The New Approaches in Humanity
Journal Homepage: www.Nahq.ir

Review Article

Privacy Rights Conflicts in Digital Identity Management in the Metaverse Era

Amir Hasannia[1]

Master of Private Law, Member of the Mazandaran Province Judiciary Lawyers Center, Sari, Iran

ARTICLEINFO **ABSTRACT**

Keywords:

Urban Management,
Education Qulaity,
Higher Education,

Received:
07 May 2023
Received in revised form:
27 May 2023
Accepted:
22 June 2023
Published:
21 July 2023
pp.42-54

This article examines the conflicts of privacy rights in digital identity management in the metaverse era. Digital identity management in the metaverse faces numerous legal challenges, such as the incompatibility of existing laws with decentralized technologies, the right to "delete" under GDPR, and intellectual property issues. In addition, legal conflicts between jurisdictions, identity verification problems, and ethical threats also add to the complexities of this area. To create a safe and trustworthy environment, there is a need to develop appropriate legal and ethical frameworks and cooperation between legislators, technology professionals, and society.

Articles were searched based on the keywords of privacy rights, digital identity, metaverse in reputable databases and citations, including PubMed, Web of Science, Scopus, Google scholar, Science Direct, SID, and Magiran. All original articles were collected and reviewed for inclusion in the study. Screening criteria were applied in three stages by applying word and exclusion criteria; 33 articles were found at the beginning of the search. In the screening stage (first 4 stages), 11 articles were excluded from the study, and at the end of the screening stage, 22 articles related to the study objective remained, which were content evaluated and included in the study. To resolve legal conflicts in the metaverse, it is necessary to amend the laws to adapt to decentralized technologies and the use of hybrid blockchains. Also, international cooperation and the development of laws taking into account the ethical aspects of technology, along with the participation of various stakeholders, are necessary to create a safe and sustainable environment.

Citation: Hasannia, A. (2023). Privacy Rights Conflicts in Digital Identity Management in the Metaverse Era. *The New Approaches in Humanities*, 1(2), 42-54. doi: NAHQ/nahq.2023.220360

http:// NAHQ/NAHQ.2023.220360

[1] Corresponding author (Email: Amir.hasannia1984@gmail.com)

Introduction

With the advent of digital technologies, the concept of identity has significantly expanded and is no longer limited to a fixed set of data such as birth certificates or national ID cards. In the metaverse, digital identity serves as a representation of an individual's presence in the virtual environment, playing a crucial role (Mystakidis, 2022). These identities are typically depicted through avatars, which act as proxies for a person's physical, behavioral, and social characteristics (Cheong, 2022). One of the most pressing issues concerning digital identity in the metaverse is the conflict between data accessibility and privacy protection. Regulations such as the General Data Protection Regulation (GDPR) in the EU attempt to strike a balance between these two aspects. However, the decentralized and dynamic nature of the metaverse poses challenges to enforcing such laws (EUR-Lex, 2016).

The metaverse, as a 3D digital space, is currently one of the most significant technological advancements in the world. It allows users to interact and experience various activities through a sense of virtual presence. In this environment, users can present alternate versions of their identities through avatars and engage with others in digital form. However, as this virtual world rapidly expands, numerous legal challenges regarding digital identity protection have emerged (Ning et al., 2021). It is important to note that the metaverse, as an emerging platform, is already having a profound impact on various aspects of life due to advancements in information and communication technology (ICT). From social and economic to cultural dimensions, the metaverse enables users to explore new experiences and expand their social connections in a virtual setting. However, these developments also bring challenges, particularly in protecting users' digital identities (Singh, 2022).

