Rethinking Digital Avatars and Personal Information Protection in the Metaverse Era

Authors: Yan Chi, Yan Chi

Date: 2024-03-16T00:00:00+00:00

Abstract

The metaverse represents a novel social formation that has emerged with the advancement of blockchain, big data, artificial intelligence, virtual reality, and other technologies. As technology evolves, regulations for new phenomena inevitably become disconnected from existing norms, necessitating their re-examination. This study focuses on issues concerning digital avatars and personal information protection, proposing that digital avatars should not be considered legal subjects but rather objects of real rights. Through the lens of digital avatars, it identifies risks of personal information infringement in the metaverse era and proposes solutions for personal information protection from both legal and practical application perspectives. The research aims to safeguard the development of the digital economy in the current metaverse market, where regulatory systems are absent.

Full Text

Rethinking Digital Avatars and Personal Information Protection in the Metaverse Era

Abstract

The metaverse represents an entirely new social form born from the development of blockchain, big data, artificial intelligence, virtual reality, and other technologies. As technology advances, regulations for emerging phenomena inevitably become disconnected from existing norms, necessitating their re-examination. This study focuses on the issues of digital avatars and personal information protection, proposing that digital avatars should not be considered legal subjects but rather objects of property rights. Through the lens of digital avatars, it introduces the risks of personal information infringement in the metaverse era and proposes solutions for personal information protection from both legal and

practical application perspectives. The aim is to safeguard the healthy development of the digital economy in the current metaverse market, where regulatory systems remain inadequate.

Keywords: metaverse; blockchain; digital avatar; personal information protection

---

The year 2021 has been dubbed the "first year of the metaverse" [1], with the industry's explosive growth capturing global attention. The metaverse is a product of information technology, essentially an advanced virtual world [2], or alternatively, the digitization of the physical world. Digital avatars serve as the behavioral agents and necessary conditions within this virtual space—all actions and activities in the metaverse depend on them. While technological progress enables new possibilities, it also creates conflicts between regulation and development. Today's metaverse market lacks effective institutional oversight and legal protection, yet the construction of digital avatars requires collecting and utilizing vast amounts of personal information, potentially triggering significant risks of personal information leakage. As the adage goes, "people cannot have freedom without order" [3]. This paper examines the legal issues surrounding digital avatars and personal information protection from a metaverse ecosystem perspective, employing literature review and comparative research methods to propose feasible future development pathways from both legal and practical application angles.

In October 2021, Mark Zuckerberg, founder of the renowned social media platform Facebook, rebranded his company as "Meta," sparking a new wave of metaverse enthusiasm. However, the metaverse concept did not emerge from nowhere. In 1992, Neal Stephenson introduced the concept of the "Metaverse" in his novel *Snow Crash* [4]. According to this vision, the Metaverse is a virtual space created through internet technology that projects the real world, where everyone exists as a virtual avatar. The prefix "Meta" derives from Greek, meaning "foundation" or "origin," while in English it conveys "beyond" or "transcendent." "Verse" refers to "universe." Simply put, the metaverse is a virtual space that both parallels and remains independent from the real world [5]. Marshall McLuhan once proposed that "any medium is an extension of human senses" [6]. If internet-era media represent a composite extension of multiple senses, then the metaverse achieves comprehensive sensory connection within the virtual world [7]. In this three-dimensional space where virtual and physical coexist, human perception, agency, and decision-making capabilities are substantially enhanced.

Blockchain has created an entirely new trust ecosystem. Through the combination of peer-to-peer networks and cryptographic technology, blockchain enables network participants to reach consensus, with each node serving as a witness to history. This inaugurates an era where trust is obtained through technological means rather than government authorization. Blockchain technology constitutes

the core technology for building the metaverse. Characterized by transparent, public, and traceable processes, blockchain opens information to public scrutiny. Consequently, it is most effective in coordinating multi-party participation scenarios. All assets in the metaverse are digitally presented based on blockchain networks, which not only prevents excessive resource concentration but also safeguards the rights of underlying users to own their data.

