Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Privacy in the Metaverse

K. Bavana[a]

[a]VIT University, Chennai, India

Received 09 February 2022; *Accepted* 25 February 2022; *Published* 01 March 2022

There has been a lot of evolution in cyberspace since the dawn of the Internet, and we can expect our lives to be impacted even more in the future. However, the future may be closer than you think. We are experiencing a shift in the way we live due to the emergence of virtual environments such as augmented reality applications, social networks, and virtual worlds. New technology is finally catching up to our wildest sci-fi fantasies which will transform our lives as we know them. At this moment, we're taking a significant stride into the mainstream metaverse, which some see as the internet's future. The change never appeared more natural because of the additional outside forces. We adapted to being confined to our houses and isolated, and now we will be able to explore the globe at our leisure in enormous virtual landscapes. The metaverse is a three-dimensional virtual realm in which users may interact with their virtual surroundings and engage in social interactions utilizing advanced human-computer interface (HCI) technology. Metaverse offers a virtual reality experience that lets people immerse themselves in different kinds or forms of reality. It is a hybrid of physical and digital reality. With the metaverse growing and technology advancing, the goal is to provide users with an alternate hyper or ultra-real world. Since Metaverse has come up, there'll be privacy issues that the users will face. This article focuses on how the metaverse affects our privacy and what are the laws deal with concerning privacy are enough to regulate.

keywords: *metaverse, privacy, GDPR, augmented reality.*

INTRODUCTION

The immersive three-dimensional digital world has been left to the movie experience for many years. The rise of the metaverse, on the other hand, offers the possibility of translating common activities – such as working, going to a concert, traveling, shopping, and socializing – into a parallel digital realm. The phrase "metaverse" comes from science fiction literature. This term was developed by Neal Stephenson by combining the words "meta" and "universe" and introducing it to the audience in his novel "Snow Crash" in 1992[1]. The metaverse can include components such as 3D avatars, digital assets, and diverse events to support a virtual economy and enhance social connections by employing technologies such as virtual reality, augmented reality, and blockchain. While this notion may appear to be far off in the future, many features of the metaverse have already arrived. A 3D virtual world platform and a 3D open-world game are two popular examples. Major gaming firms are also building their versions of the metaverse. As a result of this interconnected universe, we should expect new difficulties and risks, particularly when it comes to our privacy. Metaverses will collect more information about us than any other platform ever has. As a result, the ramifications will be more severe. Technology can create a vast appeal for virtual reality, allowing everyone to participate in the metaverse experience. As a result, more people will log in, and more data will circulate through the metaverses veins[2]. For metaverse firms, developers, and users alike, data security and privacy are key considerations. This can lead to invasion of user privacy, potential theft of personal information, and other forms of fraud. Organizations that cannot address their data security and privacy rights in the Metaverse can face serious consequences in the long run. Another feature of Augmented Reality and Virtual Reality is the ability to prove both a habitual escape from reality and a need. Most people do not have the option to opt-out. Simply put, the metaverse is breaking down the boundaries between the real world and the virtual

[1] 'What is the future of your privacy in metaverse?' (*Data Privacy Manager,* 12 December 2021) <https://dataprivacymanager.net/what-is-the-future-of-your-privacy-in-facebook-metaverse/> accessed 04 February 2022

[2] Anwesha Roy, 'Metaverse Data Protection and Privacy: The next Big-tech dilemma' (*XR TODAY,* 21 December 2021) <https://www.xrtoday.com/virtual-reality/metaverse-data-protection-and-privacy-the-next-big-tech-dilemma/> accessed 04 February 2022

world to a level never seen before. We're still recovering from the internet's impact on personal rights protection, and the next round is already pounding at the door.

Marketers can now navigate where customers move their mouse or look at the screen thanks to the Internet. They can track body movements, brain waves, and physiological responses in the metaverse. When downloading a new app, many people agree to the Privacy Policy without reading it. They may be aware that businesses and advertising companies use information such as location and clicks to provide personalized advertising. Some customers may be aware that their data is shared with third parties but may feel that they have no influence or control over the situation. Users are outraged when a data breach or misuse of app user data occurs. However, this will not affect your decision to download the app or read the Terms of Service further. It's surprising when you consider that more people are buying virtual reality headsets, augmented reality glasses, and AI-enabled products; these consumer behaviors will inevitably spread to the metaverse. But metaverse opens up a world of endless opportunities for businesses to create experiences, participate in world-building, and connect with customers in entirely new ways. However, this technique is not without risks. Deepfakes, big data, and cyber-attacks are all potential threats to a brand and customer reputation. Since these sorts of technologies are already gaining traction, marketers must be metaverse-savvy[3]. The virtual reality environment has the potential to offer Facebook another online monopoly, as well as be addicting and capture even more personal data from users.[4]