The legal challenges associated with digital identity in the metaverse include

privacy concerns where users may share personal data that is at risk of exposure and misuse (Cheong, 2022), intellectual property rights where content creation in the metaverse can lead to legal disputes between users and platforms (Barfield, 2006), and questions regarding legal liability in cases of violations. Research indicates that while the metaverse allows users to express their digital identities, the lack of clear regulations can lead to legal anomalies (Beduschi, 2019). Therefore, there is a growing need for new legal frameworks to manage digital identities in the metaverse. Emerging technologies like blockchain could serve as an effective solution for protecting digital identities (Alam, 2019). Existing legal frameworks, such as the EU's GDPR and AI Act, could serve as models for protecting digital identities in the metaverse. These regulations can help users safeguard their personal data while still benefiting from the metaverse's features (Dremliuga et al., 2020). However, blockchain technology, while promising, presents contradictions with current laws (Michèle, 2019). For instance, public blockchains store immutable data, whereas GDPR grants users the "Right to be Forgotten", creating a legal conflict (Kondova & Erbguth, 2020).

Security risks in the metaverse include digital identity theft, data manipulation, and system breaches. Studies show that 34% of metaverse users are vulnerable to identity theft (Gadekallu et al., 2022). Solutions such as private or hybrid blockchains may enhance security, but they could conflict with the metaverse's decentralized nature (Strehle, 2020). Regarding intellectual property, questions arise over whether avatars and digital assets in the metaverse are protected under copyright laws (Barfield & Blitz, 2018). This issue becomes more critical as users purchase NFT-based digital assets. Current laws, such as Iran's "Data Disclosure Mandate" or the "National Data Management Law" (2022), have yet to fully address these concerns (A'akafi Ghazani, 2022).

This study examines the legal challenges surrounding digital identity in the metaverse and proposes solutions through a descriptive-analytical approach. Key findings suggest that targeted regulations and blockchain technology can effectively protect digital identities. By providing a comprehensive analysis of the

current and future state of digital identity in the metaverse, this research aims to assist policymakers in developing effective legal frameworks for this evolving digital landscape.

Methodology:

The present study is a review of articles published in both Persian and English between 2010-2023 in domestic and international journals, examining conflicts in private law regarding digital identity management in the metaverse era, with a focus on predefined inclusion criteria. Article searches were conducted using the following keywords of privacy rights, digital identity, metaverse in reputable databases and citation indices, including PubMed, Web of Science, Scopus, Google Scholar, Science Direct, SID, and Magiran. All original articles meeting the initial criteria were collected and reviewed. A three-stage screening process was applied based on inclusion and exclusion criteria: articles lacking the specified keywords in their titles were excluded, abstracts, theses, conference reports, congress proceedings, and lecture materials were excluded, articles available only as abstracts were removed and studies not thematically aligned with the research objectives were excluded. Initially, 33 articles were identified. After preliminary screening (first four stages), 11 articles were excluded. In the final screening stage, 22 articles relevant to the study's objectives remained and underwent content evaluation before being included in the review.

Results:

The search results include 22 domestic and international articles relevant to the study's objectives, presented below.

Latifzadeh et al. (2023) in a study titled "Introducing Digital Identity in the Metaverse: Identifying Legal Challenges and Seeking Solutions," using a descriptive-analytical method, has attempted to define digital identity in the

metaverse while addressing legal challenges related to virtual identities in this environment and proposing solutions to current dilemmas. According to the research findings, the selective application of specific laws and regulations such as the European Data Protection Regulation and the European Union's Artificial Intelligence Act, along with the use of appropriate blockchain technology, can be effective in providing meaningful protection for digital identities.

A'akafi Ghazani et al. (2022) in a study titled "Metaverse and Legal Challenges in Property Rights" found that while the metaverse is recognized as a new digital space, implementing current laws such as the European General Data Protection Regulation (GDPR) in this decentralized environment faces limitations. The research emphasizes that domestic laws such as the "National Data Management Law" enacted in 2022 lack the necessary details to support digital identities in the metaverse. Additionally, using blockchain technology as a potential solution for managing self-sovereign identities conflicts with existing laws regarding the deletion of personal data (the "right to be forgotten"). This study suggests that to address these challenges, existing laws should be adapted to the realities of decentralized technologies, consensus frameworks should be developed among metaverse platforms, and a combination of artificial intelligence and blockchain should be used to enhance data security.