2. The Legal Meaning of Digital Avatars

A digital avatar refers to the audio-visual composite representing an individual from the real world within the virtual realm. It serves as both the entry point and identity for users to participate in and experience the metaverse, and has been defined as an interactive social representation of users [8]. The concept of digital avatars first emerged in gaming, referring to virtual characters controlled by players. Through system settings, players can render avatars with countless unique appearances and manipulate them to engage in various surreal activities. In the metaverse vision, the behavioral subject is not the human physical body but rather dynamic images rendered by computers based on data transmitted through fiber optics [9]. Digital avatars in the metaverse typically exhibit characteristics of privacy, uniqueness, and interactivity. As augmented reality (AR), virtual reality (VR), and artificial intelligence (AI) technologies develop, the boundary between virtual and real worlds is gradually dissolving, leading us to believe that the currently elusive metaverse will become tangible in the near future. With an increasing number of technology companies deploying commercial applications for digital humans or virtual humans, examining the legal meaning of digital avatars in the metaverse era holds significant practical importance. Legal clarification can perfect the digital avatar ecosystem and enable more scientific and stable development of the digital avatar industry.

2.1 Digital Avatars Are Not Legal Subjects

Artificial intelligence technology is one of the six pillar technologies of the metaverse. In recent years, AI has even demonstrated "creativity" surpassing humans in mental activities, making whether to grant legal personality to AI entities a focal point of academic attention. Scholars have categorized AI into weak AI, strong AI, and super AI based on technical capabilities [11], arguing that strong AI at human level and super AI far exceeding human brain capacity should possess legal personality [12]. Weak AI refers to technology that lacks autonomous consciousness and instead focuses on simulating human intelligence to solve specific problems based on deep learning [13]. Most AI commonly seen today falls into this category; for instance, AlphaGo, which gained fame by defeating professional human Go players, is a weak AI program specialized in Go. Digital avatars inevitably utilize AI technology, but the core of the metaverse lies in users' deep interactive experiences. Digital avatars represent the digital projection of users' information and even emotions, processing complex interaction information through blockchain systems and proprietary algorithms. Although

no clear definition of digital avatars currently exists, it is evident that they are human-dominated entities and should be categorized as weak AI technology.

Regarding the legal personality of weak AI, two opposing viewpoints exist: the subject theory and the object theory. The subject theory argues that given AI' s demonstrated intelligence levels and diverse functions, AI entities should be granted legal personality to become true legal subjects. Scholars such as Solum contend that AI entities should have civil subject status [14], Guo Shaofei proposes granting AI the legal status of "electronic persons" [15], and Chen Jidong suggests the relationship between AI entities and users resembles that between agents and principals. Some argue for granting AI entities fictitious legal personality through "deeming" approaches [16]. The object theory is currently more mainstream in practice. Zhao Wanyi argues that AI entities lack moral capacity and therefore should not have subject status [17], while Hao Tiechuan maintains that AI entities are essentially tools created by and serving humans [18]. In an era of rapid technological development with inadequate legal oversight, the object theory is more reasonable. Léon Duguit proposed that legal subjects should be individuals with free will who can control their own behavior [19], making will capacity and behavioral capacity the fundamental criteria for determining legal personality. Digital avatars are agents that transmit information through algorithms, programs, and software [20], essentially binary data established by civil subjects whose actions reflect the will of the natural persons or groups behind them. Consequently, they should not be granted legal subject status.

