Security and Safety, Vol. 2, 2023011 (2023)

Security and Safety in the "Metaverse"

Review

Open Access

Information Network

Digital identity, privacy security, and their legal safeguards in the Metaverse

Hong Wu* and Wenxiang Zhang*

NingboTech University, Ningbo 315100, China

Received: 30 October 2022 / Revised: 23 March 2023 / Accepted: 30 April 2023 / Published online: 30 June 2023

Abstract The Metaverse is the digitization of the real world, supported by big data, AI, 5G, cloud computing, blockchain, encryption algorithm, perception technology, digital twin, virtual engine, and other technologies that interact with human behavior and thoughts in avatars through digital identity. Cracking the trust problem brought by the avatar depends on the privacy security and authentication technology for individuals using digital identities to enter the Metaverse. To accomplish personal domination of the avatar, metaverse users need privacy data feeding and emotion projection. They must be equipped with proprietary algorithms to process and analyze the complex data generated in adaptive interactions, which challenges the privacy security of user data in the Metaverse. Distinguishing the significance of different identifiers in personal identity generation while imposing different behavioral regulatory requirements on data processing levels may better balance the relationship between personal privacy security and digital identity protection and data utilization in the Metaverse. In response to digital identity issues, there is an objective need to establish a unified digital identity authentication system to gain the general trust of society. Further, the remedies for a right to personality can be applied to the scenario of unlawful infringement of digital identity and privacy security.

Keywords Metaverse, Avatar, Digital identity, Privacy security, Privacy data, Identity authentication

Citation Wu H and Zhang W. Digital identity, privacy security, and their legal safeguards in the Metaverse. Security and Safety 2023; **2**: 2023011. https://doi.org/10.1051/sands/2023011

1 Introduction

Metaverse is a 3D digital virtual space in which natural persons living in the real physical world can interact with other avatars instantly through computer operating systems with the support of big data, AI, 5G, cloud computing, blockchain, encryption algorithm, perception technology, digital twins, virtual engine and other technologies in the form of digital identity [1]. A digital identity is a digital representation of an entity that includes personally identifiable data and supporting data. Digital identity can simplify complex human behavior into systematic data for identification in cyberspace, and the basis for individuals to enter and be identified is the authorization of digital identity [2]. An avatar is a digital version of a natural person. In the Metaverse, the resolution of the trust problem brought by the avatar depends on the privacy security and authentication technology for individuals to enter the Metaverse using a digital identity.

To accomplish personal domination of avatars by users of the Metaverse requires data feeding and even emotional ro ection and needs to be equipped with proprietary algorithms to process and analyze

the complex data generated in adaptive interactions. Moreover, the avatar is pre-trained to learn through feedback, just like any other AI system [3]. The Metaverse promises a 3D world where virtual and reality are deeply intertwined, mapped, and switched at any time. Based on the traditional two-dimensional data, the user-oriented metaverse scene also requires a full-body avatar, full-body real-time motion capture, real-time reconstruction of the surrounding spatial environment, and other three-dimensional data collection and processing. The mobile Internet allows users to hand over their lifestyle data such as hairstyle, clothing, taste, and other biometric data such as fingerprints, voice prints, and facial contours. In that case, however, the Metaverse pushes the data boundary further inside the user's body. It induces users to hand over deep bio-privacy data such as eye movements, electromyographic signals, brain waves, and genetic composition. It also tries to put the human-computer interaction mechanism in one step and build on anatomical foundations. The data authority or data discourse sought by the metaverse platform involves more dynamic data and personal dynamic digital identity. The reality is that multiple dynamic digital identities overlap and coexist. Their legal loopholes and technical flaws allow powerful platforms to exceed their authority and overreach to collect and commercially exploit personal data illegally. These are challenges to the privacy security of user data in the Metaverse.

Although the systems of the Metaverse with blockchain as the underlying technology may become increasingly autonomous and distinct from traditional law, they are still ultimately controlled by real persons. Even if blockchain achieves widespread disintermediation, the rule of law will still be needed to protect the orderly operation of the Metaverse. The healthy development of the Metaverse in the context of the digital economy urgently needs the legal protection of digital identity and privacy security, especially the legal framework of personal information protection and a unified digital identity authentication system.

