Global Journal of Human-Social Science: H
Interdisciplinary
Volume 23 Issue 1 Version 1.0 Year 2023
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-460x & Print ISSN: 0975-587X

# Data Protection in the Metaverse: Concerns and Implications

By Hedaia-T-Allah Nabil Abd Al Ghaffar

*Cairo University*

*Abstract-* In a world still striving for securing data protection and data sovereignty, the metaverse comes as one of the latest trends in technological developments and waves. Similar to its previous counterparts, the idea opens up a multitude of risks and threats, coming hand-in-hand with the opportunities it creates. This research paper tries to explore the possible data protection concerns and implications of the metaverse. The paper approaches this novel topic through the 'Life Cycle of Data Threat Model' that tries to pinpoint some threats in different stages of the data life cycle. The paper then tries to find out some emerging policy trends regarding the introduction of the metaverse, building on the currently existing policy trends of countries in data protection.

*Keywords: metaverse, data protection, national security, data privacy, security threats, avatars, data sovereignty, data life cycle.*

*GJHSS-H Classification: FOR Code: 270707*

# Data Protection in the Metaverse: Concerns and Implications

Hedaia-T-Allah Nabil Abd Al Ghaffar

*Abstract-* In a world still striving for securing data protection and data sovereignty, the metaverse comes as one of the latest trends in technological developments and waves. Similar to its previous counterparts, the idea opens up a multitude of risks and threats, coming hand-in-hand with the opportunities it creates. This research paper tries to explore the possible data protection concerns and implications of the metaverse. The paper approaches this novel topic through the 'Life Cycle of Data Threat Model' that tries to pinpoint some threats in different stages of the data life cycle. The paper then tries to find out some emerging policy trends regarding the introduction of the metaverse, building on the currently existing policy trends of countries in data protection.

*Keywords: metaverse, data protection, national security, data privacy, security threats, avatars, data sovereignty, data life cycle.*

## Introduction

The metaverse, as announced by Mark Zuckerberg in October 2021, is gaining noticeable momentum. Metaverse is expected to present huge economic and social opportunities such as in the health, education and industry sectors. However, this comes with a high cost; a wide range of risks on privacy, data protection, identity, cybersecurity, ownership, misuse, and digital sovereignty as well as economic and social risks such as impacts on vulnerable groups. Nevertheless, the metaverse is becoming a fact and reality each day, moving the world, even more, closer to the bigger idea of the metaverse. The metaverse model, as presented by Mark Zuckerberg, is a complicated futuristic idea of a one global metaverse, that requires some advanced technological and economic pillars to stand on. Despite still being quite far from this model with its prerequisites, the world is witnessing steady developments and manifestations of applying the idea, still scattered though featuring separate small metaverses rather than a one global metaverse. In this preparatory scene, it is very important to study the implications of the metaverse on privacy and data protection, being one of the biggest challenges posed by the metaverse. The paper sheds light on privacy and data protection concerns in the metaverse and how countries are preparing themselves for these challenges.

The importance of this topic comes in light of technological developments and their impact on national security. The concept of national security has been evolving over time as a result of the new challenges that pose risks to national security. The world has seen national security threats and domains widening from military and security threats to economic threats then to social and humanitarian threats, such as the food security and migration issues then finally to cybersecurity and data protection threats accompanied by technological developments. [1]. Due to the novelty of the topic, little literature is available to review, however, it is important to properly locate the study within a suitable theoretical perspective that can link it with other related topics. The paper uses the 'Life Cycle of Data Threat Model' in order to analyse the threats presented by the metaverse according to the lifecycle of data. The model depends on dividing the lifecycle of data into 7 stages; data generation, data transfer, data usage, data sharing, data storage, data archival and data destruction [2]. In this sense, the paper is a new addition to the research on data protection and national security threats. The paper hypothesizes that the metaverse is a challenge to data protection and that countries need to react legally in order to protect data privacy in the metaverse.

## I. The Metaverse Concept

Metaverse is also called ‘Web 3.0’, denoting the latest development of the Internet generations (Web 1.0 being the world wide web and Web 2.0 being social media). There is no unified definition of metaverse. Literally, it is ‘beyond universe’, and it is described as ‘an immersive and constant virtual 3D world where people interact through an avatar to enjoy entertainment, make purchases and carry out transactions with crypto-assets, or work without leaving their seat’. The term builds on several underpinnings; mainly technological and economic. [3]

Metaverse depends on several essential technologies; Virtual Reality (VR) and Augmented Reality (AR) that facilitate the entrance to the three-dimensional online environment through dedicated headsets and other devices connected to computers or games consoles. Artificial Intelligence helps create a virtual version of each user, called an ‘avatar’, who is the main player inside the metaverse, and is also used for seamless communications along with the Internet of Things technology. Economic underpinnings of the metaverse include cryptocurrencies and non-fungible tokens (NFTs) to monetize transactions inside the online

*Author: Ph.D in Political Science (Comparative Political Systems), Cairo University, Egypt. e-mail: hedaia2008@live.com*

world, backed by blockchain technology which helps in providing trust in the economic transactions.