2.2 Digital Avatars Are Objects of Property Rights

Digital avatars represent the indirect manifestation of real-world civil subjects' online activities [21], instantly exchanging information in computer networks through digital technologies such as TCP/IP protocols, and cannot exist independently of civil subjects' declarations of intent. Digital avatars can be viewed as virtual characters in current online games. In relevant laws in Japan and South Korea, virtual characters in online games are considered network virtual property and endowed with independent property value [22]. Taiwan, China defines network virtual property as "electromagnetic records," further affirming the property value of virtual characters in games and protecting them as "objects." Not all virtual products can be identified as virtual property. Zhang Mingkai summarizes the characteristics of network virtual property as manageability, transferability, and value [23], providing a restrictive interpretation of its scope. Digital avatars fully satisfy these three requirements and should be regarded as network virtual property.

The Civil Code stipulates that property rights are statutory and that the objects of property rights include only tangible property and a few rights. Ji Hailong notes that data files are generally not considered objects of property rights protection due to their non-exclusivity and susceptibility to tampering, making them difficult for specific subjects to exclusively control [24]. Article 127 of the Civil Code contains declarative provisions on the protection of data

and network virtual property but does not clarify their legal attributes. Scholars both domestically and internationally have offered various interpretations. Wen Shiyang [25] and Lin Xuxia [26] define network virtual property as existing in network environments or cyberspace, simulating real-world objects in digital form, possessing relative independence, and allowing exclusive enjoyment. Gao Limei points out that network virtual property not only has virtuality, dependence, and special exercise methods but also possesses independence, specificity, and controllability [27]. Yang Lixin argues that network virtual property is virtual objects that can establish property rights and are undoubtedly objects of property rights [28]. Wang Lei maintains that network virtual property must be used in conjunction with network service contracts and software licensing contracts, and its special exercise methods determine that it is an object of creditor' s rights [29]. Shi Jie and Wu Shuangquan argue that network virtual property represents players' intellectual achievements and should be considered an object of intellectual property rights [30]. Fairfield proposes that network virtual property should possess three legally relevant characteristics connected to the real world: competitiveness, persistence, and interconnectivity [31]. Westbrook notes that the essence of network virtual property is a string of computer code with characteristics such as exclusivity, uniqueness, scarcity, permanence, and transferability [32].

Although the Civil Code does not explicitly define network virtual property as an object of property rights, considering its distinct characteristics that differentiate it from real property and its legal features of relative independence and exclusive enjoyment, it should be treated as an object of property rights. Based on the above perspectives, digital avatars conform to the definition of network virtual property and should be regarded as objects of property rights.

3. Personal Information Protection in the Metaverse Era

3.1 Personal Information Risks in the Metaverse Era

In the metaverse, users inhabit data-constructed digital avatars, making data the core of property. Users' personal information is recorded continuously and processed across all domains, making personal information protection the focal point of interest conflicts and rule reconstruction in the metaverse era [33]. Digital avatars serve as "passports" for people navigating the metaverse, and their construction requires an enormous foundation of data information, inevitably involving the collection and use of personal identity information, property information, location information, and more, posing significant threats to personal information security. Wang Defu argues that the internal openness of the metaverse impacts personal information usage rules, while its external closure increases the difficulty of external supervision [34].

Although blockchain, as a core metaverse technology, aligns with personal information protection concepts in some respects, it also conflicts with China' s current personal information protection legal framework in multiple ways. These

conflicts include: the tension between blockchain' s immutability and the need for personal information deletion and correction; the clash between blockchain' s transparent information disclosure and personal information confidentiality requirements; and the contradiction between blockchain' s decentralized distributed architecture and the centralized responsibility system for personal information. Although China currently lacks the application environment for fully public blockchains, with private or semi-decentralized consortium chains being more common, the future implications of conflicts between personal information and blockchain cannot be underestimated.

Blockchain transactions are characterized by transparent, public, and traceable processes that open information to public scrutiny. Therefore, laws related to personal information security should clearly define data subjects and their rights in blockchain technology applications, as well as specify the legality and compliance of data [35]. Article 25 of the Personal Information Protection Law stipulates that personal information processors may not disclose processed personal information without individual consent. Article 28 provides special protection for sensitive personal information, allowing its processing only under strict protective measures, for specific purposes, with sufficient necessity, and with individual consent.