This article asserts that the key to privacy security protection does not lie in statically determining whether a particular data belongs or does not belong to personal information but instead focuses on more targeted behavioral norms on how personal identities (including digital identities) are generated in different contexts. Distinguishing the significance of different identifiers in personal identity generation while imposing different behavioral regulatory requirements on information processing levels may better balance the relationship between personal privacy security and digital identity protection and data utilization in the Metaverse. In response to digital identity issues, this article argues that as the scope of socio-economic activities in the Metaverse expands, there is an objective need to establish a unified qualification system that stores identity information in a unified encryption system of the government. It provides personal identity data that match the real physical world. It may effectively solve the problem of false identity information, whereby re-gaining the general trust of society. Further, this article asserts that the remedies for infringement of personality rights can be applied to the scenario of unlawful infringement of digital identity and privacy security (as shown in Fig. 1).

In order to critically analyze digital identity and privacy security in the Metaverse and their legal remedies, Chapter 2 elaborates on the concept, structures, and features of the Metaverse, thus laying the foundation for the critical analysis of the avatar, digital identity, and privacy security in Chapters 3 and 4. Chapter 3 analyzes digital identity and its dilemmas in the Metaverse. In particular, it explores the relationship among the avatar, digital identity, and privacy security, identity trust crisis, identity authentication dilemma, and new problems that arise when the digital identity of personal data changes from a static status to a diverse dynamic status. Chapter 4 analyzes privacy security and its challenges in the Metaverse. Specifically, it explores the production and control of user data in the Metaverse, the contradiction between transparency and privacy protection in blockchain, trust fraud, data misuse, leakage of personal data, and sexual harassment in the Metaverse. Chapter 5 builds on the previous chapters to explore the legal safeguards for digital identity and privacy security in the Metaverse. The chapter analyzes the legal framework of personal information protection in protecting the privacy security of the Metaverse; it reviews the definition and classification of personal data in the Metaverse and explores the Metaverse's consent rules. It constructs a unified digital identity authentication system for protecting digital identity and privacy security in the Metaverse. It also analyzes the civil liability for unlawful infringement of digital identity and privacy security in the Metaverse. Chapter 6 concludes the article.