The term 'metaverse' was first featured in the public consciousness through Zuckerberg's keynote presentation in 2021, however, it first originated in two novel works; Neal Stephenson's 1992 'Snow Crash' and Ernet Cline's "Ready Player One'. Those versions about the metaverse matter because they proved self-fulfilling as so far. Both versions present the metaverse as 'a massive, persistent, open and economically developed virtual world', in the sense that it is a world that never pauses, open for anyone with VR hardware, where avatars can work, socialize, play and carry out extensive trading of goods and services through electronic currencies. [4]

## II. Data Protection and Privacy Concerns in the Metaverse

As portrayed in the above section, metaverse will bring new dimensions to the data protection and privacy scene; where regulations of data protection have been so far tackling physical data about users/ people, and its movement between countries, the metaverse world will create totally new actors (avatars) in addition to the original users with massive amounts of data generated from new sources such as the data collected from facial and eye expressions, moving between different metaverses. This general idea carries many complications, concerns and policy issues to consider in terms of privacy and data protection. Some of the data protection and privacy concerns in the metaverse are presented in this section.

### a) *Complicated roles*

The metaverse world blur the roles and responsibilities that have been established by data protection regulations throughout the past years. It is difficult to determine responsibilities and liabilities in the metaverse. This is even more dangerous in the light of the massive amounts of data generated in the metaverse. It is unclear now who is responsible for storing, processing and safeguarding data. Also it is unclear who is responsible for compliance with laws and regulations where it was normally the controller's responsibility to ensure individuals can exercise their rights and parties comply with laws and regulations. Data agreements may also be very challenging in a decentralized world. [3], [5]

### b) *Data sharing and portability*

The metaverse will connect the person to their "avatar" or other digital representations. Therefore, countries would likely consider information collected about a metaverse user's activities to be personal data, subject to existing privacy and data protection laws. This raises complicated issues such as jurisdictional responsibilities as well as portability and interoperability considerations. [5]

Metaverse presents problems of interoperability and movement of users inside and between different metaverses, together with their data and assets. It is also unclear whether this creates duplication with the real-world movement of data. Determining jurisdictions in the metaverse is very challenging, as a result of adding a new important player "the avatar". Will jurisdiction apply according to the location of the real-world user or the avatar or the location of relevant servers? Some additional contractual requirements apply in many countries in addition to some localization requirements, it is unclear how will this be handled in the metaverse. It is also unclear how concepts of 'extra-territorial reach' present in the GDPR and other regulations will be applied in the metaverse. [3], [6]

### c) *Increase in the sources of data collection*

Users are likely to be providing more information about themselves than they are doing today, as a result of the diversity of sources of data collection. Instead of dealing with clear sources of data collection in the current situation, the metaverse will introduce new sources of data collection that may be very challenging to get users' consents on, such as eye-trackers that could give data and insights about emotions through the interpretation of facial expressions and brain wave patterns. Some legal experts recommend that metaverse regulations should be designed to limit the scope of emotion-responsive advertising.

Additionally, the modes used in the metaverse can pose high risks, that can be used to infringe privacy. In the metaverse environment, the players move their avatars around and the scene is observed by the player who can take either a first-person perspective and look through the eyes of their avatars, or a third-person perspective where the camera is not attached to the avatar allowing the player to watch both their own avatar as well as the environment around. In third-person perspective, which is sometimes the default, the camera can move independently of the avatar and can be taken to locations different from the avatars'. This practically allows the player to use the camera as a spying device. Even more, the camera can be attached to another avatar without this avatar's awareness. [3], [7]

One example of data sources that infringe privacy in the metaverse is some devices used in games such as Second Life Game [8]. A wrist watch for example, is provided for free in the Second Life. The watch reports the location of the watch wearer, plus any other avatars in proximity, then this data is reported to a database outside the virtual realm. The behavior of the watch wearer's friends within the avatar's proximity is monitored. Friends are unaware of the watch's function. Since the database is hosted on a website outside the virtual realm, it is within reach of search engines such as Google. This kind of real-virtual interaction poses privacy concerns and data protection infringements. [7], [9]

*d) Mass profiling*

With reference to the above concerns, metaverse poses risks of mass profiling that can be used for advertising, controlling people's decisions and state surveillance, through access to sensitive data such as emotional reactions and biometric data.

*e) Proliferation of illegal and harmful content*

The metaverse is described as one of the decentralized autonomous organizations (DAOs), where avatars are the main content creators. It is unclear how the metaverse can regulate illegal and harmful content such as sexual harassment, disinformation, extremist ideas and pornographic content. It is also unclear how the children rights will be protected in the metaverse.

