

Personal Data processing within Immersive Virtual Worlds: Privacy challenges in the interconnected data-driven Metaverse

MetaverseUA Chair Research Paper #2

**Pablo Trigo Kramcsák
Vagelis Papakonstantinou**



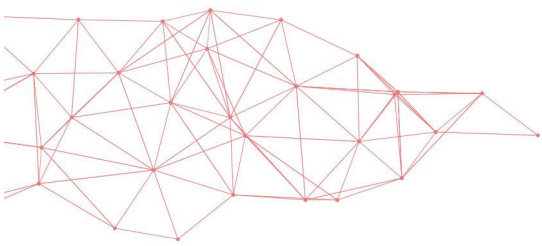
The **Chair for the Responsible Development of the Metaverse (MetaverseUA Chair)** was created by the University of Alicante (Spain) and financed by Meta Platforms under its [XR Program and Research Funds](#). The Program aims at supporting independent academic research across Europe into metaverse challenges and opportunities. The MetaverseUA Chair is a member of the [European Metaverse Research Network](#). Like all our work, this report has been produced completely independently. The ideas expressed in this paper are the sole responsibility of the author(s).

How to cite this paper:

Trigo Kramcsák, P., Papakonstantinou, V., 'Personal Data Processing within Immersive Virtual Worlds: Privacy Challenges in the Interconnected Data-Driven Metaverse' (2024) *MetaverseUA Research Paper #2*, <https://metaversechair.ua.es/working-papers/>

[Pablo Trigo Kramcsák](#) is Researcher at LSTS, Vrije Universiteit Brussel (Belgium).

[Vagelis Papakonstantinou](#) is Professor of Law at Vrije Universiteit Brussel (Belgium).



Abstract

The metaverse is a virtual space that merges the physical and digital worlds into a dynamic, interconnected, and data-driven environment. This virtual setting depends on technologies, platforms, tools, and devices designed to process large-scale and real-time big data. The ability to collect, store, and seamlessly connect massive datasets generated by metaverse interactions -including declared, observed, and inferred personal data- is growing rapidly. The immersive experiences of virtual worlds exacerbate hyper-connectivity and data-gathering challenges, which may intensify or alter the existing issues raised by big data processing models and their underlying technologies. This study aims to explore the complex landscape of data protection in virtual interactive settings. The main goal is to identify and analyse the most urgent privacy and data protection challenges that need to be solved to enable the development of trustworthy and secure metaverse ecosystems.

Keywords: virtual worlds, data processing, personal data protection, identity and authentication, accountability, data security risks

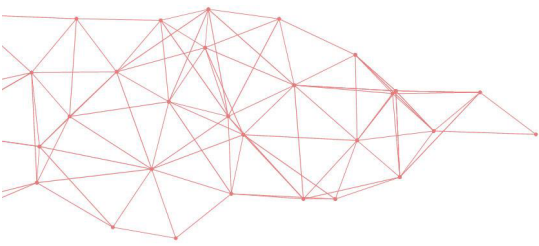


Table of Contents

1. Metaverses / Virtual Worlds: Concept and Main Features.....	1
2. Types of Metaverse(s)	2
3. Data Processing in the Metaverse. Taxonomy	3
4. Personal Data Protection Issues in the Metaverse.....	6
4.1 Intensive Data Collection and Detailed Profiling	7
4.2 Identity, Authentication and Anonymity	9
4.3 Data Consent, Transparency and Control	10
4.4 Territorial Scope of Data Regulations	11
4.5 Responsibility, Accountability and Joint Controllership	12
4.6 Interoperability and Portability	14
4.7 Data Security Risks.....	15
4.8 Exercise of Data Subject’s Rights in Immersive Digital Worlds	15
5. Conclusion	16
Bibliography	18

1. Metaverses / Virtual Worlds: Concept and Main Features

The term “Metaverse” is a neologism that combines “meta-” (meaning beyond or transcending) and “verse” (short for “universe” or the whole cosmos)¹. It refers to a novel virtual universe that surpasses the physical reality.² This concept was first introduced by the science-fiction author Neal Stephenson in his seminal work 'Snow Crash' (1992), alluding to a 'hyper-commercialized, extremely detailed rendition of a virtual-reality network',³ 'that utilises internet and augmented reality (AR) via avatars and software agents'.⁴

The concept of the metaverse is ambiguous and has many possible definitions in the literature.⁵ However, it can be grasped as a 'computer-based environment built entirely online and shared by individuals'.⁶ It is also described as an 'infinitely large, persistent, digital, and interactive information space' that 'increasingly interacts with the physical world',⁷ through the 'fusion of both virtually-enhanced physical reality and physical-persisted virtual space'.⁸ In this space, users have virtual self-representations called “avatars”.⁹

Metaverses have three core features: persistence and real-time functionality, immersive user experiences, and a comprehensive economic system.¹⁰ Moreover, to operate the metaverse, it needs four key technical characteristics:

- **Realism:** This feature enables individuals to emotionally immerse themselves in the virtual world, creating a deep connection with the environment.
- **Ubiquity:** This means that virtual spaces should be easily accessible across all digital devices while maintaining a single virtual identity. It's about ensuring accessibility and a consistent presence across various platforms.

¹ General Secretariat of the Council of the European Union, Analysis and Research Team (ART), 'Metaverse - Virtual world, real challenges' (2022). <<https://www.consilium.europa.eu/media/54987/metaverse-paper-9-march-2022.pdf>>

² Xinli Zhang and others, 'The Metaverse in Education: Definition, Framework, Features, Potential Applications, Challenges, and Future Research Topics' (2022) 13 *Frontiers in Psychology*, 2.

³ Nicholas M Kelly, "Works like Magic": Metaphor, Meaning, and the GUI in Snow Crash' (2018) 45 *Science Fiction Studies* 69, 70.

⁴ Yogesh K. Dwivedi and others, 'Metaverse beyond the Hype: Multidisciplinary Perspectives on Emerging Challenges, Opportunities, and Agenda for Research, Practice and Policy' (2022) 66 *International Journal of Information Management* 102542, 2.

⁵ European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, 'Metaverse - Study requested by the JURI Committee' (2023) 10. <[https://www.europarl.europa.eu/RegData/etudes/STUD/2023/751222/IPOL_STU\(2023\)751222_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2023/751222/IPOL_STU(2023)751222_EN.pdf)> accessed 20 September 2023. For example, the concept 'is becoming a sort of “catch-all” term to talk about Web 3.0, blockchain, cryptocurrencies, NFTs (Freeman and others, 2022), DeFi (Decentralised Finance), DAO (Decentralised Autonomous Organization), and so on' (Luciano Floridi, 'Metaverse: a Matter of Experience' (2022) 35 *Philosophy & Technology*, 73. <<https://doi.org/10.1007/s13347-022-00568-6>>)

⁶ Jack Boraham, 'What Is Metaverse Virtual World? [+4 Metaverse Realities]' (*MetaverseInsiderTech*, 11 July 2022) <<https://metaverseinsider.tech/2022/07/11/metaverse-virtual-worlds/>> accessed 6 September 2023.

⁷ Doug Antin, 'The Technology of the Metaverse, It's Not Just VR' (www.medium.com, 5 May 2020) <<https://medium.com/swlh/the-technology-of-the-metaverse-its-not-just-vr-78fb3c603fe9>> accessed 2 February 2024.

⁸ Zhang and others. (n 2).

⁹ Ben Chester Cheong, 'Avatars in the metaverse: potential legal issues and remedies' (2022) *Int. Cybersecur. Law Rev* 3, 467-494, p. 472.

¹⁰ European Commission and the Multi Stakeholder Platform on ICT Standardisation (MSP), 'Rolling Plan for ICT Standardisation - Metaverse' (2023) <<https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/metaverse#>> accessed 20 September 2023.

- Interoperability: This aspect allows different systems or platforms to seamlessly share information and interact with each other, promoting a more interconnected metaverse experience.
- Scalability: This pertains to the network architecture's capacity to accommodate a large number of users in the metaverse without compromising system efficiency or user experience. It ensures that the metaverse can grow and adapt to the demands of a growing user base.¹¹

The metaverse has undergone significant improvements in autonomy, capacity, and functionality in recent years. Technological advances in virtual reality (VR), augmented reality (AR), mixed reality (MR) and extended reality (XR) technologies,¹² along with fast global internet and powerful devices, have led to the creation of more realistic and engaging virtual environments.¹³ This is coupled with new applications, better compatibility with various technologies, and seamless integration with smart devices, making virtual experiences more lifelike. Nevertheless, it is argued that '[t]he development of the Metaverse is still in its infancy, and the business model has yet to mature'.¹⁴

Public and private entities are exploring how to leverage the metaverse and integrate it within their processes, services, and business models.¹⁵ Virtual worlds are expected to 'transform a wide range of industries by enabling more seamless and immersive experiences as well as creating a sense of presence without the need to be physically present in a location'.¹⁶ Consequently, the principal driving forces behind these virtual worlds are rooted in social and economic interactions.¹⁷ These elements have sparked growing interest and debate regarding the varied socio-economic implications that metaverses may exert globally.¹⁸

2. Types of Metaverse(s)

Virtual worlds can be broadly divided into two main categories: centralised and decentralised. These categories differ in how they are governed, developed, and managed,

¹¹ European Parliamentary Research Service (EPRS), 'Metaverse: Opportunities, Risks and Policy Implications' (2022) <https://www.europarl.europa.eu/cmsdata/268589/eprs-briefing-metaverse_EN.pdf> accessed 20 September 2023.