Shakeri and Jafarpour (2021) in a study titled "Feasibility of Implementing Moral Rights of Authors Under New Information and Communication Technologies," published in the Journal of New Technologies Law, Volume 3, Issue 6, Pages 15-29 (DOI: 10.22133/mtlj.2022.360779.1120), found that moral rights in digital spaces (such as the metaverse) face challenges such as inability to identify copyright owners, unauthorized reproduction, and lack of appropriate legal frameworks. The authors suggest that domestic laws should be updated using digital mechanisms (such as artificial intelligence and blockchain) to protect intellectual property rights in virtual environments.

The "Mandatory Data and Information Disclosure Bill" (2020) focuses on data management in digital space but does not adequately address challenges related to digital identity in the metaverse. The bill mainly focuses on public access to government data and lacks necessary details for protecting personal data in virtual environments. This limitation highlights the need to adapt laws to new digital realities.

The "National Data and Information Management Law" (2022) provides a framework for protecting national data but lacks necessary details regarding decentralized digital identities in the metaverse. The law only addresses government and public organization data management and does not mention digital structures such as blockchain or self-sovereign identities. This deficiency creates a legal gap in protecting users' digital identities in virtual space.

The draft "Protection of Personal Data Bill" (2018) attempts to preserve personal data in digital space but is incompatible with the complexities of decentralized technologies (such as blockchain) in the metaverse. The bill partially grants users the right to access and modify personal data but ignores issues such as immutability of data recorded on blockchain and accountability of metaverse platforms. This highlights the need to amend and adapt laws to the realities of new technologies.

Mirshekari (2017) in the book "Personality Rights and Civil Liability Law in the European Union," findings show that the European Union's legal frameworks for protecting individual personality rights (such as privacy and intellectual property) in digital space can serve as a model for Iran. The book emphasizes that personality rights in virtual environments (such as the metaverse) should be adapted using mechanisms such as self-sovereign identities and smart contracts.

Gadekallu et al. (2022) in the article "Blockchain for Metaverse: A Review"

(Source: Computer Science), findings show that blockchain can serve as a technical solution for managing digital identities in the metaverse, but the immutability of data recorded on blockchain conflicts with the "right to be forgotten" under GDPR. The study suggests that using hybrid blockchain (a combination of public and private blockchain) can create a balance between security and compliance with legal regulations.

Kondova & Erbguth (2020) in the article "Self-Sovereign Identity on Public Blockchain and GDPR" (Source: ACM Symposium Journal, Pages 342–345), findings show that public blockchain (immutable) conflicts with the "right to be forgotten" under GDPR. The authors suggest that using private blockchain or alternative mechanisms can resolve this contradiction.

Mystakidis (2022) in the article "Metaverse" (Source: Encyclopedia, Volume 2(1), Pages 486–497), findings show that the metaverse as a digital space has challenges in digital identity management, data security, and intellectual property. The author emphasizes that global legal frameworks are necessary to manage these challenges.

Sullivan (2018) in the article "Digital Identity - From Emerging Legal Concept to New Reality" (Source: Computer Law & Security Review, Volume 34(4), Pages 723–731), findings show that digital identity represents individual rights in digital space, and protecting it in decentralized environments such as the metaverse creates extensive legal challenges. The author suggests that domestic laws should be updated using digital technologies (such as artificial intelligence and blockchain).

Barfield et al. (2018) in the book Research Handbook on Virtual and Augmented Reality Law (Edward Elgar Publishing), findings show that intellectual property rights for avatars and digital identities in the metaverse face challenges such as

unauthorized imitation, unlimited access to personal data, and lack of international legal frameworks. The authors suggest that intellectual property laws should be updated to protect digital identities in virtual space.

Discussion and Conclusion:

In the metaverse, digital identity management faces multiple legal conflicts, the most significant of which stem from the mismatch between existing laws and the realities of decentralized technologies. The GDPR, as one of the most comprehensive frameworks for personal data protection, is designed around centralized structures. However, the metaverse, through technologies like blockchain, stores data in immutable systems (Kondova & Erbguth, 2020).
This contradicts the "right to be forgotten" under the GDPR, since data recorded on public blockchains cannot be deleted (Michèle, 2019). This contradiction complicates legal accountability: Are blockchain developers, metaverse platforms, or users themselves responsible for GDPR compliance? One alternative is the use of private rather than public blockchains. Private systems offer more control over data and facilitate the enforcement of user rights under the GDPR (Strehle, 2020). However, this approach may conflict with the metaverse's principle of decentralization.