*f) The legal identity of avatars*

It is still unclear whether it is necessary to grant legal personality to avatars to hold them responsible for their actions. Will this be separate from the legal identity of the original users or are they linked? Does this pose risks to data protection and the risks of user identification? Since there are no specific laws regulating avatars, the content that users reveal via avatars may breach the personal protection of users and make them identifiable. Additionally, it is allowable in the metaverse to create alternate accounts, named as Alts, which allows users to engage in the metaverse with different identities. These Alts provide a kind of anonymity which can be used for illegal acts and behaviors. [3],[5], [7]

*g) Intellectual property rights protection*

It is challenging to guarantee intellectual property rights in the metaverse, where content is distributed and replicated through Web 3.0 and blockchain-based platforms. NFTs were presented as some technical solution, however, there may raise issues around the applicable law and jurisdictions. [3], [5].

*h) Sharing data for investigative purposes*

It is still vague how will the data on metaverse be shared for investigative purposes. Cross-border investigations involving metaverse must be safeguarded by international treaties balancing considerations of security and data protection and privacy.

*i) Digital sovereignty implications*

The metaverse poses extensive risks regarding digital sovereignty of countries; how countries will be exercising sovereignty of their lands and citizens in all meanings, will the avatars be citizens, how would the sovereignty over lands be exercised in the metaverse. The scene has also witnessed many governments introducing digital banks in the metaverse, how will they exercise sovereignty versus the real world, how will they exercise sovereignty over their economies and currencies? Also it is unclear how countries will exercise sovereignty in terms of imposing taxes over citizens.

Some national values may be at risk as well, such as how freedom of expression and the protection of human rights and dignity may be guaranteed? Shall the metaverse get the world history back to some practices that the world bypassed throughout the years by regulations? The answers are still unclear. [10]

## III. Countries' Reactions towards Data Protection in the Metaverse

The Zuckerberg keynote presentation pushed many countries to act towards the metaverse. A handful of countries started introducing their own national metaverses, while others started drafting laws.

As an extension of the ideological and cultural trends in data protection, we can distinguish an American trend versus a European trend versus a Russian and Chinese trend. As it is the case with current data protection trends, the USA adopts a universal and global vision of the metaverse, while the EU launched the European Metaverse Initiative, supported by ideas such as the French aspirations of a European metaverse. The EU started setting the scene by introducing some regulations that would guarantee data protection and privacy in the metaverse, such as the Digital Services Act and the Digital Markets Act that came into force in November 2022. Both acts tackle content regulation and protection of users from online harm. This is in addition to the EU's Artificial Intelligence Act, which plays a critical role in regulating the identity of avatars and related content. Other European countries started to draft and amend regulations such as the French advertising authority which updated the guidelines to clarify the rules applicable to virtual universes. [11], [12],[13],[14],[15].

Russia has also announced the introduction of the Russian metaverse by 2025, in opposition to the American metaverse, which is considered as 'extremist' in the Russian view. The Russian metaverse is a national one and foreign metaverses will be limited by regulations. This is a very logical extension of the Russian trend in data protection [16]. Similarly, China introduced its first metaverse in November 2021 under state supervision. The city of Shanghai has already started introducing public services in the metaverse. [17]

South Korea Telecom operator SK has also introduced its own telecom metaverse and announced its extension to 49 countries [18], while the UAE introduced the first law of its kind 'Virtual Assets Law', as well as a separate virtual assets regulating entity and a metaverse strategy. [19]

In short, we can still see the struggle for dominance between western, Russian and Chinese models of hegemony and geopolitical race, with different reactions toward data protection in the metaverse.

We're also witnessing some calls for studying the different legal aspects of the metaverse, and introducing separate regulations for the virtual worlds, as the University of Amsterdam suggested that ‘Privacy of the virtual identity can neither be adequately protected by real-world privacy rights, nor by privacy enhancing technologies in the virtual platform. Therefore, the virtual right to privacy should be granted to avatars in respect of their bodily, locational, and informational privacy’ [20].

## IV. Conclusion

The metaverse carries inside it many opportunities, however, risks and concerns are very challenging and are expected to lead to revolutionary changes in behavioral, economic, social and data protection patterns. With respect to data protection challenges, and in light of the life cycle of data threat model, it can be concluded that the metaverse presents security threats with regard to almost all stages of the data life cycle. There are many challenges related to the data generation stage, such as the increase in the sources of data collection and the legal identity of avatars. Some other challenges are related to data transfer such as the issues of interoperability of the two worlds and how would the data be transferred. Other challenges relate to the usage stage, such as mass profiling threats and the proliferation of illegal and harmful content. There are also challenges related to the data sharing stage such as the questions posed about the legality of sharing data between the two worlds as well as the sharing of data for investigative purposes. The same goes for data storage, archival and destruction, where the metaverse concept poses many questions about those stages.