¹² Agencia Española de Protección de Datos, 'Metaverse and Privacy' (www.aepd.es, 29 September 2022) <<https://www.aepd.es/en/prensa-y-comunicacion/blog/metaverse-and-privacy>> accessed 21 September 2023.

¹³ Arjun Nagendran and others, 'Avatar Led Interventions in the Metaverse Reveal That Interpersonal Effectiveness Can Be Measured, Predicted, and Improved' (2022) 12 Scientific Reports 21892.

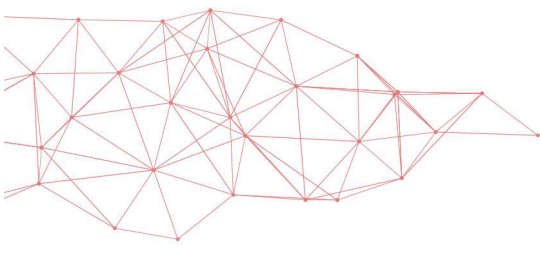
¹⁴ Hang Wang and others, 'A Survey on the Metaverse: The State-of-the-Art, Technologies, Applications, and Challenges' (2023) 10 IEEE Internet of Things Journal 16, 14671-14688, p.14673.

¹⁵ Dwivedi and others (n 4).

¹⁶ Lau Christensen and Alex Robinson, 'The Potential Global Economic Impact of the Metaverse' (2022) Analysis Group, 2. <<https://www.analysisgroup.com/globalassets/insights/publishing/2022-the-potential-global-economic-impact-of-the-metaverse.pdf>>

¹⁷ Mitchell Goldberg and Fabian Schär, 'Metaverse Governance: An Empirical Analysis of Voting within Decentralized Autonomous Organizations' (2023) 160 Journal of Business Research 113764.

¹⁸ World Economic Forum, 'Social Implications of the Metaverse' (2023) <https://www3.weforum.org/docs/WEF_Social_Implications_of_the_Metaverse%20_2023.pdf> accessed 1 February 2024.



presenting different functions and possibilities for their users. Some virtual worlds may also mix elements from both types.¹⁹

A centralised metaverse resembles traditional internet platforms, where a few entities have significant power over the infrastructure, governance, and data. 'This implies that a single person or entity may seize total authority over the metaverse and decide how it should be run [...] with database servers and policies to control the virtual world'²⁰ Then, a central authority oversees the entire ecosystem, determining and enforcing rules, policies, and governance, while users wield limited influence over decision-making processes. This central stakeholder often exerts substantial control over user data, encompassing its collection, copy, storage, and dissemination (for example, managing user identities, authentication, and profiles). Centralised platforms typically rely on revenue models such as advertising and subscriptions to sustain themselves, impacting user experiences and data utilisation.

A decentralised metaverse runs on a distributed network where control and infrastructure are shared among nodes or participants, distributing and 'decentralizing its key components'²¹ This type of metaverse enables more user autonomy and ownership, as well as peer-to-peer interactions, impacting on managing digital assets, content moderation, and client and device diversity.²² It often uses blockchain technology and decentralised protocols to support its features, which impacts the levels of decentralisation.²³ Users can participate in the governance and development of this metaverse model. However, they also need to overcome the technical and coordination challenges arising from the decentralised metaverse's unique aspects.

3. Data Processing Operations in the Metaverse. Taxonomy

Data collection (personal or non-personal) has emerged as an indispensable component of ever-expanding immersive virtual spaces that 'accumulate, store and exchange massive volumes of data every second'.²⁴ This is integrated into the infrastructure architecture of Metaverses, along with the design of its technological enablers, which include wearable haptic devices, the Internet of Things (IoT), and virtual platforms.²⁵

On that basis, it can be asserted that the metaverse is an inherently data-driven framework, 'comprised of vast, bordering on infinite amounts of information'.²⁶

The data-centric nature of the Metaverse presents unique privacy challenges due to its immersive, multifaceted, and real-time characteristics, including deeper profiling,

¹⁹ Ikram Ud Din and others, 'Integration of IoT and Blockchain for Decentralized Management and Ownership in the Metaverse' (2023) 36 International Journal of Communication Systems e5612.

²⁰ Ibukun Ogundare, 'Centralized vs Decentralized Metaverse: Complete Guide' (www.coinspeaker.com , 16 February 2023) <<https://www.coinspeaker.com/guides/centralized-vs-decentralized-metaverse-complete-guide/>> accessed 20 September 2023.

²¹ Omar Hashash and others, 'Towards a Decentralized Metaverse: Synchronized Orchestration of Digital Twins and Sub-Metaverses' (2023) ICC 2023 - IEEE International Conference on Communications, Rome, Italy, 2023, 1905-1910, <doi: 10.1109/ICC45041.2023.10279406> accessed 15 November 2024.

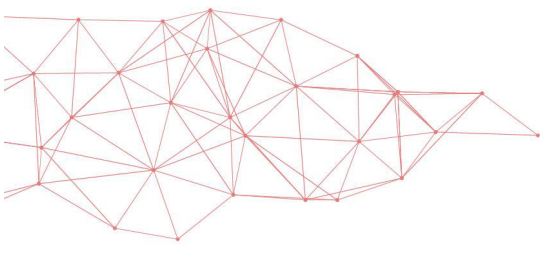
²² Goldberg and Schär (n 17).

²³ Nir Kshetri, 'A Typology of Metaverses' (2022) 55 Computer 150.

²⁴ Gaurav G. Arora, 'Data protection in Metaverse: Ascertaining privacy in the ever-expanding virtual world (*ET Edge Insights*, 27 December 2022) <<https://etedge-insights.com/technology/data-protection-in-metaverse-ascertaining-privacy-in-the-ever-expanding-virtual-world/>> accessed 15 November 2024

²⁵ Kisoo Kim and others, 'Metaverse Wearables for Immersive Digital Healthcare: A Review' (2023) 10 Advanced Science 2303234. <<https://doi.org/10.1002/advs.202303234>> accessed 15 November 2024

²⁶ Antin (n 7).



constant monitoring, and interference of special categories of data.²⁷ 'The Metaverse is based on technologies that enable multisensory interactions with virtual environments, digital objects and people'.²⁸ In this sense, [m]ulti-sensory experiences in the metaverse will expand the scope of data privacy beyond the normal data points to include emotional, biometric, and physiological data, meaning users will be monitored at an almost forensic level.²⁹ Within this context, various data types are collected, including user profiles, user-generated content, preferences, location data, physiological and biometric information, as well as patterns of user behaviour. 'The metaverse can be perceived as a social microcosmos where players (individuals using the metaverse) can exhibit realistic social behaviour'³⁰, which goes beyond what we usually experience in traditional online environments. Therefore, metaverse systems 'can collect far more sensitive information than traditional systems'.³¹ The demand for interoperability and cross-platform integration adds to the complexity of this landscape.

The data processed in virtual worlds can be categorised into three primary groups: declared data (information voluntarily shared by users),³² observed data (data originating from user actions, interactions, and preferences),³³ and inferred data (information derived through analysis of existing data).³⁴

(i) Declared Data:

Declared data represents information users willingly and consciously share while interacting in the virtual world. The significance of declared data lies in its direct and explicit nature. This category covers the following aspects of user data:

- User Profiles: Users can create and edit their profiles with information such as their name, age, gender, and contact details.
- Preferences: Users can choose their interests, hobbies, and other preferences during account setup or later, to tailor the virtual experience.
- Personal Details: Users can share other information, such as their biography or profile photo, to customise their virtual identity.

²⁷ European Data Protection Supervisor, 'Metaverse' (www.edps.europa.eu) <<https://edps.europa.eu/press-publications/publications/techsonar/metaverse>> accessed 12 October 2023.

²⁸ Stylianos Mystakidis, 'Metaverse' (2022) Encyclopedia 2, no. 1, 486-497, p.487.

²⁹ GlobalData Thematic Intelligence, 'Data Privacy Concerns Will Be Amplified by the Metaverse' (www.verdict.co.uk, 20 January 2023) <<https://www.verdict.co.uk/data-privacy-metaverse-challenge/?cf-view>> accessed 16 November 2024

³⁰ Lik-Hang Lee and others, 'All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda' (2021) Journal of Latex Class Files, Vol. 14, No. 8, September 2021, 39.

³¹ Dwivedi and others. (n 4) 8.

³² It could be defined as 'data actively and knowingly provided by the data subject' (Article 29 Data Protection Working Party, 'Guidelines on the right to data portability - WP 242 rev.01, 5 April' (2017) 10. <<https://ec.europa.eu/newsroom/article29/items/611233>>).

³³ It could be defined as 'data provided by the data subject by virtue of the use of the service or the device' ('JUSTICE AND CONSUMERS ARTICLE 29 - Guidelines on the Right to "Data Portability" (Wp242rev.01) <<https://ec.europa.eu/newsroom/article29/items/611233>> accessed 15 November 2024.)