Another approach is the development of "Joint Controller Agreements" among metaverse platforms to distribute legal responsibilities among stakeholders (Colcelli, 2019). These frameworks can clarify the roles of governments, tech companies, and international institutions in data governance. In the realm of intellectual property, questions arise regarding the protection of avatars and digital assets like NFTs. Barfield & Blitz (2018) pointed out that unauthorized imitation of avatars and misuse of personal data highlight the need to adapt intellectual property laws to new conditions. Furthermore, Cheong (2022) found that 34% of metaverse users are exposed to digital identity theft, emphasizing the urgent need

for technical and legal solutions. On the technical side, integrating AI and blockchain could help detect and prevent identity theft (Heister & Yuthas, 2022). However, the use of AI in data management introduces ethical challenges, such as data-driven discrimination and privacy violations (Beduschi, 2019). These issues underscore the need to balance security with respect for individual rights. From a digital identity management researcher's perspective, the metaverse era brings numerous private law challenges that require careful study and appropriate legal solutions. One such challenge is the lack of transparency in data ownership. In the metaverse, users often create digital identities and data on decentralized platforms, which can lead to disputes over data ownership. For instance, if a user stores their data on a decentralized platform, questions arise about who has access rights to that data and who is responsible for its protection.

Another challenge is privacy. One of the biggest challenges in digital identity within the metaverse is protecting users' privacy. While blockchain technologies can help maintain privacy, their inherent transparency can also lead to the exposure of personal information. Users may worry that their real identities could be easily uncovered. Legal conflicts between jurisdictions are also a critical issue. Since the metaverse is a global space, laws and regulations from different countries may conflict. For example, data protection laws in the EU (like the GDPR) may not align with privacy laws in other countries. These conflicts can result in confusion and non-compliance.

Identity verification problems present another challenge. In the metaverse, user identification is largely based on digital addresses and decentralized identities. This can lead to difficulties in verifying real-world identities, causing legal issues in cases like fraud or identity theft. Intellectual property rights also face significant challenges in this space. Digital identity management in the metaverse is troubled by issues related to intellectual property. Users may use content created by themselves or others in the metaverse, but this raises questions about IP rights and how to protect them.

Ethical threats are another concern. Managing digital identity in the metaverse comes with ethical challenges. For example, using AI technologies to analyze and manage digital identities can lead to concerns about privacy and the violation of user rights. Ultimately, managing digital identity in the metaverse era requires the development of appropriate legal and ethical frameworks to address private law conflicts. It is necessary for lawmakers, tech experts, and society to work together to create a safe and trustworthy environment for users.

Table 1. Summary of Legal Conflicts in Digital Identity Management in the Metaverse

Topic	Legal Challenges	Proposed Solutions	Sources
Data Protection	Conflict between blockchain immutability and the GDPR's right to be forgotten.	Use of hybrid solutions (e.g., private and public chains) or off-chain storage of sensitive data.	(Michèle, 2019; Bernal Bernabe et al., 2019)
Ownership of Identity and Assets	Lack of clarity around ownership of avatars and digital assets (e.g., NFTs).	Define digital ownership rights in national and international laws and use decentralized registries.	(Barfield & Blitz, 2018; Belk et al., 2022)
Identity Fraud and Impersonation	Possibility of avatar copying and misuse of virtual identities.	Use multi-factor authentication (MFA) and blockchain-based self-sovereign identity (SSI) systems.	(Naik & Jenkins, 2020; Cheong, 2022)
Smart Contracts	Some smart contracts are incompatible with traditional legal frameworks (e.g., contract termination).	Integrate "Legal Smart Contracts" with enforceable clauses recognized by courts.	(European Commission, 2021; Dremliuga et al., 2020)
International Legal Conflicts	Divergence in privacy and data ownership laws between countries (e.g., GDPR vs. weaker regulations).	International alignment through treaties or global standards (e.g., EU Digital Identity Framework).	(EUR-Lex, 2016; Madiega et al., 2022)
Accountability	Lack of clarity on who is responsible for data breaches or violations (e.g., platform or user?).	Clearly define roles in new laws (e.g., platform responsibility for user identity verification).	—

