and will remain accessible. Especially, certificates like diplomas must be kept in distributed ledgers with blockchain assurance.

According to the findings, in addition to blockchain technology, other methods for ensuring security in educational metaverse platforms for universities include the necessity of transitioning to a two-factor authentication system for data security and the use of biometric encryption techniques such as palm verification and retina scanning for system access. When accessing a university in the metaverse, requiring dual-factor authentication rather than just a username and password—meaning that entering our email password alone is insufficient and a code must also be sent to our mobile phone—could somewhat hinder malicious computer experts from easily achieving their objectives. On the other hand, measures must be taken to confirm that university students' digital identities and avatars belong to them. The most reliable measure for this is biological verification. Cameras can also be enabled on platforms, and facial recognition can be performed using artificial intelligence. Although most current glasses do not have this feature, retina scanning can be added to glasses with a simple application. Research data supports the necessity of using metamask for biological identity verification, especially in the educational metaverse, for security concerns.

In metaverse universities, the use of biological passwords will significantly facilitate the identification of the real identity of the avatar entering the system, but there is also a risk that these biometric data could be compromised. At this point, the experts involved in the research emphasized that a distinction must be made between biometric data used for identity verification and biometric data used for identification and information collection. They emphasized that biological data should be used solely to verify the identities of students and faculty members and should not be used to collect information.

Another crucial step that must be taken without delay for data privacy and security in higher education is the enactment of necessary laws, regulations, and relevant legislation. For regulations at the higher education level, university administrators, and national laws, state officials should collaborate with system implementers, field experts, and metaverse service providers to determine the sanctions for data theft, distortion, modification, and sale to private entities. The current international laws and regulations established on Web 2.0 technology allow companies holding data to store, share, sell, and claim rights over the data based on contracts made between institutions, individuals, and companies (Ateş, 2021). This is a sensitive issue with critically important threats that must be reviewed in the metaverse age, where data is more valuable than oil and money, more dangerous than nuclear and weapons. It is essential to reorganize legal frameworks and regulations within the framework of the metaverse.

However, making regulations in higher education within the framework of metaverse ethics is not as easy as making regulations in physical universities. The ambiguous aspect of virtual reality is directly related to the confusion in the moral debate surrounding the metaverse. In other words, creating ethical guidelines and regulations for the metaverse is difficult since determining its reality status is difficult. Moreover, even if the necessary ethical regulations are made, since individuals' perceptions of morality in an online environment are not equivalent to their perceptions of morality in a physical environment, their tendency to comply with these rules might also change, and their inclination to behave without rules and limits in metaversal environments might be much higher. The findings suggest that students and even instructors are more likely to engage in disruptive and socially inappropriate behaviour in virtual classrooms, as anonymous users use their avatars as a means to hide their true identities behind the pixels. Individuals tend to feel less responsible and guilty for unethical behaviour on metaverse platforms than in real life. In line with the findings, because anonymous individuals utilize their avatars to conceal their genuine identities behind the pixels, students and even teachers are more prone to act disruptively and inappropriately in virtual classrooms. Participants expressed that people on metaverse platforms typically feel less guilty and accountable for acting unethically than they do in real life. "Anonymity in a deindividualized situation" contributes to people's unbridled and antisocial behaviour, which in turn leads to uninhibited behaviour, because it eliminates the mental process that would typically constrain people's behaviour in social situations and force them to conform to social norms (Diener, 1977; Reicher, 1995; Watson, 1973; Zimbardo, 1969). Research findings indicate that anonymity in the virtual universe is a factor that makes higher education institutions vulnerable to data attacks and data theft. Cyberattacks on data in the metaverse include malicious software, ransomware, identity fraud, copyright infringement, and data theft. Cyberattacks targeting data in the metaverse can take many forms, including malicious software, ransomware, identity fraud, copyright infringement, data theft, or data breaches. This could make metaverse universities vulnerable targets for various data attacks, such as phishing, ransomware, and avatar piracy. Higher education institutions affected by such attacks may suffer not only financial losses but also damage to their reputation.