³⁴ Inferred data (or derived data) 'refers to data which is created by the controller on the basis of the data provided by the data subject (regardless of whether these data were observed or actively provided by the data subject, or a combination thereof' ('Guidelines 8/2020 on the Targeting of Social Media Users | European Data Protection Board' <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_en> accessed 15 November 2024.)

(ii) Observed Data:

This category covers the information that results from users' activities, interactions, and behaviours in the virtual environment. Within this context, metaverse devices and sensors can collect and use data from the physical world to improve user's immersive experience.³⁵ This data can come from various sources, such as metaverse core service providers or third parties, who use a service, platform, software, or device. This data type is helpful in understanding user behaviour and providing feedback for virtual world operators to enhance their platforms and services. The aim of capturing such information, including biometric data, 'is to integrate this mixed modality (input and output) to build a holistic user experience in the metaverse'.³⁶ Observed data includes a wide range of data points, such as:

- **User Activities:** Data related to what users do in the virtual world, such as the places they go, the objects they interact with, and the actions they perform. 'For example, a VR headset requires external cameras as well as other motion sensors, which may result in the processing of data regarding private spaces like users' homes. In this scenario, it is likely that non-user data may also be captured if, for example, the user lives with other individuals who are captured in the background'.³⁷
- **Sensorial Data:** Data from users' sensory experiences and perceptions, which can reveal personal details about their environment, activities, or preferences. This includes visual data (from micro-optics, image recognition and other sensors), audio data (from voice recordings, noise, and ambient audio), and tactile data (from touch or physical sensations, such as haptic feedback from devices like touchscreens, bodysuits and gloves, gaming controllers, virtual reality devices and biometry systems). This also includes body language data, such as eye movements, facial expressions, gestures, and skin temperature. For example, 'VR glasses extract information from iris variations, and remotes that interface with the metaverse reveal postural changes, allowing analysis of emotional response'.³⁸
- **Communication Logs:** Data from user conversations, messages, and interactions in virtual worlds, using communication tools.
- **Location Tracking:** Data from users' virtual locations and interactions with specific virtual spaces, gathered by virtual world platforms and service providers.
- **Virtual Transactions:** Data from in-game purchases, the use of virtual currency, and other commercial activities in virtual environments.

(iii) Inferred Data:

This category covers the new insights or knowledge derived from declared and observed data using advanced data analysis techniques, including AI decision-making systems.³⁹ It refers to 'the data that a third-party observer could deduce - "infer" - from the

³⁵ Lee and others. (n 30) 41.

³⁶ *ibid.*

³⁷ Bristows Team 'Data protection in the metaverse' (Bristows, 27 October 2022) <<https://www.bristows.com/news/data-protection-in-the-metaverse/>> accessed 10 October 2023.

³⁸ Agencia Española de Protección de Datos (n 12).

³⁹ AI tools could be relevant, among other aspects, for the operation of automatic digital twins, computer agents and the autonomy of the avatar (Lik-Hang Lee and others, 'All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda' (2021) *Journal of Latex Class Files*, Vol. 18, No. 8, September 2021, 14). 'In many AI-aided services and applications in the metaverse, the decisions are made by AI agents, which are driven by ML models as black boxes without the capability of interpretability and explainability' (Thien Huynh-The and others, 'Artificial Intelligence for the Metaverse: A

analysis of human characteristics or, in other words, interpret from the collection, absorption and rationalisation of human characteristics'.⁴⁰ For example, motion-based fingerprinting 'can be used to accurately infer a number of specific personal characteristics about the user, including their height, handedness, and gender. And when combined with other data that's commonly tracked in virtual and augmented environments, this motion-based fingerprinting method is likely to yield even more accurate identifications.'⁴¹ It should be noted that inferences could "reveal" sensitive details about the individual, such as medical diseases, physical disabilities or previously experienced traumas'.⁴² Some key aspects and uses of inferred data are:

- Preferences and Interests: Virtual world systems can estimate users' likes and dislikes by analysing their stated preferences and observed behaviours.
- Recommendations: Inferred data is essential for providing personalised content recommendations. For example, it can suggest virtual places to visit, items to buy, or connections to make.
- Targeted Advertising: Advertisers can use inferred data to tailor advertisements to users' likely interests, thus increasing the relevance and effectiveness of advertising in the metaverse.
- Enhanced Functionality: Inferred data can also enhance the functionality of virtual worlds by anticipating user needs and automating certain processes to improve user experiences.

4. Personal Data Protection Issues in the Metaverse

The immersive extended reality experiences within the metaverse can potentially exacerbate the existing challenges of hyper-connectivity and the vast accumulation of big data. 'All the technologies that make up the metaverse environment (social networks, AI, IoT, neural interfaces, etc.) have their own privacy risks that need to be managed'.⁴³ For example, 'Internet-connected devices such as wearables allow monitoring and collect users' information [...] These devices can collect several types of data: personal information (e.g., physical, cultural, economic), users' behaviour (e.g., habits, choices), and communications (e.g., metadata related to personal communications)'.⁴⁴ But in addition, the joint application of all these technologies can lead to individual and societal effects that generate risks to rights and freedoms on a scale that is difficult to estimate a priori'.⁴⁵

Survey' (2023) Engineering Applications of Artificial Intelligence, Volume 117, Part A, 105581, ISSN 0952-1976, <<https://doi.org/10.1016/j.engappai.2022.105581>>

⁴⁰ Luca Bolognini and Marco Emanuele Carpenelli, 'The future of personal data in the Metaverse' (2022) Istituto Italiano per la Privacy e la Valorizzazione dei Dati, 8. <<https://zenodo.org/records/6413046>>

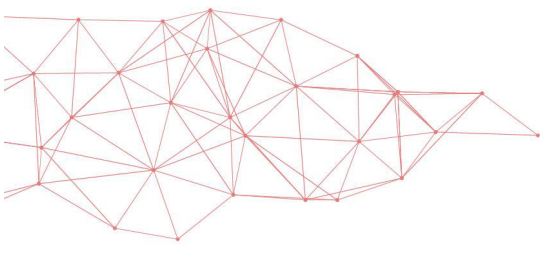
⁴¹ Louis Rosenberg, 'Privacy in the Metaverse might be Impossible (new research study)' (*Medium*, 30 March 2023) <<https://medium.com/predict/privacy-in-the-metaverse-might-be-impossible-new-research-study-64935481c6de>> accessed 10 February 2024.

⁴² Eleonora Margherita Auletta, Francesca Tugnoli and Giada Iovane, 'Personal data protection in the Metaverse: operational challenges and regulatory uncertainties' (*ICTLC*, 28 September 2022) <https://www.ictlc.com/personal-data-protection-in-the-metaverse-operation-challenges-and-regulatory-uncertainties/?lang=en#_ftn4> accessed 10 February 2024.

⁴³ Agencia Española de Protección de Datos (n 12).

⁴⁴ Lee and others. (n 30) 39.

⁴⁵ Agencia Española de Protección de Datos (n 12).



In this sense, it is argued that achieving privacy in the metaverse could be an insurmountable task without implementing innovative safeguards to shield users.⁴⁶

As the metaverse evolves and matures, it is increasingly important to delve into the profound privacy and data protection considerations that come with its growth, mainly related to the European Union General Data Protection Regulation (GDPR). Considering that 'the metaverse "exists to breach the borders of reality and distance, connecting people from all over the globe," the GDPR would likely apply given the scope of data processing and the nature of the platform'.⁴⁷

The metaverse poses a significant challenge to fundamental data protection principles due to its intricate data architecture.⁴⁸ Unlike traditional platforms, it requires users to share more personal data,⁴⁹ including sensitive categories such as physiological and biometric information. This makes it difficult to apply the principles of purpose limitation and data minimisation, which aim to limit and reduce the amount and scope of data collection and usage. Moreover, the principle of data protection by design, which requires privacy considerations to be integrated into the systems' architecture, faces obstacles in the metaverse due to its underlying dynamics, overlapping components and vast network of technologies. The need for interoperability and cross-platform integration also adds complexity to the implementation of robust privacy and data protection measures across the metaverse ecosystem.

Given the transformative nature of these developments and the distinctive challenges of the European regulatory landscape, as well as the broader spectrum of data protection considerations, it is crucial to examine how these factors could affect metaverse development.

4.1 Intensive Data Collection and Detailed Profiling

Virtual environments are designed to support extensive data integration, enabling the processing of new categories of data with greater granularity and precision.⁵⁰ The Metaverse is characterised by pervasive data collection practices, which could involve real-time monitoring and analysis of user actions, interactions, and preferences, resulting in collecting 'more than ever user data'.⁵¹ Given this, it is possible to assert that the metaverse forms 'a big data network, which will bring huge data processing pressure to the digital world'.⁵²

⁴⁶ Vivek Nair and others, 'Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data' (2023) 32nd USENIX Security Symposium (USENIX Security 23), 895-910, <<https://www.usenix.org/conference/usenixsecurity23/presentation/nair-identification>> accessed 15 November 2024

⁴⁷ Bailly Martin, 'Privacy in a Programmed Platform: How the General Data Protection Regulation Applies to the Metaverse' (2022) 36 Harvard Journal of Law & Technology 1, 235

⁴⁸ BEUC, The European Consumer Organisation 'Call for Evidence on an EU Initiative on Virtual Worlds' (2023) <https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-053_Call_for_evidence_on_an_EU_initiative_on_virtual_worlds.pdf> accessed 5 November 2024

⁴⁹ Martin (n 47) 252.