Take non-fungible token (NFT) transactions as an example. To better gain the trust of NFT trading communities, users can easily search for on-chain transaction system data and code information through blockchain browsers. In April 2022, the famous singer Jay Chou' s announcement that his NFT digital avatar gift had been stolen sparked widespread concern. While on-chain property has been praised for its encryption and security, it also carries risks of personal information theft. The blockchain completely records NFT transaction processes, allowing other users to quickly query transaction parties' names, transaction processes, smart contract addresses, and other system data and code information through blockchain browsers. Although data on the chain consists of de-identified information such as hash values that cannot directly link to information subjects' identities, it does not meet complete anonymization standards and can still identify specific natural persons with additional information, falling within the definition of personal information under Article 4 of the Personal Information Protection Law. Table B.1 of the Information Security Technology - Personal Information Security Specification shows that personal virtual property information such as virtual currency and virtual transactions belongs to personal sensitive information, meaning NFT transaction information can be further classified as personal sensitive information.

3.2 Solutions for Personal Information Protection

From a legal perspective, personal information protection in the digital era should adopt a two-dimensional view balancing protection and utilization to ensure flexibility in legal application [36]. Chapter 4 of the Personal Information Protection Law specifically stipulates individuals' rights in personal information

processing activities, including the right to know, decide, access, copy, transfer, and request correction, supplementation, and deletion of personal information. Given the particularities of the metaverse and blockchain, fully subjecting them to the Personal Information Protection Law' s requirements would be overly stringent. Targeted regulations should be established based on recognition of these conflicts. The most prominent issue between the metaverse and personal information protection lies in the inherent conflict between blockchain' s data immutability and the need for personal information deletion, correction, and supplementation. The law should establish a "Right to Be Forgotten" for blockchain data. This right refers to information subjects' entitlement to request data controllers delete unreasonable, outdated information published online that would damage their social evaluation or cause adverse effects if retained [37]. Article 17 of the General Data Protection Regulation (GDPR) explicitly stipulates six scenarios where individuals have the right to request information controllers delete relevant personal information. While theoretical disputes exist regarding the relationship between the right to deletion and the right to be forgotten, this paper aligns with the view that "the deletion right stipulated in Article 47 of the Personal Information Protection Law appears similar to the right to be forgotten but remains substantively different and should not be directly equated" [38]. The right to be forgotten should be incorporated into the Personal Information Protection Law framework to balance different interests. Technically, personal information can be "deleted" by sending it to a black hole address. Article 16 of the GDPR also stipulates the Right to Rectification, where data subjects can request information controllers correct inaccurate personal data or complete their information through supplementary statements. Article 46 of the Personal Information Protection Law similarly grants individuals the right to request correction and supplementation of inaccurate or incomplete personal information. No technical barriers exist for information correction on blockchain; new personal information blocks can be added to cover old blocks [39].

From a practical application perspective, the UK's Financial Conduct Authority proposed the innovative concept of regulatory sandboxes, which involve designating specific sandbox areas for small-scale pilot programs and comprehensive supervision of enterprises. The rise of regulatory sandbox applications is closely related to blockchain governance [40], and China' s first regulatory sandbox practice, led by the Guiyang government, also concerned blockchain finance [41]. This approach optimizes regulatory mechanisms through government guidance, social participation, and market-oriented operations. Going forward, sandbox programs can be flexibly applied through inter-departmental government coordination to conduct pilots in economically developed cities such as Shanghai and Shenzhen, reducing personal information infringement risks while encouraging healthy metaverse industry development. At present, virtual currency and public blockchains lack application environments in China. In January 2022, the Blockchain-based Service Network (BSN) Development Alliance, initiated by the State Information Center, China Mobile, China UnionPay, and others, launched the localized NFT practice "Distributed Digital Certificate" (DDC).