A reconsideration of Kant's deontological perspective on ethics in the context of metavethics may contribute to the discussions of the metaverse where the line between the physical and the virtual is blurred, where it is not known what the boundaries of reality are, where the debate continues as to whether an avatar is just a virtual representation of one's physical reality or whether it is one's true self. On the one hand, while studies on the proteus effect (Fox *vd.*, 2013; Patsantaras, 2020; Pena *vd.*, 2009) revealing that the good or bad life experiences of avatars in the virtual universe have the same effect on individuals as in the real world, on the other hand, in a period when people in the virtual universe increase their immorality, bullying and exhibit a hedonistic attitude because they do not personally witness the consequences of their behaviour on others and can hide their anonymity.

In light of Kant's paradigm, empirical experience is where knowledge originates (Kant, 1998; Wood, 2017). This implies that we have no way of understanding how or what things are in themselves; we can only know them as they seem to us. Since the mind's operations cannot be extended outside of the phenomenal world, we are unable to learn anything about objects beyond their outward appearances, according to the Kantian ethical framework. Since objects in both the actual and virtual worlds are merely a structured collection of mental representations, their position in virtual reality is identical to that of the real world in this regard (Kucuk & Yildirim, 2023; Stanovsky, 2004). Since we can only identify other avatars as they seem to us, we must accept them as unique individuals, even regardless of whether they are extensions of actual people or even AI-generated characters (Kucuk & Yildirim, 2023). This implies that we must always view them as ends in and of themselves rather than as tools.

The metaverse is a new world where a digital twin of the physical world is created, where people can move, talk, produce, and engage in activities just like in the real world with 3D avatars, where they can own homes and offices, create their own spaces, produce digital goods and projects—in short, where they have many times more movement and production capabilities than in this world. Research data suggests that this situation will create conditions that are far more controversial and contradictory than those in the physical world regarding the concepts of the individual rights, and property. At this point, understanding Kant's paradigm that "empirical experience is where knowledge originates" will contribute to resolving conflicts over the individual rights, and property in the metaverse. Participants also emphasized that this new universe for humanity should be more democratic, libertarian, and free from the fictional patterns and constraints of the old world. Overall, if we want future metaverse universities to be more democratic, respectful of humanity, and free, we should act based on Kant's ethical philosophy that what we perceive is no different from reality, and we should behave responsibly in virtual environments just as we do in real ones.

The idea that morality ought to be rational is another significant addition made to metavethics by Kant's deontological ethical viewpoint. Science, which looks for the universal rules governing the natural world, is the foundation of his conception of morality. As we shall see the correct thing to do is always a rational thing. According to Kant, ethics is an ethic of obligation that consists of directives concerning what we should do. However, these commands originate from within us, from our reasoning, as opposed to other directives, which typically originate from an authority or wants, desires, and needs, and this is what is meant by a categorical imperative, a truly moral imperative (Kranak, 2019; Kucuk & Yildirim, 2023). The premise behind Kant's first articulation of the categorical imperative is that moral principles ought to be universal laws; for example if we consider analogous laws, such as the law of gravity, or scientific laws, such as Newton's three laws of motion, we can see that they are universal and equally applicable to all people, irrespective of their identities or needs and our moral laws must have the same shape if they are to be rational (Kranak, 2019). Kant's ideas, which argue that people should only act by distinguishing between "right" and "wrong" with a rational mind by the maxim that you would like to see become a universal law, instead of focusing on the consequences of their behaviour or their wishes and desires such as making themselves happy, can make an important contribution to metavethics in this period when its foundations are just beginning to be laid.

Metaverse technology offers the potential to establish a more realistic, qualified, immersive, inclusive, and customized learning environment for higher education. However, it also has the power to deprive humanity of what it has strived to achieve throughout the ages, such as freedom, social justice, tolerance, and virtue. Therefore, to shape healthy and high-quality metaversities, we must focus on producing more metaverse-oriented research, particularly in the social sciences, to gain a deeper understanding and a broader perspective on organising this emerging educational world. The educational metaverse ought to be governed by social and human sciences, including sociology, psychology, philosophy, and educational sciences, and directed by academia rather than by corporate and technological behemoths. This approach enables us to maintain the capacity to develop an improved educational metaverse for future generations, grounded in the ideals of justice, equality, tolerance, respect, responsibility, freedom, and virtue.