Table 2. Analytical Table of Legal Conflicts in Digital Identity Management in the Metaverse

Analysis Axis	Key Conflicts	Legal Consequences	Proposed Solutions	Implementation Challenges
Rule of Law	• Conflict between national laws and the cross-border nature of the metaverse • Lack of clarity in legal jurisdiction	• Difficulty determining applicable law in disputes • Creation of legal gaps	• Develop international treaties specific to the metaverse • Establish transnational regulatory bodies	• National resistance to surrendering sovereignty • Lengthy international processes
Privacy	• Inherent conflict between blockchain immutability and the GDPR's right to be forgotten • Extensive collection of biometric data	• Potential violation of data protection principles • Increased risk of mass surveillance	• Use of advanced encryption technologies (e.g., Zero-Knowledge Proofs) • Develop data governance frameworks	• High implementation costs • Need for user education
Digital Ownership	• Legal uncertainty regarding virtual assets (e.g., NFTs) • Conflict over IP definitions for avatars	• Increase in legal disputes • Reduced investment security	• Register ownership on distributed ledgers • Pass specific laws on digital assets	• Lack of uniform legal recognition across countries • Technical issues in proving ownership
Civil Liability	• Lack of clarity on liability for data breaches • Ambiguity regarding avatar-related misconduct	• Difficulty compensating damages • Erosion of user trust	• Define layers of responsibility in smart contracts • Create digital insurance mechanisms	• Difficulty in tracing offenders • Immaturity of compensation systems

In the era of the metaverse, digital identity management faces multifaceted challenges in the realms of privacy, intellectual property, and data security. Although existing regulations such as the GDPR and the AI Act provide foundational frameworks, they are not fully compatible with the decentralized nature of the metaverse. Blockchain technology, as an innovative solution, enables the creation of self-sovereign identities,

yet it presents legal contradictions with current laws (Gadekallu et al., 2022). For instance, the immutability of data on public blockchains conflicts with the "right to be forgotten" under the GDPR.

Proposed solutions include revising existing laws to align with decentralized technologies, adopting hybrid blockchains, and developing joint frameworks between metaverse platforms (Matsson, 2022). Moreover, international cooperation is essential for establishing global standards, as the metaverse is inherently a borderless space (UNCTAD, 2023). Ultimately, integrating artificial intelligence with blockchain could help strike a balance between security and privacy, but doing so requires regulations that take the ethical dimensions of technology into account (Sullivan, 2018).

From the perspective of a researcher in digital identity management in the metaverse era, significant challenges persist in the areas of privacy, intellectual property, and data security. While regulations like the GDPR and AI Act offer a baseline for data protection, they are not well-suited to the decentralized and dynamic nature of the metaverse. Blockchain, with its capacity for enabling self-sovereign identities, is seen as a promising innovation. However, it also brings legal conflicts—particularly regarding the right to delete data, which contradicts the permanence of records on public blockchains.

To resolve these conflicts, revising current legal frameworks to accommodate decentralized technologies and adopting hybrid blockchains are seen as practical steps. Additionally, the development of collaborative frameworks between metaverse platforms and international cooperation to create global standards are necessary, given the inherently borderless nature of the metaverse. Finally, while combining AI and blockchain may help balance security and privacy, this requires the establishment of laws that address the ethical implications of emerging technologies.

Therefore, to create a secure and sustainable environment in the metaverse, it is essential for various stakeholders—including lawmakers, technology developers, and users—to work together to devise solutions that are both effective and aligned with human rights.