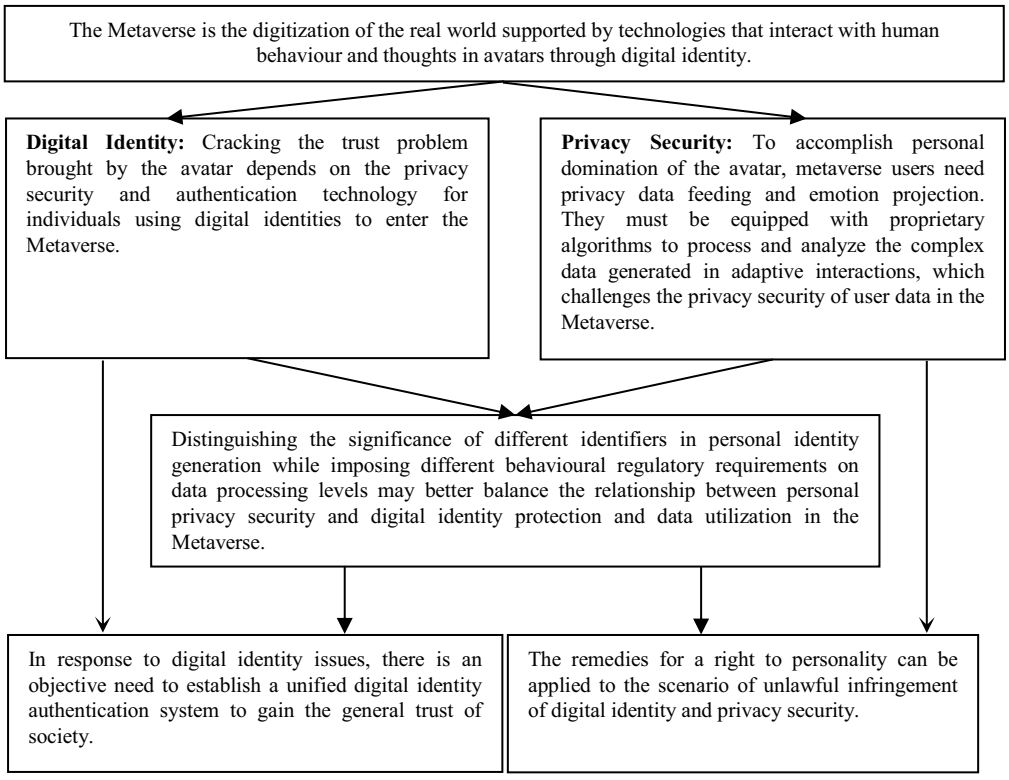

Figure 1. Thoughts of the Article.

2 The Rise of the Metaverse: Concepts, Features, and Structures

The Metaverse is generally considered a 3D digital virtual space in which natural persons living in the real physical world interact instantly with other avatars through a computer operating system in the form of a digital identity. The concept of Metaverse was first proposed by novelist Neal Stephenson in 1992 and later made into the movie Snow Crash [4]. From the technical aspect, the Metaverse is a collection of digital technologies such as big data, AI, 5G, cloud computing, blockchain, encryption algorithm, perception technology, digital twins, and virtual engine. These digital technologies are being fully integrated into all fields and processes of the human economy, politics, culture, and society with new concepts, business models, bringing extensive and profound impacts to human production and life. Technologies, such as "wearable sensing systems" and "avatar personalization engines", allow people to move between the real world and the digital world with their sense of touch. Digital Twins technology allows the natural person to have his biometric data and a realistic digital image in the Metaverse. People in the real world can perform different actions simultaneously using their digital identities and multiple personalities on the Metaverse to achieve a non-linear narrative.

Jon Radoff, the founder of Beamable, proposed seven layers of the metaverse structure. It includes experience, discovery, creator economy, spatial computing, decentralization, human-computer interaction, and infrastructure [5]. From the perspective of geospatial research, Chaowei Xiao et al. argues that the Metaverse has a multi-layered nested structure of people and objects in virtual space and real space and has five layers: physical environment layer, physical facilities layer, virtual network layer, virtual role layer, and physical role layer [6]. Professor Wei Cai believes that the Metaverse can provide four "social products" to the real world, including accessibility, diversity, equality, and humanity, and he proposes a three-level architecture of the Metaverse system, including infrastructure, interaction, and ecosystem [7]. The development of the Metaverse lies in its "social" attributes. Professor Yu Guoming argues that the Metaverse is a new economic, social, and civilizational system composed of various online and offline platforms [8]. According to political scientist Yu Jingdong, both "civilization" and "ecosystem" in the Metaverse mean that virtual game socialization is no longer limited to entertainment and recreation but relies on a new form of organization and develops toward identity, philosophy, and community [9]. In the

Metaverse, blockchain technology and open source code provide the technical conditions for constructing the decentralized governance of the Metaverse. A Decentralized Autonomous Organization (DAO), it operates autonomously without centralized control or third-party intervention. Specifically, assets flow freely; members contribute freely; the community votes; and the paths and nodes in the system can complete information processing and solve problems. This is called "code as law" [10]. In a Metaverse society, the avatar must comply with the metaverse autonomy guidelines. The Roblox community guidelines state that all participants need to comply with the four aspects of its guidelines including safety, civility & respect, fairness & transparency, and security & privacy. Among them, the safety part of the code covers the protection of children, threats of violence, bullying and harassment, suicide and self-harm, sexual content, terrorist and extremist content, illegal and regulated activities, and real-world physically dangerous activities. The civility and respect section includes rules against discriminatory slander and hates speech, dating and romantic content, extortion, political content, real-world tragic events, harmful offline speech and behavior, disruptive voices, and kindness to Roblox employees and affiliates. The rules in the fairness and transparency section focus on prohibiting deception and regulating spam, cheating and exploitation, misleading parodies and misrepresentations, violations of intellectual property rights, contests and sweepstakes, directing users to leave the platform, and advertising. The rules in the security and privacy section prohibit unauthorized access, sharing of personal information, misuse of Roblox systems, and improper use of Roblox for profit.