⁵⁰ Agencia Española de Protección de Datos (n 12).

⁵¹ Lee and others. (n 30) 25.

⁵² Jiayi Sun and others, 'Big Data Meets Metaverse: A Survey' (2022) arXiv preprint, arXiv:2210.16282, 1 <<https://doi.org/10.48550/arXiv.2210.16282>>

This situation not only gives rise to new privacy concerns but also amplifies existing ones,⁵³ elevating 'the risk of invasion of privacy'.⁵⁴ For instance, these spaces could monitor the user's features such as facial expressions, voice inflections, postures and, if allowed, vital signs, including heart rate, blood pressure, respiration rate, pupil dilation, and even galvanic skin response.⁵⁵ Moreover, the immersive aspect of the Metaverse could reduce the users' ability and perception to make decisions that avoid the collection and processing of personal data.⁵⁶

The Metaverse also enables a new level of user profiling. Metaverse stakeholders can currently track behavioural patterns to construct user profiles. However, the scope of profiling within the Metaverse is expected to expand significantly as new forms of personal data are collected. This extensive data gathering and recording have the potential to give rise to the creation of highly complex user profiles. By combining various data types, which encompass declared, observed, and inferred personal information, specific personal attributes and interactions can be uncovered. This allows for a level of knowledge and profiling of individuals that surpasses what was previously achievable in social networks.⁵⁷ Highly detailed profiles pose significant risks to the users' rights and freedoms. Individuals could be categorised into specific groups, which can restrict their options and potentially erode their freedom. As a result, these data processing activities can potentially perpetuate or reinforce stereotypes, patterns of discrimination, and social segregation. For example, this could materialise as limitations on avatars' access to certain virtual spaces based on their social and emotional interactions or characteristics such as religious beliefs, sexual orientation, or racial and ethnic background.

One of the main challenges of processing data within the metaverse is the complexity and diversity of the data sources and types. The metaverse 'can be seen as a digital copy of what we see in our reality',⁵⁸ where some interactions occur 'in "mirror worlds" that duplicate real-life environments'.⁵⁹ Given this, the data collected in the metaverse includes not only the actions and reactions of users, but also their (passive and active) sensory inputs,⁶⁰ which are continuously recorded, such as eye and body tracking (for instance, it could be possible 'visualizing, recording and synchronizing experiences in VR with human body signals').⁶¹ Furthermore, data collection does not only involve the primary user of a system or service, but also the secondary users who interact with them and just occasionally utilise the virtual world's tools. This is common in communication platforms, social media, and collaborative tools, and may be even more prevalent in large-scale, immersive, and 'persistent multiuser environment'.⁶²

⁵³ Martin (n 47) 254.

⁵⁴ Wang and others. (n 14) 14672.

⁵⁵ Louis Rosenberg, 'The Growing Need for Metaverse Regulation' (2023) in Kohei Arai (ed) *Intelligent Systems and Applications. IntelliSys 2022. Lecture Notes in Networks and Systems*, vol 544. (Springer, Cham). <https://doi.org/10.1007/978-3-031-16075-2_39>, 544.

⁵⁶ Philipp Koehler, 'The Metaverse and some of its emerging challenges for data protection law' (*TaylorWessing*, 10 October 2022) <<https://www.taylorwessing.com/en/insights-and-events/insights/2022/10/the-metaverse-and-some-of-its-emerging-challenges-for-data-protection-law>> accessed 15 November 2024

⁵⁷ Agencia Española de Protección de Datos (n 12).

⁵⁸ Lee and others. (n 30) 39.

⁵⁹ Janna Anderson and Lee Rainie, 'The Metaverse in 2040' (*Pew Research Center*, 30 June 2022) <<https://www.pewresearch.org/internet/2022/06/30/the-metaverse-in-2040/>> accessed 15 November 2024

⁶⁰ Mystakidis (n 28) 488.

⁶¹ Leonardo Angelini and others, 'Towards an Emotionally Augmented Metaverse: a Framework for Recording and Analysing Physiological Data and User Behaviour' (2022). 13th Augmented Human International Conference, 1-5 <<https://doi.org/10.1145/3532530.3532546>> accessed 15 November 2024

⁶² Mystakidis (n 28) p.486.

Building upon the earlier point, the wealth of data available within virtual environments allows advertisers to craft highly personalised and, at times, invasive advertisements inside the metaverse (e.g., avatar-based ads).⁶³ Furthermore, advertisers may be able to more accurately assess the impact of their advertising on individuals using data collected by XR technology, such as eye movement, pupil dilation and heartbeat.⁶⁴ Such practices can result in continuous surveillance and encroach upon individuals' intimate space, affecting autonomy over their virtual experiences.

4.2 Identity, Authentication and Anonymity

In virtual spaces, the abundance of varying identity requirements across different platforms can introduce considerable challenges and risks for users. These issues range from threats of identity theft to online harassment.⁶⁵ It is important to note the 'extent to which biomechanics may serve as a unique identifier in VR, on par with widely used biometrics such as facial or fingerprint recognition'.⁶⁶

Avatars may not provide sufficient protection for users' real identities, as they may be linked to personal information or accounts that metaverse service providers can access and share with other stakeholders. A small amount of data may be sufficient to identify users in virtual worlds, potentially erasing any chance of genuine anonymity in these virtual environments.⁶⁷ [T]he most basic data stream needed to interact with a virtual world – simple motion data [basic data points tracked by virtual reality systems] – may be all that's required to uniquely identify a user within a large population [...] Researchers often refer to this as "telemetry data" and it represents the minimal dataset required to allow a user to interact naturally in a virtual environment'.⁶⁸

Additionally, motion data streaming is a key component of the metaverse. It can reveal specific personal characteristics of users, such as their height, dominant hand, and gender. By combining this data with other information gathered in virtual and augmented environments, this motion-based fingerprinting technique can increase the accuracy of user identification.⁶⁹

In this context, it's crucial to recognise that, at best, avatars have pseudo-anonymised information features that may expose users' real-life identities in some cases, through inferences and profiling. There would be a relationship between the physical and demographic attributes assigned to avatars in a virtual environment and how those attributes correspond with the characteristics of the users' authentic selves and their

⁶³ Kyle Coble, Jay Ratican and James Hutson, 'Beyond the pixelated mirror: Understanding avatar identity and its impact on in-game advertising and consumer behavior' (2023) *Metaverse*; 4(2): 2377. <doi:10.54517/m.v4i2.2377.> accessed 15 November 2024

⁶⁴ Bristows (n 37).

⁶⁵ Anna Maria Collard, 'Crime in the metaverse is very real. But how do we police a world with no borders or bodies?' (*World Economic Forum*, 18 August 2022) <<https://www.weforum.org/agenda/2022/08/crime-punishment-metaverse/>> accessed 15 November 2024

⁶⁶ Nair and others. (n 46) 895.

⁶⁷ Ronald Leenes, 'Privacy in the Metaverse: Regulating a complex social construct in a virtual world' (2008) in Simone Fischer-Hübner and others (eds) *The Future of Identity in the Information Society. Privacy and Identity 2007. IFIP – The International Federation for Information Processing*, vol 262. (Springer, Boston, MA). <https://doi.org/10.1007/978-0-387-79026-8_7> accessed 15 November 2024

⁶⁸ Rosenberg (n 41).

⁶⁹ *ibid.*

idealised selves.⁷⁰ In the same vein, special categories of personal data under article 9 GDPR may be involved when the avatar 'is a realistic representation of an individual, revealing that individual's skin tone, body shape and clothing.'⁷¹ It should be noted that special categories of data could also include assumptions or inferences about such data, especially when combined with other data or depending on the processing context or purposes.⁷²

4.3 Data Consent, Transparency and Control

Virtual spaces present complex challenges for data subject's autonomy, consent, and control over their data. Many digital platforms lack clear and simple terms of data usage, and do not enable users to easily modify their data-sharing preferences and monitor their data usage. Users are often unaware of how their data is processed and shared, which compromises their ability to give informed, specific, and voluntary consent.⁷³

These issues are more pronounced in metaverse environments, where multiple data controllers coexist and interact. Additionally, the collection of 'large amounts of personal data within a short period raises issues regarding the transparency of the personal data that is being processed'.⁷⁴ In such scenarios, obtaining informed consent from users is difficult and cumbersome. Metaverse contexts may also merge different purposes for processing, being difficult for the data subjects to consent for each purpose separately.⁷⁵ In this sense, it is suggested that there would be two possible ways to get consent and inform users in metaverses: using the same rules for the whole metaverse or using different rules for each entity.⁷⁶ Moreover, the validity of consent depends on the power balance between users and metaverse stakeholders.⁷⁷ A dominant or monopolistic position of a metaverse stakeholder can affect the users' freedom of choice and consent. Another important aspect of data protection in virtual spaces is to explore alternative legal grounds for data processing. For instance, the performance of a contract (Art. 6(1)(b) GDPR) may justify some data collection and processing activities in metaverses. However, this legal ground poses two main questions. The first one is how to determine the contractual necessity of the data processing, without allowing data controllers to alter users' reasonable expectations through terms and conditions. The other is how to evaluate the fairness of the contractual terms, and if the data processing is necessary for the

⁷⁰ Daniel Zimmermann, Anna Wehler and Kai Kaspar, 'Self-Representation through Avatars in Digital Environments' (2023) 42 *Current Psychology* 21775.