Conclusions and Implications

The research findings describe the profound risks of the educational metaverse in terms of data security and privacy in higher education. However, we should not ignore the positive effects of the metaverse arising from the integration of high technologies such as augmented

reality, artificial intelligence, and decentralized Internet with education for the universities of the future. In this sense, it can be said that this study, which set out with the concern of how to achieve an ideal, healthy, responsible, and ethical metaverse in higher education, provides a comprehensive risk analysis report for the metaverse and contributes to the roadmap that higher education administrators will need for an ideal metaverse.

The metaverse is a new world vision that may impact all systems involving human beings, potentially leading to radical transformations across all vital areas within itself. However, it is vital that higher education institutions, which are the driving force of society, perform this acting role effectively, successfully, and meticulously based on ethics and responsibility.

Beyond that, instead of adopting pre-made platforms, this research concludes that each university should develop its own digital twin, platform, and training scenarios in the metaverse, in order to enhance data security. By considering that every university has different needs and dynamics, universities may explore the model of educational platform they require in line with their demands and philosophy.

In the current era, it is high on the agenda that traditional universities might evolve towards metaversities, which are virtual campuses running on servers. The studies to be carried out for the new generation XR university models needed in this table might make a significant contribution to the field, enabling the education world to be prepared for the metaverse era. In this context, based on the conclusions derived from the research, for a healthy and responsible metaverse in higher education, the metaversities to be established must be decentralized, autonomous organizations, based on block chain technology, and personal data should not be entrusted to the servers of a private company and made market material or left at the mercy of the university authority in order to maintain the status quo.

Each university needs a strong cybersecurity team to counter Web 3.0-based cyber-attacks, protecting the metaversity's system and guiding users on security protocols. Besides, it is critically important for each state to initiate R&D studies in terms of its security quickly and to produce the VR headsets and XR equipment that its universities will need internally. Data is the new oil, the new power. The foreign-dependent supply of XR devices, which appears to be a harmless application, actually corresponds to a country's free delivery of its land and oil to a foreign company, essentially paying for it. In the case of metaversal education in universities, each student in that country might need an XR device for access, and outsourcing these devices means that the data will be handed over to that company.

The study presents a comprehensive view of the necessity for the metaverse to be grounded in ethical principles through a deliberate and collaborative effort, highlighting the need for metaversal regulations and robust strategies in higher education. Some ethical considerations should guide a metaverse policy in higher education, according to the experts who participated in the research. Academia, policymakers, and high-tech companies should come together to discuss how their institutions can participate in the metaverse in a way that ensures data privacy and security, and enact laws, regulations, and guidelines that protect individuals' biological, behavioural, and environmental data and ensure their privacy within a human rights framework.

On the other hand, since metavethics is a very recent concept, its scope is still very limited, and there are hardly any studies on metavethics in higher education. While this situation reinforces the need for exploratory research in this field, it also appears as a limitation in terms of strengthening the theoretical foundations of this study and providing a deeper perspective on the field of study.

Competing Interest

No potential conflict of interest was reported by the authors.

Data Availability Statement

The data that support the findings of this study are available on request from the corresponding author, [N.G.]. The data are not publicly available.

Ethical Approval

Ethical permission with a number 361920 was obtained from G.U., the social and humanities ethics committee, for this research on 11.09.2023.

Note

This article is derived from the dissertation thesis of the corresponding author, [N.G.].