The metaverse concept poses many risks and threats to the data sovereignty of countries as a whole. Countries and the international community shall therefore act proactively before the actual introduction of the metaverse as portrayed in order to minimize the risks posed by the metaverse while getting the good of it.

## Acknowledgement

*This paper and the research behind it would not have been possible without the valuable contributions and support of my dad and supervisor, Dr. Nabil Abd Al Ghaffar, Professor of Political Science (Faculty of Economics and Political Science - Cairo University). In the loving memory of my beloved dad who contributed greatly in preparing the original text from which this paper is extracted.*

*To my beloved mum...Grateful for your love and support.*

## References Références Referencias

1. Abd Al Ghaffar, H.-t.N. (2020), "Government Cloud Computing and National Security", Review of Economics and Political Science, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/REPS-09-2019-0125
2. Dahshan, Mai Mansour, “*Data Security in Cloud Storage Services”.* Master Thesis, American University in Cairo, 2013, https://fount.aucegypt.edu/etds/1201/
3. European Parliament, European Parliamentary Research Services (June 2022) ‘Metaverse: Opportunities, Risks and Policy Implications’, available at: https://epthinktank.eu/2022/06/24/metaverse-opportunities-risks-and-policy-implications/
4. Gilbert, S. (June 2022), ‘The Political Economy of the Metaverse’, Instituit Francais Des Relations (Geopolitics of Technology Program), available at: https://www.ifri.org/en/publications/briefings-de-lifri/political-economy-metaverse
5. Smith, R., ‘Reed Smith Guide to the Metaverse’, Issue 1 (May 2021), available at: https://www.reedsmith.com/en/perspectives/metaverse
6. Abd Al Ghaffar, Hedaia-t-Allah Nabil, Data Protection Laws Trends: Practice and Debate, Social Science Research, Global Journals, 2021, available at: https://socialscienceresearch.org/index.php/GJHSS/article/view/3882
7. Leenes, R., Privacy in the Metaverse: Regulating a Complex Social Construct in a Virtual World, Tilburg University, Netherlands, available at: https://dl.ifip.org/db/conf/ifip9-6/fidis2007/Leenes07.pdf
8. Second Life Game: https://secondlife.com/
9. Lee C., et.al. (2007), Security Issues within Virtual Worlds such as Second Life, Edith Cowan University, Australian Information Security Management Conference, available at: https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1044&context=ism
10. CMS, Data Protection Challenges, the importance of cybersecurity, advertising regulation in the metaverse, available at: https://cms.law/en/int/publication/legal-issues-in-the-metaverse/part-3-data-protection-challenges-the-importance-of-cybersecurity-advertising-regulation-in-the-metaverse
11. Council of the European Union (March 2022), Metaverse-Virtual World, Real Challenges, available at:
12. Mangada, E., et.al., The Metaverse Challenges and Regulatory Issues, SciencesPo, Master in Public Policy and Master in European Affairs, Spring Semester 2022, available at:
13. Lomas, N., Europe wants to shape the future of virtual worlds with rules and taxes, 14th of September 2022, available at: https://techcrunch.com/2022/09/14/eu-metaverse-virtual-worlds-tax/

14. Goschenko, S., European Union to Launch Global Metaverse Regulation Initiative in 2023, September 2022, available at: https://news.bitcoin.com/european-union-to-launch-global-metaverse-regulation-initiative-in-2023/
15. European Data Protection Supervisor, EU Dashboard on Metaverse, available at: https://edps.europa.eu/press-publications/publications/techsonar/metaverse_en
16. The First Metaverse in the Russian Federation will appear In 2025-2026, 20th of September 2022, available at: https://bigasia.ru/en/content/news/society/pervaya-metavselennaya-v-rf-poyavitsya-v-2025-2026-godakh/
17. Holland and Knight, EU, South Korea, Japan Announce Metaverse Regulation Plans, 26th of September 2022, available at: https://www.hklaw.com/en/insights/publications/2022/09/eu-south-korea-japan-announce-metaverse-regulation-plans
18. Weissberger A., SK Telecom launches its metaverse platform 'ifland' in 49 countries and regions, 23rd of November 2022, available at: https://techblog.comsoc.org/2022/11/23/sk-telecom-launches-its-metaverse-platform-ifland-in-49-countries-and-regions/
19. PwC, The UAE Virtual Assets Market (2022), available at: https://www.pwc.com/m1/en/publications/documents/uae-virtual-assets-market.pdf
20. Tata Consultancy Services (2022), User Privacy Protection in the Emerging World of Metaverse, available at: https://www.tcs.com/content/dam/tcs/pdf/discover-tcs/Research-and-Innovation/user-privacy-protection-metaverse-experience.pdf