3 Digital identity and its dilemma in the Metaverse

The development of metaverse technology extends the social scope of people, which will lead to the transfer of power to social individuals, and the subject status of individuals will be highlighted in the Metaverse. With the support of the Internet of Things, cloud computing, big data, 5G, AI, blockchain, and other technologies, Metaverse will bring people's behavior and thoughts into another virtual space through digital identity. In order to enter this virtual space, individuals virtualize their physical bodies. As an intermediary between the avatar and real individuals, digital identity is inevitably a topic that cannot be detoured. However, the basis for establishing this vision is the Metaverse's benign and orderly ecological environment. The digital identity system may become an essential guarantee for the development of this environment. However, the power of granting individual digital identities and the identification and authentication of digital identities are associated with many issues. Questions such as who has the authority to grant individual digital identities, the extent to which digital identities should include personal information, and the degree of acceptance of digital identity mechanisms by real individuals need to be further studied.

3.1 Avatars and digital identities

The Metaverse is a purely digital ecosystem. Users can create avatars to live and interact in the Metaverse as digital identities. An "avatar" is a role played by a real-world individual in a virtual world [11]. Dynamic interaction between the avatar and the player can be formed through the technical means of deep learning. Instead of textual self-descriptions, individuals can acquire identities by forming their visual images, skills and attitudes, and social interactions in a given environment. Thus, the avatar is also defined as a user-interactive social representation [12]. Some scholars believe that there are three kinds of identity relationships between the individual and the avatar: first, the identification with the avatar, when a holistic expression is formed between the two; second, the independence between the individual and the avatar, when the latter is regarded as a mere game tool; and third, the avatar as a compensatory object when the avatar is regarded as an ideal projection of certain qualities of the individual [13]. The insight of this classification is that whether the avatar should be included in the individual's dynamic identity needs to be judged in specific scenarios. To accomplish personal domination of the avatar requires data feeding, even emotional projections, and needs to be equipped with proprietary algorithms to process and analyze the complex privacy data generated in adaptive interactions. Moreover, the avatar is trained to learn through feedback like any other AI system.

Behind the avatar is the starting point of the Metaverse, that is, digital identity. Individuals need to use digital identity to enter the online society to ensure they have a unique identity, exercise their

rights, and fulfill their obligations. In private law, identity seems to have ended with Maine's assertion of "from identity to contract". According to Article 3.1.2 of ISO/IEC 24760-1 2019, identity is a collection of attributes associated with an entity. A digital identity is a digital representation of an entity that includes personal data and other supporting data. Its applications mainly include individual access using identity authorization and authentication. Authentication is identity verification and does not involve identity conferring or identity content per se. Authentication has its roots in trust mechanisms in the virtual space. Unlike the physical world, digital identity relies on cryptographic trust rather than humanistic trust [14]. When we interact in the real world, we communicate, our voices are heard, and trust is generated. Luhmann argues familiarity generates trust, thereby reducing the world's complexity [15]. In the Metaverse, we have no way of knowing whether the other person is real or not. As typified by Peter Steiner's famous cartoon in the New Yorker, "on the Internet, no one knows you are a dog". Identity verification relies on the collection of personal data. Any transaction, or payment, in the Metaverse requires authentication. However, the Internet architecture does not have an independent identity layer; identity issues in the application layer of specific applications are managed separately; and, for a long time, digital identity has been characterized as an accounting system. This subordinate status of the application system objectively determines the user's activities in different systems, that is, to repeat the registration of many accounts. However, account dispersion in the inconvenience also may lead to the risk of collision and privacy leakage problems, and a bigger problem is not to avoid identity fraud. The self-representation of the avatar in the virtual environment created by the Metaverse affects the natural persons' behavior in the real world, called the "Protoss effect". In the Metaverse, the arbitrary creation of digital identities would be contrary to good customs. Many games require players to perform actions they would not normally engage in their daily lives, asking them to steal, murder, and engage in reckless acts of violence. The Metaverse needs to uphold its values, which include foundational values such as justice and rationality, and other values such as encouraging innovation and exploration and advocating diversified development. The vulnerability of digital systems and the risk of identity theft are ever-present in the Metaverse. The abstract, specialized, and difficult-to-perceive nature of digital identity makes individuals naturally distrust it. Individuals do not understand and cannot fully trust the system, much less the program set by the code developer. In the Metaverse, cracking the trust problem posed by the avatar depends on the security and authentication technology for individuals to enter the Metaverse using a digital identity.