⁷¹ Bristows (n 37).

⁷² European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users. Version 2.0. Adopted on 13 April 2021' (2021) 30. <https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf> accessed 15 November 2024

⁷³ Jasmine Wang and Eddie Liu, 'Data Usage in Social Media' (*Medium*, 24 December 2020) <<https://medium.com/big-data-at-berkeley/data-usage-in-social-media-21d606ec4451>> accessed 15 November 2024

⁷⁴ Danique Knibbeler, Max Mohrmann and Sarah Zadeh, 'EU: Privacy and security concerns in the metaverse' (*DataGuidance*, August 2022) <<https://www.dataguidance.com/opinion/eu-privacy-and-security-concerns-metaverse>> accessed 15 November 2024

⁷⁵ *Ibid.*

⁷⁶ Koehler (n 56).

⁷⁷ Ljubisa Bojic, 'Metaverse through the prism of power and addiction: what will happen when the virtual world becomes more attractive than reality?' (2022) *European Journal of Futures Research* 10, 22. <<https://doi.org/10.1186/s40309-022-00208-4>> accessed 15 November 2024

performance of the contract(s) that the user agreed to, which could be hard given metaverse's extensive data-gathering and sharing model.

4.4 Territorial Scope of Data Regulations

Metaverses have a global cross-border scope, dependent on the 'free flow of information across platforms and boundaries of the physical world'.⁷⁸ In this context, it is necessary to identify the applicable legal framework(s) for worldwide accessible virtual spaces. The metaverse's decentralised structure, extensive interoperability, and the lack of specific regulations also add to this challenge.⁷⁹

Another challenge is to determine the exact location of end-users within the metaverse, which can be influenced by various factors. These factors include the physical coordinates of the individual controlling the avatar, the spatial position of the avatar within the virtual world, or the server's geographic location that handles the data. 'As the metaverse becomes more fully developed and jurisdictional issues relating to the location of the avatar to determine the appropriate forum to resolve potential dispute becomes unclear'.⁸⁰ The situation becomes more complex when there are multiple avatars, service providers, stakeholders, and other virtual personas involved.

A key issue in this context is the fragmented legal landscape regarding data protection and privacy, which may have different and sometimes conflicting requirements for every participant in the metaverse. 'In many cases, multiple privacy regimes will apply to the same data and even the same individual'.⁸¹ These requirements cover various aspects, such as transparency and information obligations, lawfulness, the rights of data subjects, reporting procedures for security breaches, and the rules for the cross-border transfer of data. In this line, '[u]niversal terms and conditions seem unlikely'.⁸² Moreover, identifying the relevant layers of domestic regulatory frameworks for ubiquitous virtual worlds can be challenging and time-consuming, as they may overlap with each other. This issue can pose significant difficulties for virtual environments that follow the legal regulations of the operator or developer's home country from the design phase, when building the metaverse's different infrastructures and its underlying technologies. They may not consider the data protection laws that may apply in other regions where their services are available or provided.

Given that data protection laws are regulations that address fundamental rights that cannot be waived, this may limit the choice of law terms or agreements.⁸³ For instance, the GDPR applies to the processing of personal data of data subjects in the EU by non-EU

⁷⁸ CNBCTV18 Team 'Data Privacy in the Contours of the Virtual World: Complexities of the Metaverse' (CNBCTV18, 10 September 2022) <<https://www.cnbctv18.com/views/view-data-privacy-in-the-contours-of-the-virtual-world-complexities-of-the-metaverse-14696621.htm>> accessed 15 November 2024

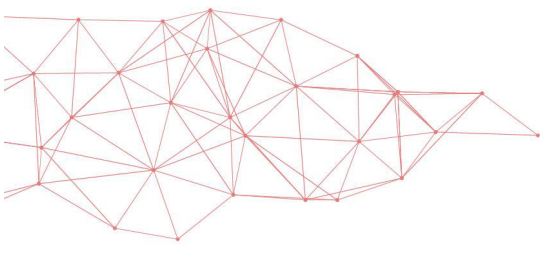
⁷⁹ Philipp Müller-Peltzer, 'The Metaverse: Data Protection in a New Virtual World | SRD' (Schürmann Rosenthal Dreyer, 15 June 2022) <<https://www.srd-rechtsanwaelte.de/en/blog/metaverse-data-protection/>> accessed 15 November 2024

⁸⁰ Cheong (n 9) p.471.

⁸¹ Matthias Artzt and Gary Weingarden, 'Metaverse and Privacy' (2022) 15(59) International In-House Counsel Journal 7763, 7765.

⁸² Norton Rose Fulbright, 'The Metaverse: The evolution of a universal digital platform' (Norton Rose Fulbright, November 2022) <<https://www.nortonrosefulbright.com/en-nl/knowledge/publications/5cd471a1/the-metaverse-the-evolution-of-a-universal-digital-platform>> accessed 15 November 2024

⁸³ Jie (Jeanne) Huang, 'Applicable Law to Transnational Personal Data: Trends and Dynamics' (2020) 21 German Law Journal 1283-1308 <<https://doi.org/10.1017/qlj.2020.73>> accessed 15 November 2024



platforms or third state-controllers or processors who are not established in a member state, if the processing activities are related to either offering goods or services to such data subjects in the Union, or monitoring their behaviour within the EU. Furthermore, platforms and metaverse operators cannot isolate the data of EU users from local users.⁸⁴ Regarding other clauses that could help interpret the metaverse terms and conditions and the contractual relationship between the provider and the user, it is important to note that '[t]his type of clause isn't universally enforced worldwide, so one may still face litigation in several forums'.⁸⁵

4.5 Responsibility, Accountability and Joint Controllershship

The metaverse dynamic and ever-evolving nature, where diverse platforms, services, and content coexists, poses significant challenges for data protection compliance, as it is hard to pinpoint a single entity accountable for data operations. 'To enable interoperability, data collected by one entity in the Metaverse may have to flow seamlessly between different operators and even platforms'.⁸⁶ Additionally, third-party developers often collect and process data on their own, which increases the complexity of data management. As the Metaverse expands and more entities interact within it, they will form a web of intricate connections, making it 'extremely difficult to attribute each of them to the given data protection roles defined by the GDPR'.⁸⁷ This exercise would involve 'picking apart a tangled web of relationships, and there may be no obvious or clear answers'.⁸⁸

In metaverse contexts, data controllers are parties or stakeholders who collect and process user data within the virtual space. They include "providers" ('the technology, platform and service providers that build the infrastructure and devices for the metaverse') and participants ('[i]ndividuals also known as end-users of the metaverse').⁸⁹

(i) Metaverse Platform Operator or Administrator: This is a key player in metaverse environments, as it has significant influence over the metaverse's architecture, policies, and user experiences. Their role is similar to that of a steward, who designs, oversees, and nurtures the virtual environment where countless users interact and engage. One of their main tasks is to establish and enforce the rules and regulations that govern the metaverse, such as user behaviour, content creation, and interaction. The operator also maintains the underlying infrastructure of the metaverse, ensuring its functionality and reliability. In the course of managing the metaverse, operators collect and process various types of information, ranging from basic user profiles to more sensitive data like user-generated content, communication records, and even biometric information. The purpose and scope of data collection may vary but often aims to personalise user experiences, enhance security, and optimise services. In addition to data management, operators have a crucial responsibility for ensuring the security and stability of the metaverse. This involves protecting the virtual world from disruptions, cyberattacks, and unauthorised access, so that users can interact safely and confidently.

⁸⁴ Bristows (n 37).

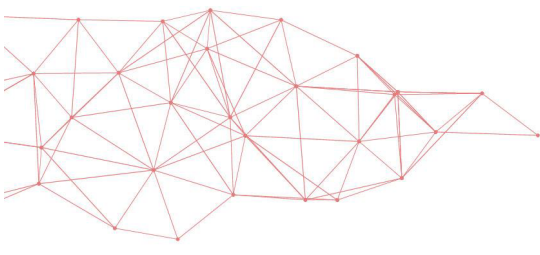
⁸⁵ Artzt and Weingarden (n 81).

⁸⁶ Norton Rose Fulbright (n 82).

⁸⁷ Koehler (n 56).

⁸⁸ Norton Rose Fulbright (n 82).

⁸⁹ World Economy Forum and Accenture, 'Interoperability in the Metaverse. Briefing Paper' (2023) World Economic Forum. <https://www3.weforum.org/docs/WEF_Interoperability_in_the_Metaverse.pdf> accessed 15 November 2024



(ii) Metaverse Service Providers: These are entities that offer different services within the metaverse, such as social interaction tools, e-commerce, or content hosting. Metaverse service providers also collect and process user data for their specific services, which makes them data controllers.

(iii) Third-Party Developers: These are developers who create applications, games, or experiences within the metaverse. They can be data controllers as well if they collect and process user data.

(iv) Users: In some cases, users themselves can act as data controllers. This happens when users create content, interact with others, or manage personal data within the metaverse.