BSN is currently the world' s largest blockchain service network infrastructure, with over a hundred data centers deployed globally. By openly deploying DDC on BSN' s consortium chains, the BSN-DDC basic network can be generated. The DDC network consists of more than ten open consortium chains, allowing only platform access while supporting cross-chain transfers and external nodes controlled by third parties. Through advanced technology and a unique multi-party supervision and co-management model, it achieves personal information protection and represents a successful localized exploration aligned with future metaverse development directions.

4. Conclusion

According to Bloomberg News forecasts, the global metaverse market will reach $800 billion by 2024. China has already formed a substantial metaverse market, yet its governance system remains inadequate. Digital identity carried by personal information constitutes the only bridge connecting the physical and virtual worlds [42]. Future efforts should further strengthen research on digital avatars and personal information protection from both technical and institutional perspectives, taking into account market development conditions and China' s national circumstances. Through prudent assessment of potential issues and establishment of scientific and reasonable standards, we should continuously explore a metaverse ecosystem aligned with social development processes to promote healthy and stable development of the digital economy.

References [1] Guo Quanzhong. The Origin, Current Situation, and Future of the Metaverse[J]. Journalism Lover, 2022(1):26-31. [2] Fang Lingzhi, Shen Huangnan. Technological and Civilizational Changes—A Conceptual Study of the Metaverse[J]. Industrial Economic Review, 2022(1):5-19. [3] Samuel P. Huntington. Political Order in Changing Societies[M]. Shanghai: Shanghai People' s Publishing House, 2008. [4] Neal Stephenson. Snow Crash[M]. Sichuan: Sichuan Science and Technology Publishing House, 2018. [5] Zhao Guodong, Yi Huanhuan, Xu Yuanzhong. Metaverse[M]. Beijing: China Translation Publishing House, 2021. [6] Marshall McLuhan. Understanding Media: The Extensions of Man[M]. Beijing: The Commercial Press, 2000. [7] Yu Guoming. The Evolutionary Logic of Future Media: Iteration, Recombination, and Dimensional Ascension of "Human Connection" —From the "Era of Scenarios" to the "Metaverse" and then to the "World of Mind" [J]. Journalism and Communication, 2021(10):54-60. [8] Vincent Miller. Key Elements of Digital Culture[M]. Beijing: Tsinghua University Press, 2017. [9] Sun Yujie. Avatars: Digital Avatars in the Metaverse[J]. Art Market, 2022(5):29-33. [10] Yang Yanchao. Challenges of Artificial Intelligence to Intellectual Property Law[J]. Governance Studies, 2018(5):120-128. [11] Piero Scaruffi. The Nature of Intelligence: 64 Questions on AI and Robotics[M]. Beijing: China Industry and Information Technology Publishing Group, Posts & Telecom Press, 2018. [12] Peng Xincheng, Chen Jidong. On the Consideration Elements of Legal Personality of Artificial Intelligence Entities[J]. Contemporary Law Review, 2019(2):52-62. [13] Mo Hongwei.