References

- Abbate, S., Centobelli, P., Cerchione, R., Oropallo, E., & Riccio, E. (2022). A first bibliometric literature review on the metaverse. In T. Daim & N. Basoglu (Eds.), *2022 IEEE Technology and engineering management conference (Temscon Europe)* (pp. 254–260). IEEE. <https://doi.org/10.1109/temsconeurope54743.2022>
- Akdemir, N., & Tuncer, C. O. (2021). *Siber ansiklopedi: Siber ortama çok disiplinli bir yaklaşım* [Cyber encyclopedia: A multidisciplinary approach to cyberspace]. Pegem Akademi. <https://doi.org/10.14527/9786257582209>
- Arbogast, M. A. (2019). *Immersive technologies in preservice teacher education: The impact of augmented reality in project-based teaching and learning experiences* [Ph.D. Dissertation]. The University of Toledo, Toledo. http://rave.ohiolink.edu/etdc/view?acc_num=toledo1553266590134835
- Barnett, R. (2017). Constructing the university: Towards a social philosophy of higher education. *Educational Philosophy and Theory*, 49(1), 77–88. <https://doi.org/10.1080/00131857.2016.1183472>
- Brocki J. M. & Weardon, A. J. (2006). A Critical evaluation of the use of interpretative phenomenological analysis (IPA) in health psychology. *Psychology and Health*, 21, 98–101. <https://doi.org/10.1080/14768320500230185>
- Brunnbauer, J. B. (2022). Ethical challenges for the metaverse development. *Proceedings of the National Academy of Sciences of the United States of America*, 119(8). <https://doi.org/10.1073/pnas.2120481119>
- Check Point. (2022). *Check Point Software's 2022 Security Report*. <https://pages.checkpoint.com/cyber-security-report-2022>
- Datta, P., Namin, A. S., & Chatterjee, M. (2018). A survey of privacy concerns in wearable devices. In N. Abe, H. Liu, C. & Pu, X. Hu (Eds.), *2018 IEEE International conference on big data (Big Data)* (pp. 4549–4553). IEEE. <https://doi.org/10.1109/BigData44402.2018>
- Dayarathna, R. (2022). Ethics in the metaverse. In T. Perera & S. M. Vithanarachchi (Eds.), *Sri Lanka Association for the Advancement of Science Proceedings of the 78th Annual Sessions 2022- Part II* (pp. 79–86). SLAAS.
- Deloitte Insight. (2022). *Cyber risks survey*. <https://www2.deloitte.com/us/en/insights/topics/cyber-risk.html>
- Diener, E. (1977). Deindividuation: Causes and consequences. *Social Behaviour and Personality*, 5(1), 143–155.
- Fırıncioğulları, S. (2016). A short review on social science and hermeneutics. *Sosyoloji Dergisi*, 33, 37–48. <https://dergipark.org.tr/tr/pub/sosder/issue/41007/495541>
- Fox, J., Bailenson, J. N., & Tricase, L. (2013). The embodiment of sexualized virtual selves: The Proteus effect and experiences of self-objectification via avatars. *Computers in Human Behaviour*, 29(3), 930–938. <https://doi.org/10.1016/j.chb.2012.12.027>
- Gibson, W. (1984). *Neuromancer*. Ace Books.
- Glesne, C. (2015). *Becoming qualitative researchers: An introduction*. New Jersey: Pearson.