The role and responsibility of each party may differ depending on the jurisdiction and the contractual terms applicable to a particular metaverse. Moreover, the nature of the metaverse, whether centralised or decentralised, can affect data control. In a centralised virtual space, the platform operator usually has more control and responsibility for data processing activities. This may entail access to a wider range of user data. Service providers operating within a centralised metaverse often have to comply with the platform operator's policies and standards. On the other hand, the distribution of responsibility is more balanced in a decentralised environment. Users tend to have more control over their data, and the governance structure may involve multiple stakeholders, thus sharing accountability across a network of actors. Service providers can operate with more independence.

In addition, the multiple entities involved in virtual worlds perform different roles, and their responsibilities and liabilities can change depending on the situation. It could be difficult to determine who are the (joint)controllers and (sub)processors according to the GDPR.⁹⁰ The lack of clarity about the roles of the entities involved in data processing⁹¹ may hinder the compliance with the data protection norms and duties. As a result, end-users/data subjects may face significant obstacles when they seek to enforce their rights against any data controller or processor.

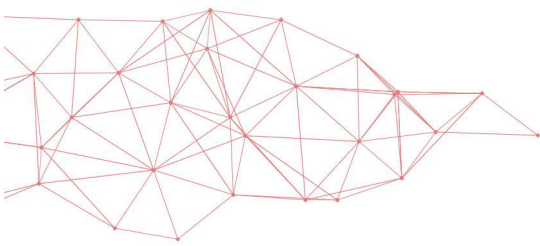
Article 26 GDPR delineates the concept of joint controllership, which arises when two or more entities collaborate in defining the objectives and methods of processing personal data. The determination of joint controllership hinges on the extent of involvement rather than the number of entities participating in the processing. According to the European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR, to be considered joint controllers, it is required that multiple actors collaboratively decide both the purpose and the means of processing, either through a shared decision or through converging/complementary decisions. This determination is contingent upon factual circumstances and is not contingent on potential contractual agreements among the involved parties. As per the Court of Justice of the European Union (CJEU), 'joint controllership may possibly stem from technical configurations'.⁹² The absence of access to personal data by one of the parties involved does not preclude the existence of joint controllership.⁹³ Furthermore, the CJEU clarifies

⁹⁰ Knibbeler and others. (n 74).

⁹¹ Koehler (n 56).

⁹² Jiahong Chen and others, 'Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption' (2022) 10 International Data Privacy Law 4, 279-293, 283 <<https://doi.org/10.1093/idpl/ipaa011>> accessed 15 November 2024

⁹³ Case C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH [2018] CJEU ECLI:EU:C:2018:388



that various operators may play distinct roles at different stages of data processing and may contribute to varying degrees.⁹⁴

4.6 Interoperability and Portability

The metaverse is often depicted as a singular concept, but it is more likely to comprise multiple virtual worlds, each created by different platform providers.⁹⁵ To enable a seamless and user-friendly transition between these diverse virtual spaces, platform providers need to focus on two essential elements: interoperability and data portability.

Interoperability can be defined as the ‘ability to interact, exchange and make use of data and resulting information to enable movement, transactions and participation across systems, platforms, environments and technologies’.⁹⁶ This concept refers to the ability of different virtual spaces, systems, or platforms to interact and function properly. Also referred as “cross-metaverse interoperability”, it provides ‘a seamless experience for users to interact with metaverses’,⁹⁷ reducing disruptions and friction in their digital experience. ‘Metaverse’s interoperability indicates the capacity to smoothly visit different virtual worlds in the Metaverse and move their data and assets to their preferred locations or Virtual Service Provider’.⁹⁸

Data portability right, described in Article 20 GDPR, allows data subjects ‘to receive the personal data a company processes about them and transmit that data to another company’.⁹⁹ This right is key for enhancing end-user’s experience and the interoperability of different platforms and services. It allows users to access, reuse, and transfer their data across various metaverses, fostering a user-centric environment. To achieve these goals, common technical standards, such as ‘standard data formats’,¹⁰⁰ are necessary. They prevent ‘vendor lock-in’, a situation where ‘end-users are stuck in a specific metaverse environment and cannot easily re-use their personal data’,¹⁰¹ limiting consumer choices.¹⁰² Currently, switching between metaverses is difficult for individuals, as each metaverse has its own protocols and there is little interoperability among them.¹⁰³

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1681248>.> accessed 15 November 2024

⁹⁴ Case C-40/17 *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV* [2019] CJEU EU:C:2019:629 <<https://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1680229>> accessed 15 November 2024

⁹⁵ Bristows (n 37).

⁹⁶ World Economy Forum and Accenture (n 89).

⁹⁷ Taotao Li and others ‘MetaOpera: A Cross-Metaverse Interoperability Protocol’ (2023) *IEEE Wirel. Commun.* 30(5): 136-143, p.136.

⁹⁸ Siem Ghirmai and others, ‘Self-Sovereign Identity for Trust and Interoperability in the Metaverse’ (2022) *IEEE Smartworld, Ubiquitous Intelligence \& Computing, Scalable Computing \& Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous \& Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta)*, 2468-2475, 2469. <doi:10.1109/SmartWorld-UIC-ATC-ScalCom-DigitalTwin-PriComp-Metaverse56740.2022.00345> accessed 15 November 2024

⁹⁹ Sanna Toropainen, ‘The right to data portability in the fair data economy – extending the right of individuals to benefit from managing their data’ (2023) *Sitra*, 13. <https://media.sitra.fi/app/uploads/2023/09/sitra_the-right-to-data-portability-in-the-fair-data-economy-final.pdf> accessed 15 November 2024

¹⁰⁰ Franklyn Ohai, ‘The Threat Landscape of Extended Reality: Beyond Privacy and Data Protection’ (*CiTiP KuLeuven*, 21 November 2023) <<https://www.law.kuleuven.be/citip/blog/the-threat-landscape-of-extended-reality-beyond-privacy-and-data-protection/>> accessed 15 November 2024

¹⁰¹ Knibbeler and others. (n 74).

¹⁰² European Parliamentary Research Service (n 11).

¹⁰³ Toropainen (n 99) 28.

4.7 Data Security Risks

The Metaverse poses a potential cybersecurity threat due to its additional data layer,¹⁰⁴ 'especially in terms of availability, resilience and confidentiality of personal data that are part of the processing carried out in the metaverse'.¹⁰⁵ The combination of metaverse core features -including socialization, immersive interaction, real world-building, and expandability, 'makes current security and privacy issues more critical'.¹⁰⁶

The security challenges in these virtual spaces vary depending on the platform architecture (centralised or decentralised), the processing activities, and the devices involved. Furthermore, there is an 'additional attack surface when integrating IoT data'.¹⁰⁷ This exposes them to unforeseen security problems.¹⁰⁸ Virtual worlds' security risks include 'personal information leakage, eavesdropping, data theft, unauthorized access, phishing, data injection, broken authentication, insecure design, and more'.¹⁰⁹

Determining when and how to control personal information becomes challenging due to the intricate nature of metaverse services, where different types of data exchange occur in real-time.¹¹⁰

The seamless transfer of data between devices necessitates a broader perspective on security, as relying solely on the security of individual devices or tools may not be sufficient for comprehensive data security. Therefore, prioritizing the security of the underlying infrastructure, networks and hardware devices is crucial,¹¹¹ which implies adopting a holistic "security by design" approach.¹¹²

4.8 Exercise of Data Subject's Rights in Immersive Digital Worlds

Given the metaverse's global accessibility, a patchwork of data protection laws may come into play. In these varying regimes, each carrying its own principles and rules, data protection rights and obligations can diverge significantly, contingent upon the data protection regime that applies to a particular case.¹¹³ As users traverse these virtual environments, they may encounter a dynamic interplay of regulatory frameworks, each with distinct requirements (both substantive and procedural), including specific data subject rights, the conditions for their exercise, and the available legal remedies.

¹⁰⁴ Mystakidis (n 28) p.493.

¹⁰⁵ Agencia Española de Protección de Datos (n 12).

¹⁰⁶ Yan Huang, Yi (Joy) Li, and Zhipeng Cai, 'Security and Privacy in Metaverse: A Comprehensive Survey' (2023), *Big Data Mining and Analytics*, vol. 6, no. 2, 234-247 <[doi:10.26599/BDMA.2022.9020047](https://doi.org/10.26599/BDMA.2022.9020047)> accessed 15 November 2024

¹⁰⁷ IBM Institute for Business Value, 'Seven Bets' (2023) IBM Corporation, 26. <<https://www.ibm.com/downloads/cas/GN7B276L>> accessed 15 November 2024

¹⁰⁸ Tuba Parlar, 'Data Privacy and Security in the Metaverse' (2023) in Fatih Sinan Esen, Hasan Tinmaz, Madhusudan Singh (eds) *Metaverse. Studies in Big Data*, vol 133 (Springer, Singapore 2023), 131. <https://doi.org/10.1007/978-981-99-4641-9_8> accessed 15 November 2024

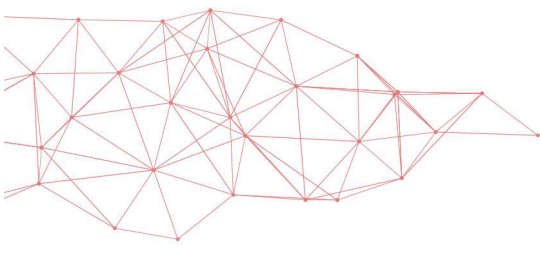
¹⁰⁹ Huang and others (n 106).