To participate in the Metaverse, you need to collect a large amount of personal information. Organizations can now track how people navigate the Internet and explore apps on smartphone applications and websites. Tomorrow, businesses will be able to collect information about individuals' physiological responses, movements, and even brainwave patterns within the Metaverse, giving them a much better understanding of their customers' cognitive processes and behaviors. Users engaged in Metaverse activities are "logged in" for a

[3] Cathy Hackl, 'Now is the time to talk about Ethics and Piracy in the Metaverse' (*Forbes,* 2 August 2020) <https://www.forbes.com/sites/cathyhackl/2020/08/02/now-is-the-time-to-talk-about-ethics--privacy-in-the-metaverse/?sh=1be97308ae6c> accessed 04 February 2022

[4] Matthew Ball, 'The Metaverse: What it is, Where to find it, and Who will build it', (*Matthew Ball. Vc,* 13 January 2020) <https://www.matthewball.vc/all/themetaverse> accessed 04 February 2022

long period of time. As a result, Metaverse users no longer have to proactively provide personal information by unlocking their smartphones and browsing their favorite websites and apps. Instead, while individuals go about their virtual lives, their data will be collected in the background.

EXISTING LAWS THAT CAN BE APPLIED TO REGULATE THE METAVERSE

As we progress toward a more connected society, lawmakers throughout the world have been pressing for tougher privacy and data protection regulations. However, the law is frequently unable to keep up with technological changes. When it comes to the digital world, laws created a century ago and interpreted by judges who are often uninformed of current technology, especially cutting-edge technology, seldom perform a good job of justice. This kind of opportunity entails a lot of data security duties. When processing personal data in this new environment, companies creating or participating in metaverses must comply with data protection regulations. The Metaverses nature creates several questions about how that compliance will be implemented in practice. The EU's General Data Protection Regulation (GDPR) and the UK's Data Protection Act may both apply to the metaverse. However, given the metaverses' new nature, the mechanisms governing informed consent around data processing may need to be reconsidered to guarantee that users' rights are safeguarded. Furthermore, because the metaverse has no limits, we should expect that the GDPR will apply, although the sections dealing with data transmission and processing beyond the EU may need to be addressed. The GDPR applies based on the subject's location at the time their data is processed, not on their citizenship or home country.

Whether an organization determines the purposes and means of processing personal data (referred to as "controller" under the EU General Data Protection Regulation (GDPR)) or simply processes personal data on behalf of others (referred to as "processor" in GDPR), the data protection laws of many jurisdictions impose various obligations on organizations. Choosing how and why Metaverse processes personal data and deciding which organizations process personal data on behalf of others can be difficult. The **European Commission (EC) has proposed the Digital Services Act (DSA)**, which aims to improve user transparency and

safety in online settings while also allowing creative digital firms to grow. The introduction of responsibility and security requirements for digital platforms, services, and products by DSA is a significant component and thus raises questions on how to find a compromise between ensuring content moderation, data sharing and use, and regulatory oversight. Processed by the provider of digital intermediary services; avoiding unjustified fines for service providers. Vendors working in the Metaverse could anticipate facing similar challenges[5].

THE DIGITAL MARKETS ACT (DMA) OF THE EU WILL

- To detect gatekeeper platforms, create a new framework.
- Certain gatekeeper techniques should be required or prohibited.
- Give the European Commission greater investigative powers and the ability to enforce behavioral and structural solutions, such as divestitures.

According to the European Commission, the Gatekeeper platforms benefit from significant economies of scale, extremely powerful network effects, high levels of user dependency, locking effects, lack of multi-storage for the same purpose as end-users, vertical integration, and data-related advantages. These qualities expose users to take actions that can significantly reduce the competitiveness of "Core platform services" and may result in unfair treatment of businesses and end-users. The European Commission defined the core platform services based on the fact that these services are frequently controlled by highly centralized multi-sided platforms that serve as gateways for business users (Metaverse vendors) to connect their consumers and vice versa. According to the European Commission, gatekeeper authority is frequently abused through unfair behavior toward economically dependent business users (vendors) and customers, resulting in entry hurdles and limited competition in these sectors.