- Hassanzadeh, M. (2022). Metaverse, metaversity, and the future of higher education. *Sciences and Techniques of Information Management*, 8(2), 7–22. <https://doi.org/10.22091/stim.2022.2243>
- Ich, E., Miah, A., & Lewis, S. (2019). Is digital health care more equitable? The framing of health inequalities within England’s digital health policy 2010–2017. *Sociology of Health & Illness*, 41, 31–49. <https://doi.org/10.1111/1467-9566.12980>
- IEEE Standards Association. (2022, July 15). *Demystifying and defining the metaverse: Keynote speakers* [Video]. YouTube. <https://www.youtube.com/watch?v=7vhHyoucC7ovet=9s>
- Fraenkel, J. R., & Wallen, N. E. (2008). *How to design and evaluate research in education* (7th ed.). New York: McGraw-Hill.
- Joye, S. R. (2016). The Pribram–Bohm hypothesis. *Consciousness: Ideas and Research for the Twenty-First Century*, 3(1), 1–20. <https://digitalcommons.ciis.edu/conscjournal/vol3/iss3/1/>
- Kaddoura, S., & Al Husseiny, F. (2023). The rising trend of metaverse in education: Challenges, opportunities, and ethical considerations. *PeerJ Computer Science*, 9 (1), 12–52. <https://doi.org/10.7717/peerjcs.1252>
- Kant, I. (1998). *Critique of pure reason* (P. Guyer & A. W. Wood, Trans.). Cambridge University Press. (Original work published 1781).
- Karadayı, Z. (2022). *Sanal gerçeklik teknolojisi ile desteklenen deneysel öğrenmenin öğretmen eğitiminde uygulanmasına ilişkin bir durum çalışması* [A case study on the implementation of experiential learning supported by virtual reality technology in teacher education]. [Ph.D. Dissertation]. Çanakkale Onsekiz Mart Üniversitesi, Çanakkale.
- Karsantık, İ., & Çetin, M. (2020). Yükseköğretim kültürü ölçeğinin geliştirilmesi: geçerlik ve güvenilirlik çalışması [Development of higher education culture scale: validity and reliability study.]. *Mehmet Akif Ersoy Üniversitesi Eğitim Fakültesi Dergisi*, 54, 258–281.
- Kaya, E. (2022). *Metaverse: Meta insana hazır mısınız?* [Metaverse: Are you ready for meta-human]. Nemsis.
- Ko, C. (2021, November 12). Artificial intelligence (AI) in geomatics at York University. *YorkU*. <https://euc.yorku.ca/research-spotlight/artificial-intelligenceai-in-geomatics-at-york-university/>
- Kranak, J. (2019). Kantian deontology. *Introduction to Philosophy: Ethics*. Rebus Community.
- Kshetri, N. (2022). Policy, ethical, social, and environmental considerations of Web3 and the metaverse. *IT Professional*, 24(3), 4–8. <https://doi.org/10.1109/MITP.2022.3178509>
- Kucuk, E. E., & Yildirim, C. (2023, April). Is “categorical imperative” metaversal? A Kantian ethical framework for social virtual reality. In A. Schmidt & K. Väänänen (Eds.), *Extended abstracts of the 2023 CHI conference on human factors in computing systems* (pp. 1–7). SIGCHI. <https://doi.org/10.1145/3544549.3585911>
- Lee, K. F., & Quifan, C. (2021). *AI 2041: Ten visions for our future*. Currency Publishing.
- Li, Y., Wei, W., & Xu, J. (2022). The exploration on ethical problems of educational metaverse. In L. J. Zhang (Ed.), *International conference on metaverse* (pp.29–38). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-23518-4_3
- Miles, M. B., ve Huberman, A.M. (1994). *Qualitative data analysis: An expanded sourcebook*. Sage publications.
- Moghaddam, A. (2006). Coding issues in grounded theory. *Issues in Educational Research*, 16(1), 52–66. <http://www.iier.org.au/iier16/moghaddam.html>
- Park, S. M., & Kim, Y. G. (2022). A metaverse: Taxonomy, components, applications, and open challenges. *IEEE Access*, 10, 4209–4251. <https://doi.org/10.1109/ACCESS.2021.3140175>
- Patsantaras, N. (2020). Virtual Bodies (avatars) and sport exercises: Some important thoughts. *European Journal for Sport and Society*, 17(4), 339–356. <https://doi.org/10.1080/16138171.2020.1792087>
- Patton, M. Q. (2014). *Qualitative research & evaluation methods: Integrating theory and practice*. Sage publications.
- Pena, J., Hancock, J. T., & Merola, N. A. (2009). The priming effects of avatars in virtual settings. *Communication Research*, 36(6), 838–856. <https://doi.org/10.1177/0093650209346802>
- Price, K., & Price, J. (2023). The metaverse: Higher education’s next frontier. *Journal of Business Administration Online*, 17(1), 10–18. <https://files.eric.ed.gov/fulltext/EJ1440308.pdf>
- Rawal, B. S., Ahmadand, S., Mentges, A., & Fadli, S. (2022). Opportunities and challenges in the metaverse: The rise of the digital universe. In L. J. Zhang (Ed.), *International conference on metaverse* (pp. 3–7). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-23518-4_3