¹¹⁰ Dwivedi and others (n 4) 8.

¹¹¹ World Economy Forum with Accenture, 'Metaverse Privacy and Safety. Briefing Paper' (2023) World Economic Forum <https://www3.weforum.org/docs/WEF_Metaverse_Privacy_and_Safety_2023.pdf> accessed 15 November 2024

¹¹² Dwivedi and others (n 4) 8.

¹¹³ Artzt and Weingarden (n 81).



Moreover, the privacy policies of the metaverse technologies and devices are often broad and unclear, preventing data subjects from making informed choices as consumers.¹¹⁴

Exercising data subjects' rights in the metaverse presents many challenges.¹¹⁵ One of the primary difficulties is the cross-border nature of the metaverse. Users worldwide can interact within the same virtual environment, creating a jurisdictional tangle. Determining which data protection laws apply to each user's data and which authorities are responsible for enforcement can be convoluted. GDPR's extraterritorial reach adds an additional layer of complexity.

Another problem arises from the complex concept of identity within virtual worlds. In the metaverse, users commonly adopt pseudonyms or avatars, making it challenging to link their virtual personas to real-world identities. This ambiguity can hinder the precise identification and proper response to GDPR data subject requests. On the other hand, metaverse stakeholders may face challenges in de-identifying XR data, which could undermine the effectiveness of GDPR data anonymisation requirements.¹¹⁶

Moreover, decentralised metaverses and distributed ledger systems, given their features and governance design, make it challenging for users to exercise their rights, such as accessing their data or requesting its erasure. In decentralised systems, 'protecting users' privacy is completely their responsibility [...] because there is no central agency to monitor what occurs in these virtual environments'.¹¹⁷ 'Due to lack of clarity on the regulation of blockchain-based systems (which may be located abroad), law enforcement becomes a challenge'.¹¹⁸ Additionally, the ability to delete or rectify personal data might pose significant challenges when data is stored in encrypted or hashed databases. Finally, there may not be a straightforward way for users to reach out to data controllers or processors in the metaverse (who may hide behind proxies),¹¹⁹ and the lack of transparency regarding data handling practices further compounds these difficulties.

5. Conclusion

The metaverse represents a fusion of the physical and digital worlds, creating a dynamic and interconnected space powered by cutting-edge technologies 'designed to enhance our physical senses or foster immersive experiences with computer-generated

¹¹⁴ Natalia Menéndez González and Efe Bozkir, 'Eye-tracking devices for virtual and augmented reality metaverse environments and their compatibility with the European Union general data protection' (2023) Working Paper RSC 2023/69 Robert Schuman Centre for Advanced Studies Centre for a Digital Society. <https://cadmus.eui.eu/bitstream/handle/1814/76162/RSC_WP_2023_69.pdf?sequence=1&isAllowed=y> accessed 15 November 2024

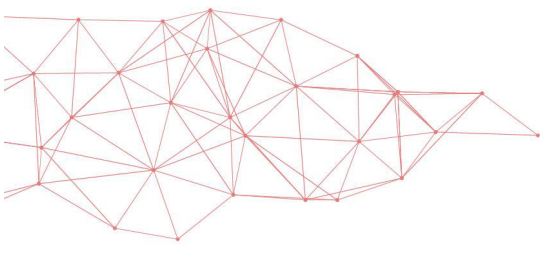
¹¹⁵ In the operation of the Metaverse, adherence to the rights of the individuals had not been feasible in some instances [for example] due to difficulties in identifying the parties responsible for data security. (Vibhushinie Bentotahewa and others 'Privacy and Security Landscape of Metaverse' (2023) in Nitin Naik and others (eds) *Advances in Computational Intelligence Systems. UKCI 2023. Advances in Intelligent Systems and Computing*, vol 1453. (Springer, Cham), 407. <https://doi.org/10.1007/978-3-031-47508-5_32> accessed 15 November 2024).

¹¹⁶ Shannon Pierson, 'Securing the Metaverse: Addressing Harms in Extended Reality' (2023) The Minderoo Centre for Technology and Democracy, 31. <<https://www.mctd.ac.uk/wp-content/uploads/2023/07/MCTD-SecuringTheMetaverse-Report-WEB-1.pdf>> accessed 15 November 2024

¹¹⁷ Ibukun Ogundare, 'Centralized vs Decentralized Metaverse: Complete Guide' (*Coinspeaker*, 16 February 2023) <<https://www.coinspeaker.com/guides/centralized-vs-decentralized-metaverse-complete-guide/>> accessed 15 November 2024

¹¹⁸ CNBCTV18 Team 'Data Privacy in the Contours of the Virtual World: Complexities of the Metaverse' (CNBCTV18, 14 September 2022) <<https://www.cnbctv18.com/views/view-data-privacy-in-the-contours-of-the-virtual-world-complexities-of-the-metaverse-14696621.htm>> accessed 15 November 2024

¹¹⁹ Artzt and Weingarden (n 81).



components'.¹²⁰ Central to its functioning is the intricate interplay of various platforms, hardware, software and IoT devices that collect vast and real-time big data.

This unprecedented level of data collection and processing raises a number of data protection challenges that need to be addressed in the metaverse. Some of the major ones are: detailed profiling of data subjects, adequate protection of digital identity, anonymity and re-identification, lawful data processing and transparency, cross-border data flows and territorial scope of different privacy/data protection regimes, responsibility and accountability, joint controllership, interoperability and portability, data security, and ensuring the exercise of data subjects' rights.

The architecture of virtual worlds plays a key role in grappling with these challenges. Its configuration poses difficulties in ensuring compliance with data protection principles such as purpose limitation and data minimisation. The need for interoperability and cross-platform integration also complicates the implementation of robust privacy and data protection measures across the metaverse ecosystem.

It is argued that the principle of data protection by design and by default is crucial when dealing with these challenges, which requires privacy considerations to be integrated into the systems' architecture at the earliest stages of their development. However, the application of this principle in virtual spaces contexts faces hurdles due to the metaverse's underlying dynamics, overlapping components and vast network of technologies, considering also fragmented privacy regulatory approaches and requirements. This approach should be embedded not only in each of the metaverse components, but also in the metaverse as a whole and in its interaction with other virtual worlds.

¹²⁰ Elizabeth Renieris, 'Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse' (2023) MIT Press, 112.



Bibliography

Agencia Española de Protección de Datos, 'Metaverse and Privacy' (AEPD, 29 September 2022)

Anderson J and Rainie L, 'The Metaverse in 2040' (*Pew Research Center*, 30 June 2022)

Angelini L and others, 'Towards an Emotionally Augmented Metaverse: a Framework for Recording and Analysing Physiological Data and User Behaviour' (2022) 13th Augmented Human International Conference, 1
<<https://dl.acm.org/doi/abs/10.1145/3532530.3532546>>

Antin D, 'The Technology of the Metaverse, It's Not Just VR' (*Medium*, 5 May 2020)

Artzt M and Weingarden G, 'Metaverse and Privacy' (2022) 15(59) *International In-House Counsel Journal* 7763.

Auletta E, Tugnoli F and Iovane G, 'Personal data protection in the Metaverse: operational challenges and regulatory uncertainties' (*ICTLC*, 28 September 2022)

Bentotahewa V and others, 'Privacy and Security Landscape of Metaverse' (2023) In Nitin Naik and others (eds) *Advances in Computational Intelligence Systems. UKCI 2023. Advances in Intelligent Systems and Computing*, vol 1453. (Springer, Cham), 407.
<https://doi.org/10.1007/978-3-031-47508-5_32>.

BEUC, The European Consumer Organisation 'Call for Evidence on an EU Initiative on Virtual Worlds' (2023)

Bojic L, 'Metaverse through the prism of power and addiction: what will happen when the virtual world becomes more attractive than reality?' (2022) *Eur J Futures Res* 10, 22.
<<https://doi.org/10.1186/s40309-022-00208-4>>

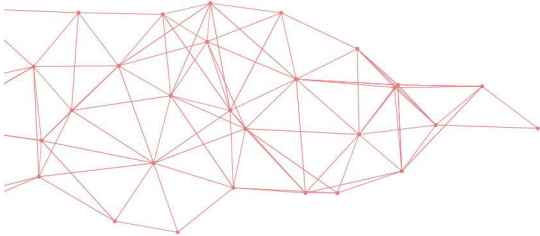
Bolognini L, and Carpenelli M, 'The future of personal data in the Metaverse' (2022) *Istituto Italiano per la Privacy e la Valorizzazione dei Dati*, 8.

Boraham J, 'What Is Metaverse Virtual World? [+4 Metaverse Realities]' (2022)

Bristows, 'Data protection in the metaverse' (2022)

Chen J and others 'Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption' (2022) 10 *International Data Privacy Law* 4, 279-293, 283.

Chester Cheong B, 'Avatars in the metaverse: potential legal issues and remedies' (2022) *Int. Cybersecur. Law Rev* 3, 467-494.