[5] 'The Metaverse: Evolution of a universal digital platform' (*Norton Rose Fulbright,* July 2021) <https://www.nortonrosefulbright.com/de-de/wissen/publications/5cd471a1/the-metaverse-the-evolution-of-a-universal-digital-platform> accessed 05 February 2022

Article 5 would impose several legal requirements on gatekeepers. The following are requirements for gatekeepers in connection to the Metaverse[6]:

- Do not merge personal data from core platform services with data from other gatekeepers or third-party services, and do not sign end users to other services without consent to the mixing of personal data. Such restrictions would have serious consequences in the absence of such agreement, as data exchange within the metaverse is necessary for the participant's uninterrupted travel.
- Businesses can promote offers to end-users and enter into contracts with them, but end users also have access and use of the content, subscriptions, features, and other items offered to them by their apps via the platform of the gatekeeper. The gatekeeper's core platform services are available regardless of whether the end-user uses them. The use of gating subsystems with distinct terms and conditions in the Metaverse might compromise seamlessness.
- Business users should not be forced to use, offer, or interact with a gatekeeper's identity service. Identity theft throughout the Metaverse will be a major issue, as it will affect how much control Metaverse stakeholders have over customer connections[7].

Proposed EU AI Regulations: A proposal for an AI Regulation has been published by the European Commission. Artificial intelligence may be able to facilitate many human interactions in the Metaverse. There would be some AI technologies would be banned, and AI providers and users would be required to comply with different duties regarding high-risk AI systems, as well as transparency obligations. If much human/system interaction within the Metaverse is seamless and driven by AI in the future, stakeholders can expect to be required to comply with regulatory requirements of this type in the years to come.

Protection of Personal Information Act, 4 of 2013 (POPIA): One of the essential criteria of the POPIA is transparency. The data subject whose information is collected by a responsible party

[6] Lisa Heens, Marty Hansen, & Vicky Ling, 'European Commission Proposes New Artificial Intelligence Regulation' (*Covington,* 24 May 2021) <https://www.covingtondigitalhealth.com/2021/05/european-commission-proposes-new-artificial-intelligence-regulation/> accessed 05 February 2022
[7] Lisa Heens (n 6)

must be informed that the responsible party is collecting such personal information and for what purposes. In essence, the data subject must have a sufficiently clear understanding of how, why, with whom, where, and when a responsible party processes their data. This is intended to give the data subject enough information to determine if the responsible party is processing their data lawfully. If not, the data subject has sufficient information to exercise their POPIA rights. It's unclear how open and transparent organizations like Meta will be when it comes to alerting data subjects about the data they're collecting and how it's being used. It still has to be seen how concerns like processing lawfulness will be addressed. Given the massive amount of personal data that will be available for processing via the metaverse, it will be fascinating to see how other concerns like reasonableness and minimalism of processing will be addressed. Furthermore, cybercrime concerns like illicit data mining and identity theft may and most likely will arise in the metaverse.

As a result, the question will be whether national regulators and governments are well-equipped and able to address the challenges raised above. The problems themselves aren't new, but the playing field is. As a result, it will be intriguing to see if governments can exhibit the required digital resources and awareness to address the governance, content moderation, and massive ramifications for privacy and data protection that new technologies like the metaverse will surely bring. But, more crucially, how will data subjects, i.e. individual Meta users; demand that their privacy and personal information be protected is an important question[8].

METAVERSE AND THE INDIAN LAWS

In the pre-Covid era, thinking about a metaverse could have seemed strange, but now that meetings, events, classes, and other activities are happening online, reaching out for a Metaverse might be considered a more sophisticated, technically challenging, but reasonable approach. The phenomenon didn't occur overnight; rather, it developed over a period of two to three decades. As a hypothetical Internet version, the Metaverse supports permanent, three-

[8] Ahmore Burger Smidt, 'The Metaverse and Data Privacy: Will regulation keep up?' (*Werksmans Attorney*, 1December 2021) <https://www.werksmans.com/legal-updates-and-opinions/the-metaverse-and-data-privacy-will-regulation-keep-up/> accessed 06 February 2022

dimensional virtual worlds on traditional computers and via virtual and augmented reality devices. The virtual world is one that many students, gamers, technologists, fashionistas, and other professionals long for. In order to produce Metaverse, using personal data for rendering services, a great number of sensors, and a great deal of software are necessary, which will make the process even more complicated. With the right standards and regulations, the metaverse and the digital world can be greatly enhanced. However, the lack of regulations can be the source of problems. Facial data, body language, and biometric data, as well as searches and other personal data, must be properly regulated to protect users from data breaches and to fix legislative loopholes. Without adequate protection of the data, firms may attempt to exploit it to create tailored ads and increase profits through effective advertising. The Central Government has issued particular standards to manage the data collected from users by the community. The current Data Protection System is governed by the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, promulgated under the Information Technology Act, 2000. The Act states that an organization's code compliance may be proved by having written security processes, and information security policies must encompass technological, operational, and physical security measures.