Referemces:

Akafi Ghaziani, M., Milani, S. M., & Akafi Ghaziani, V. (2022). Metaverse and legal challenges in property rights. *Journal of New Technologies Law*, 3(6), 143-153. https://doi.org/10.22133/mtlj.2022.353672.1109

Alam, T. (2019). Blockchain and its Role in the Internet of Things (IoT). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 151-157. https://doi.org/10.32628/CSEIT195137

Barfield, W. (2006). Intellectual property rights in virtual environments: Considering the rights of owners, programmers and virtual avatars. *Akron Law Review*, 93(3), 649-700. https://law.bepress.com/cgi/viewcontent.cgi?article=4342&context=expresso

Barfield, W., & Blitz, M. (2018). *Research Handbook on the Law of Virtual and Augmented Reality*. Edward Elgar Publishing. https://doi.org/10.4337/9781786438591

Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. *Big Data & Society*, 6(2), 1-6. https://doi.org/10.1177/2053951719855091

Bernal Bernabe, J., Canovas, J. L., Hernandez-Ramos, J. L., Torres Moreno, R., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access*, 7, 164908-164940. https://doi.org/10.1109/ACCESS.2019.2950872

Cheong, B. C. (2022). Avatars in the metaverse: Potential legal issues and remedies. *International Cybersecurity Law Review*, 3(2), 467-494. https://doi.org/10.1365/s43439-022-00056-9

Colcelli, V. (2019). Joint controller agreement under GDPR. *EU and Member States - Legal and Economic Issues*, 3, 1030-1047. https://doi.org/10.25234/eclic/9043

Dremliuga, R., Dremliuga, O., & Iakovenko, A. (2020). Virtual reality: General issues of legal regulation. *Journal of Politics and Law*, 13(1), 75-81. https://doi.org/10.5539/jpl.v13n1p75

EUR-Lex. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data. *Official Journal of the European Union*, 1-88.

Gadekallu, T. R., Huynh-The, T., Wang, W., Yenduri, G., Ranaweera, P., Pham, Q. V., ... & Liyanage, M. (2022). Blockchain for the metaverse: A review. *Computer Science*, 1-17. https://doi.org/10.48550/arXiv.2203.09738

Heister, S., & Yuthas, K. (2022). How blockchain and AI enable personal data privacy and support cybersecurity. In *Blockchain Potential in AI*. IntechOpen. https://doi.org/10.5772/intechopen.96999

Iranian Parliament. (2018). Draft Personal Data Protection Bill.

Iranian Parliament. (2020). Data and Information Disclosure Mandate Bill.

Iranian Parliament. (2021). National Data and Information Management.

Kondova, G., & Erbguth, J. (2020). Self-sovereign identity on public blockchains and the GDPR. In *Proceedings of the 35th Annual ACM Symposium on Applied Computing* (pp. 342-345). https://doi.org/10.1145/3341105.3374066

Latifzadeh, M., & Ghoboli Dirafshan, S. M. M. (2023). Introducing digital identity in the metaverse: Identifying legal challenges and seeking solutions. *Private Law Studies*, 53(2), 349-372. (Original in Persian:

Matsson, D. (2022). GDPR, blockchain & personal data - The rights of the individual v. the integrity of blockchain. In *Gothenburg University Publications Electronic Archive (GUPEA)* (pp. 1-64).

Michèle, F. (2019). *Blockchain and the general data protection regulation* (pp. 1-120).

Mirshakkari, A. (2017). *Personality rights and civil liability law in the European Union*. Sahami Publishing.

Mystakidis, S. (2022). Metaverse. *Encyclopedia*, 2(1), 486-497. https://doi.org/10.3390/encyclopedia2010031

Ning, H., Wang, H., Lin, Y., Wang, W., Dhelim, S., Farha, F., Ding, J., & Daneshmand, M. (2021). A survey on metaverse: The state-of-the-art, technologies, applications, and challenges. *Cornell University*, 1-34. https://doi.org/10.48550/arxiv.2111.09673

Shakeri, Z., & Jafarpour, Y. (2022). Feasibility study of applying moral rights of authors under new information and communication technologies. *Journal of New Technologies Law*, 3(6), 15-29. https://doi.org/10.22133/mtlj.2022.360779.1120 (Original in Persian)

Singh, R. (2022). *User privacy protection in the emerging world of metaverse* (pp. 1-7).

Sullivan, C. (2018). Digital identity - From emergent legal concept to new reality. *Computer Law & Security Review*, 34(4), 723-731. https://doi.org/10.1016/j.clsr.2018.05.015