- Reicher, S., Spears, R., and Postmes, T. (1995). A Social identity model of deindividuation phenomena. *European Review of Social Psychology*, 6, 161–198. <https://doi.org/10.1080/14792779443000049>
- Ruwodo, V., Pinomaa, A., Vesisenaho, M., Ntinda, M., & Sutinen, E. (2022). Enhancing software engineering education in Africa through a metaversity. In J. E. Mitchell (Ed.), *2022 IEEE Frontiers in Education Conference (FIE)* (p. 1–8). IEEE. <https://doi.org/10.1109/fie56618.2022.9962729>
- Saraçoğlu, D. (2022). Metaverse and new cybersecurity threats. In F. S. Esen (Ed.), *Metaverse technologies to build future worlds opportunities and threats* (p. 131–159). Nobel.
- Seggie, F. N. & Bayyurt, Y. (2015). *Nitel Araştırma Yöntem, Teknik, analiz ve yaklaşımları* [Qualitative research methods, techniques, analysis and approaches]. Anı Press.
- Smith, C. H., Molka-Danielsen, J., Rasool, J., & Webb-Benjamin, J. B. (2023). The world as an interface: Exploring the ethical challenges of the emerging metaverse. In T. Bui (Ed.), *Proceedings of the 56th Hawaii International Conference on System Sciences* (pp. 6045–6054). HICSS. <https://hdl.handle.net/10125/103367>
- Smith, J. A. (2011). Evaluating the contribution of interpretative phenomenological analysis. *Health Psychology Review*, 5(1), 9–27. <https://doi.org/10.1080/17437199.2010.510659>
- Stanovsky, D. (2004). Virtual Reality. In L. Floridi (Ed.), *The Blackwell Guide To The Philosophy Of Computing And Information* (pp.167–177). Blackwell.
- Stephenson, N. (1992). *Snow Crash*. Bantam Books.
- Suh, W., & Ahn, S. (2022). Utilizing the metaverse for learner-centred constructivist education in the post-pandemic era: An analysis of elementary school students. *Journal of Intelligence*, 10(1), 17–32. <https://doi.org/10.3390/jintelligence10010017>
- Sun, X., Zhang, F., Wang, C., & Lv, B. (2021). Application of 5 G mobile communication technology in a specific environment of a power system. In A. Rachedi (Ed.), *2021 International Wireless Communications and Mobile Computing (IWCMC)* (pp. 648–651). IEEE. <https://doi.org/10.1109/IWCMC51269.2021.9488112>
- Sutikno, T., & Aisyahrani, A. I. B. (2023). Non-fungible tokens, decentralized autonomous organizations, Web 3.0, and the metaverse in education: From university to metaversity. *Journal of Education and Learning (EduLearn)*, 17(1), 1–15. <https://doi.org/10.11591/edulearn.v17i1.23629>
- Takahashi, D. (2021, July 14). *The ethics of the metaverse* [Video]. Venture Beat. <https://venturebeat.com/games/the-ethics-of-the-metaverse/>
- Watson, R. I. (1973). Investigation into deindividuation: Using a cross-cultural survey technique. *Journal of Personality and Social Psychology*, 25(3), 342–345. <https://doi.org/10.1037/h0034218>
- WEF. (2022). *Global Risks Report 2022*. World Economic Forum. <https://www.weforum.org/publications/global-risks-report-2022/>
- Williams, M., & Moser, T. (2019). The art of coding and thematic exploration in qualitative research. *International Management Review*, 15(1), 45–55. <https://doi.org/10.2139/ssrn.3440749>
- Wood, A. (2017). Is Kant a great moral philosopher? In S. Hetherington (Ed.), *What makes a philosopher great?* (pp. 169–186). Routledge.
- Zalilo, M., & Clarkson, P. J. (2022). Designing the metaverse: A study on inclusion, diversity, equity, accessibility, and safety for digital immersive environments. *Telematics and Informatics*, 75, 1–12. <https://doi.org/10.1016/j.tele.2022.101909>
- Zallio, M., & Clarkson, P. J. (2023). Metavethics: Ethical, integrity and social implications of the metaverse. *Intelligent Human Systems Integration*, 69, 683–691. <https://doi.org/10.54941/ahfe1002891>
- Zimbardo, P. G. (1969). The human choice: Individuation, reason, and order versus deindividuation, impulse, and chaos. *Nebraska Symposium on Motivation*, 17, 237–307.

Received: April 18, 2025

Revised: May 19, 2025

Accepted: August 12, 2025

Cite as: Gündüz, N., & Sincar, M. (2025). Data privacy and security challenges in metaversities: The ethical dilemmas in the future of higher education. *Problems of Education in the 21st Century*, 83(4), 525–544. <https://doi.org/10.33225/pec/25.83.525>

Nurten Gündüz
(Corresponding author)

PhD, Higher School of Foreign Languages, Gaziantep University, A Block,
Sehitkamil, Gaziantep, Türkiye.
E-mail: nrtnutar@gmail.com
ORCID: <https://orcid.org/0000-0003-3684-1920>

Mehmet Sincar

PhD, Department of Educational Administration, Gaziantep University, Gaziantep,
Türkiye.
E-mail: mehmetincarc@yahoo.com
ORCID: <https://orcid.org/0000-0002-4979-5014>