Christensen L and Robinson A, 'The Potential Global Economic Impact of the Metaverse' (2022) Analysis Group, 2.

CNBCTV18 'Data Privacy in the Contours of the Virtual World: Complexities of the Metaverse' (2022)

Coble K, Ratican J and Hutson J, 'Beyond the pixelated mirror: Understanding avatar identity and its impact on in-game advertising and consumer behavior' *Metaverse* 2023; 4(2): 2377. <doi: 10.54517/m.v4i2.2377.>

Collard A, 'Crime in the metaverse is very real. But how do we police a world with no borders or bodies?' (*World Economic Forum*, 18 August 2022)

Dwivedi Y and others, 'Metaverse beyond the Hype: Multidisciplinary Perspectives on Emerging Challenges, Opportunities, and Agenda for Research, Practice and Policy' (2022) 66 *International Journal of Information Management* 102542,2

European Commission and the Multi Stakeholder Platform on ICT Standardisation (MSP), 'Rolling Plan for ICT Standardisation - Metaverse' (2023)

European Data Protection Supervisor, 'Metaverse' (EDPS)

European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, 'Metaverse - Study requested by the JURI Committee' (2023) 10.

European Parliamentary Research Service (EPRS), 'Metaverse: Opportunities, Risks and Policy Implications' (2022)

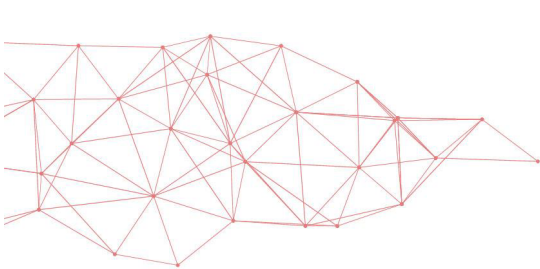
General Secretariat of the Council of the European Union, Analysis and Research Team (ART), 'Metaverse - Virtual world, real challenges' (2022).

Ghirmai S and others 'Self-Sovereign Identity for Trust and Interoperability in the Metaverse' (2022) *IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta)*, 2468-2475, 2469.

GlobalData Thematic Intelligence, 'Data Privacy Concerns Will Be Amplified by the Metaverse' (*Veredict*, 20 January 2023)

Goldberg M and Schär F, 'Metaverse Governance: An Empirical Analysis of Voting within Decentralized Autonomous Organizations' (2023) 160 *Journal of Business Research* 113764.

Hashash O and others, 'Towards a Decentralized Metaverse: Synchronized Orchestration of Digital Twins and Sub-Metaverses' (2023) *ICC 2023 - IEEE International Conference on Communications, Rome, Italy, 2023*, 1905-1910, <doi: 10.1109/ICC45041.2023.10279406>



Huang J, 'Applicable Law to Transnational Personal Data: Trends and Dynamics' (2020) 21 German Law Journal 1283.

Huang Y, Li Y and Cai Z, 'Security and Privacy in Metaverse: A Comprehensive Survey' (2023), in Big Data Mining and Analytics, vol. 6, no. 2, pp. 234-247, June 2023, <doi:10.26599/BDMA.2022.9020047>

Huynh-The T and others 'Artificial Intelligence for the Metaverse: A Survey' (2023) Engineering Applications of Artificial Intelligence, Volume 117, Part A, 105581, ISSN 0952-1976, <<https://doi.org/10.1016/j.engappai.2022.105581>>

IBM Institute for Business Value, 'Seven Bets' (2023) IBM Corporation, 26.

Kelly N, "Works like Magic": Metaphor, Meaning, and the GUI in Snow Crash' (2018) 45 Science Fiction Studies 69.

Kim K and others, 'Metaverse Wearables for Immersive Digital Healthcare: A Review' (2023) Adv. Sci. 2023, 10, 2303234. <<https://doi.org/10.1002/adv.202303234>>

Knibbeler D, Mohrmann M and Zadeh S., 'EU: Privacy and security concerns in the metaverse' (*DataGuidance*, August 2022)

Koehler P, 'The Metaverse and some of its emerging challenges for data protection law' (*Taylor Wessing*, 10 October 2022)

Kshetri N, 'A Typology of Metaverses' (2022) 55 Computer 150.

Lee L-H and others, 'All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda' (2021) Journal of Latex Class Files, Vol. 14, No. 8, September 2021.

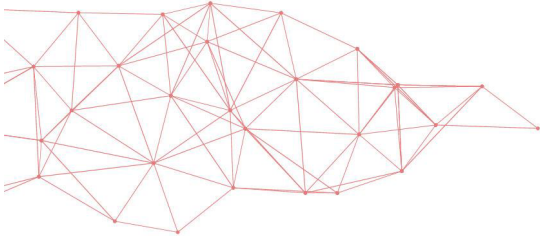
Leenes R, 'Privacy in the Metaverse' (2008) in Simone Fischer-Hübner and others (eds) *The Future of Identity in the Information Society. Privacy and Identity 2007*. IFIP – *The International Federation for Information Processing*, vol 262. (Springer, Boston, MA). <https://doi.org/10.1007/978-0-387-79026-8_7>

Li T and others 'MetaOpera: A Cross-Metaverse Interoperability Protocol' (2023) IEEE Wirel. Commun. 30(5): 136-143.

Martin B, 'Privacy in a Programmed Platform: How the General Data Protection Regulation Applies to the Metaverse' (2022) 36 Harvard Journal of Law & Technology 1, 235

Menéndez González N and Bozkir E, 'Eye-tracking devices for virtual and augmented reality metaverse environments and their compatibility with the European Union general data protection' (2023) Working Paper RSC 2023/69 Robert Schuman Centre for Advanced Studies Centre for a Digital Society.

Mystakidis S, 'Metaverse' (2022) Encyclopedia 2, no. 1, 486-497.



Müller-Peltzer P. 'The Metaverse: Data Protection in a New Virtual World | SRD' (*Schürmann Rosenthal Dreyer*, 15 June 2022)

Nagendran A and others, 'Avatar Led Interventions in the Metaverse Reveal That Interpersonal Effectiveness Can Be Measured, Predicted, and Improved' (2022) 12 *Scientific Reports* 21892.

Nair V and others, 'Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data' (2023) 32nd USENIX Security Symposium (*USENIX Security* 23), 895--910

Ogundare I, 'Centralized vs Decentralized Metaverse: Complete Guide' (*CoinSpeaker*, 16 February 2023)

Ohai F, 'The Threat Landscape of Extended Reality: Beyond Privacy and Data Protection' (*CiTiP KuLeuven*, 21 November 2023)

Parlar T, 'Data Privacy and Security in the Metaverse' (2023) in Fatih Sinan Esen, Hasan Tinmaz, Madhusudan Singh (eds), *Metaverse. Studies in Big Data*, vol 133. (Springer, Singapore 2023), 131. <https://doi.org/10.1007/978-981-99-4641-9_8>

Pierson S, 'Securing the Metaverse: Addressing Harms in Extended Reality' (2023) *The Minderoo Centre for Technology and Democracy*, 31.

Renieris E, 'Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse' (2023) MIT Press, 112.

Rosenberg L, 'The Growing Need for Metaverse Regulation' (2023) in Kohei Arai (ed) *Intelligent Systems and Applications. IntelliSys 2022. Lecture Notes in Networks and Systems*, vol 544. (Springer, Cham). <https://doi.org/10.1007/978-3-031-16075-2_39>

Rosenberg L, 'Privacy in the Metaverse might be Impossible (new research study)' (*Medium*, 30 March 2023)

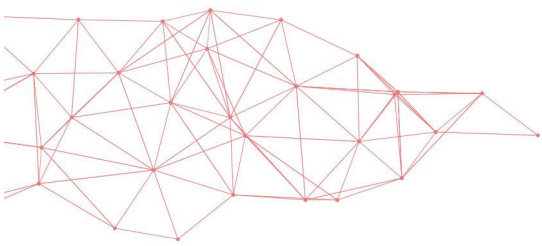
Sun J and others, 'Big Data Meets Metaverse: A Survey' (2022) arXiv preprint, arXiv:2210.16282, 1.

Toropainen S, 'The right to data portability in the fair data economy - extending the right of individuals to benefit from managing their data' (2023) *Sitra*, 13.

Ud Din I and others, 'Integration of IoT and Blockchain for Decentralized Management and Ownership in the Metaverse' (2023) 36 *International Journal of Communication Systems* e5612.

Wang H and others, 'A Survey on the Metaverse: The State-of-the-Art, Technologies, Applications, and Challenges' (2023) 10 *IEEE Internet of Things Journal* 16, 14671-14688.

Wang J and Liu E 'Data Usage in Social Media' (*Medium*, 24 December 2020)



World Economic Forum, 'Social Implications of the Metaverse' (2023)

World Economy Forum and Accenture, 'Interoperability in the Metaverse. Briefing Paper' (2023)

Zhang X and others, 'The Metaverse in Education: Definition, Framework, Features, Potential Applications, Challenges, and Future Research Topics' (2022) 13 Frontiers in Psychology.

Zimmermann D, Wehler A and Kaspar K, 'Self-Representation through Avatars in Digital Environments' (2023) 42 Current Psychology 21775.



MetaverseUA
Chair



Universitat d'Alacant
Universidad de Alicante