The Act aims to protect users' personal information from being shared without their consent. The Bureau of Indian Standards offered policy assurance to guarantee that data collection firms assure their clients of suitable privacy procedures and a Data Privacy Management System[9]. The applicable requirements do not clarify whether they apply to foreign organizations in India or Indian organizations outside of India; nonetheless, if the organization fails to comply with acceptable data privacy standards, it may be held liable for damages under the IT Act. The standard requires organizations to conduct periodic audits and to fund a data privacy expert group. Organizations must also devise, document, and maintain measures to reduce the risk of data breaches and protect personal information. Article 19 of the Indian Constitution guarantees every person the right to free speech and expression; nevertheless, the

[9] David B. Hoppe, 'Heavy Meta: Privacy and Cybersecurity in the Metaverse' (*Mondaq*, 25 January 2022) <https://www.mondaq.com/unitedstates/privacy-protection/1150088/heavy-meta-privacy-and-cybersecurity-in-the-metaverse> accessed 08 February 2022

same article sets some reasonable limitations on that right. The Act gives organizations the authority to prohibit the spread of fake news, as well as communication that is opposed to public policy, morality, decency, and state security. It is now up to the moral code and corporate ethics standards to judge if the content is offensive, deceptive, or compromising the security of the state. Section 69 of the Information Technology Act of 2000 empowers the Central Government and State Governments to issue orders authorizing the interception or decryption of any information in the interest of the state's security, sovereignty, and integrity. The government will and should monitor data in the Metaverse environment, and if it is regarded to be against public policy or state security, it may be withdrawn, and the organization penalized as a consequence of the regulations. Legal growth in the metaverse age would necessitate law inserting itself in a way that balances fundamental rights, like freedom of expression, with public interest protection. Other legal difficulties that we can't predict will emerge when portions of the Metaverse take shape. We should anticipate Metaverse stakeholders to face a slew of new difficulties that would apply in any trade or digital scenario, such as anti-money laundering concerns, sanctions, technology export limitations, financial services regulation, intellectual property infringement, and so on.

CONCLUSION

The metaverse raises complex issues that will very certainly necessitate changes to existing laws and regulations. Until then, instituting proper legal and technological safeguards can assist to limit risk and providing some safety for metaverse users. Emerging technology businesses operating in the metaverse should be well aware of the metaverses privacy legislation concerns. These businesses should consider putting in place their own privacy rules, personal data protection policies, data retention policies, data subject consent forms, licensing agreements, and other legal papers in the metaverse (or virtual platform). A law firm that specializes in emerging technologies may assist in the writing of these legal agreements as well as assist with the metaverses privacy and cybersecurity-related regulatory problems. Firms can follow some factors that they must consider while operating in the metaverse. The following can be a few factors that I have understood after a thorough study on the topic:

Consent mechanisms must improve when new data kinds are introduced: HCI devices may help in the collecting of many types of data, including biometric data from people. Users must be told about privacy issues, and consent procedures must be simple to follow. Consent should also be updated regularly, with no assumption of perpetual authorization, and these procedures should be improved with each new data type.

Transparent monetization can assist to alleviate worries about data exploitation: One of the most significant causes of data abuse is the widespread perception that the internet is a free service. In reality, ad revenues generated by ad targeting based on user data fuel services such as Google and Facebook. Some of the issues in the metaverse may be avoided if users were rewarded for their data collection. Cookies are turned off by default in privacy-focused browsers, and users may earn incentives or tokens if they want to see tailored adverts.

Data privacy and ease-of-use may be at odds: Finally, there will be situations when firms must choose between data privacy and user comfort or ease of use. Interoperability improves greatly when both platforms, for example, are regulated by a single set of terms and conditions. However, for the sake of the user, consent should be reaffirmed at every point of data re-entry, even if it means adding an extra authentication layer.

The first step in securing data safety and privacy in the metaverse is to build privacy-sensitive technologies from the ground up. Facebook has already taken certain moves in this direction. It recently decommissioned its face recognition technology, which could recognize when a user appeared in tagged images or other locations. It's also beefing up its age verification processes to ensure that interactions on its platforms are age-appropriate. The company has also created a Transfer Your Information (TYI) tool that is GDPR compliant and allows users to withdraw their data from Facebook at any time. Finally, the company is working on privacy-enhancing technologies (PETs), which combine encryption and statistical techniques to limit the usage of personal data for advertising purposes. All of these will contribute significantly to ensuring that users have access to a safe, private, and controlled metaverse. Even if the metaverse is a decade distant, those businesses establishing their own or expecting to operate

in one must adhere to identical rules right now. The metaverse might be the first true combat, putting our willingness to fight for our privacy to the test.