Ethical Issues in Strong and Weak Artificial Intelligence[J]. Science and Society, 2018(1):14-24. [14] Solum, L. B. Legal Personhood for Artificial Intelligence[J]. North Carolina Law Review, 1992(70):1231-1287. [15] Guo Shaofei. On the Legal Subject Status of "Electronic Persons" [J]. Oriental Law, 2018(3):38-49. [16] Jin Donghan. The Reconstruction of Order—Artificial Intelligence and Human Society[M]. Shanghai: Shanghai University Press, 2017. [17] Zhao Wanyi. Analysis of the Legal Subject Status of Robots—On the Basic Requirements for Regulating Robots[J]. Journal of Guizhou Minzu University (Philosophy and Social Sciences), 2018(3):147-167. [18] Hao Tiechuan. Do Not Fantasize About or Overestimate the Impact of Artificial Intelligence on the Rule of Law[N]. Legal Daily, 2018-1-3(10). [19] Léon Duguit. Constitutional Theory[M]. Beijing: The Commercial Press, 1959. [20] Susanne Beck. The Problem of Ascribing Legal Responsibility in the Case of Robotics[J]. AI & Society, 2016(31):473-481. [21] Lin Xuxia. On the Legal Status of "Virtual Subjects" [J]. Journal of Fujian Normal University (Philosophy and Social Sciences Edition), 2007(3):73-80. [22] Xiao Zhike. Legal Attributes and Criminal Law Protection of Virtual Property[J]. Journal of Shanghai University (Social Sciences Edition), 2021(6):108-118. [23] Zhang Mingkai. The Nature of Illegal Acquisition of Virtual Property[J]. Law Science, 2015(3):12-25. [24] Ji Hailong. The Private Law Positioning and Protection of Data[J]. Chinese Journal of Law, 2018(6):72-91. [25] Wen Shiyang. Legislative Considerations of "Right Objects" in the General Principles of Civil Law —Focusing on Special "Objects" [J]. Law Science, 2016(4):14-22. [26] Lin Xuxia. On the Nature of Virtual Property Rights[J]. China Legal Science, 2009(1):88-98. [27] Gao Limei. The Interpretive Path for Network Virtual Property Protection[J]. Tsinghua University Law Journal, 2021(3):179-193. [28] Yang Lixin. The Meaning and Important Value of Network Virtual Property Provisions in the General Principles of Civil Law[J]. Oriental Law, 2017(3):64-72. [29] Wang Lei. Insisting on the Creditor' s Rights Theory of Network Virtual Property Rights—On the Systematic Position of Network Virtual Property in China's Civil Code[J]. Jianghan Tribune, 2017(1):121-129. [30] Shi Jie, Wu Shuangquan. On the Legal Attributes of Network Virtual Property[J]. Political Science and Law Review, 2005(4):33-40. [31] Joshua A.T. Fairfield. Virtual Property[J]. Boston University Law Review, 2005(85):1047-1102. [32] Westbrook T. J. Owned: Finding a Place for Virtual World Property Rights[J]. Michigan State Law Review, 2006:…[33] Chen Jidong. Beyond Legal Imagination of the Metaverse: Digital Identity, NFT, and Multi-dimensional Regulation[J]. Rule of Law Research, 2022(3):43-54. [34] Wang Defu. New Challenges and Legal Responses to Personal Information Protection in the Metaverse[J]. China Market Regulation Research, 2021(11):60-62. [35] Ma Zhiguo, Liu Hui. Research on the Systematization of China' s Blockchain Legal Governance Rules[J]. Journal of Xi' an Jiaotong University (Social Sciences Edition), 2020(3):72-80. [36] Zhang Xinbao. From Privacy to Personal Information: Theoretical and Institutional Arrangements for Rebalancing Interests[J]. China Legal Science, 2015(3):38-59. [37] Yang Lixin, Han Xu. The Localization and Legal Application of the Right to Be Forgotten in China[J]. Law Application, 2015(2):24-34. [38] Long Weiqui. Interpretation of the Personal Information Protection Law of the People' s Re-

public of China[M]. Beijing: China Legal Publishing House, 2021. [39] Wang Lusheng. The Inherent Conflict and Reconciliation Between Blockchain and Personal Information Protection Legal Norms[J]. Legal Forum, 2022(3):81-95. [40] Su Yu. The Model, Architecture, and Mechanism of Digital Token Regulation[J]. Oriental Law, 2021(3):77-94. [41] Li Jing. Research on Digital Currency Regulation from the Perspective of "Regulatory Sandbox" [J]. E-Government, 2020(11):74-85. [42] Lu Qing. Identity Construction and Its Legal Protection in the Digital Age: Reflections Centered on Personal Information Protection[J]. Chinese Journal of Law, 2021(5):3-23.

Note: Figure translations are in progress. See original paper for figures.