3.2 Authentication of Digital Identity and its Dilemma in the Metaverse

Cracking the trust puzzle caused by the avatar in the Metaverse depends on which digital identity is used [16]. Authentication becomes the user's passport to access the Metaverse. With the construction of digital identity and NFT as a circulation tool, users can maintain a high degree of synchronization and interoperability between the Metaverse and the real world. The fundamental aspect of strengthening the authentication and management of digital identity is ensuring the existence of a real subject behind the avatar to reduce the fraud and identity problems associated with online interactions. Digital signatures of avatars in the Metaverse may bring new changes to the existing digital signature law in the physical world. However, it is still doubtful whether digital signatures are sufficient for metaverse identity verification. How does the centralized authentication system at this stage fit the trend of decentralized development of blockchain? How can the decentralized authentication system established by enterprises spontaneously be mutually recognized and interoperable? Decentralized Identity (DID) and other Internet-trusted identity responsibility models improve responsibility regulation from three technical levels, that is, verification, application, and information. Some scholars suggest that although there are more and more other registration systems, the Metaverse can theoretically define a "root avatar" as a complete identity set that consolidates all digital identities [17]. However, a unique system identifier in the Metaverse would require additional protocols, a task of unimaginable complexity. This involves issues of sovereignty and jurisdiction and is one of the essential starting points for government involvement in the Metaverse. However, the Metaverse is a digital manifestation of the real world with multiple identities. It is questionable whether a system can be used to inscribe and handle multiple digital identities. After the decentralization of identity, digital identity takes on positive contents such as identity service provision, property transfer, and privacy data protection that are not found in traditional identity authentication, which need to be studied more deeply.

Blockchain technology on the Metaverse is only used for integrity checks. The behavior of avatars in the Metaverse is essentially the behavior of natural persons in the real world. However, the blockchain technology used in the current Metaverse is still "peer-to-peer". There is no verification by a neutral and independent organization. All kinds of subjects submit their identity proofs, which are stored in the user terminal after verification by the system, instead of a centralized origin. Although the requirements of personal information protection are met, the authenticity of individual identity verification is neglected. Moreover, the current blockchain is only used for integrity verification, which only plays a role in verifying the user's access at a later stage, and there is no prior recognized and trusted authoritative authenticity comparison.

The multiple identities of subjects in the Metaverse are mixed. The open-source, decentralized identity framework of blockchain provides decentralizable identities for various subjects in different metaverses. Ideally, this may require constructing a unified, trusted identity authentication platform to meet the identity authentication needs of metaverse platforms across geographies and borders. This proposition may require the establishment of a digital identity authentication confirmed by the governmental security authentication system. However, in reality, the authentication system established spontaneously by private chains, or alliance chains alone, is often limited only to industry data. The data authentication formats and security levels are different, so it is impossible to achieve mutual recognition and interoperability; it is also impossible to obtain the original information about the natural person's identity. Simply speaking, establishing a unified digital identity authentication system seems contrary to the general trend, and centralization and decentralization itself are also contradictory. Where is the boundary of these two points? How can they co-exist? These are issues that will be addressed in another technology-focused article.

3.3 The close connection between digital identity and privacy security in the Metaverse

Some scholars believe that the Metaverse should be guaranteed by a "decentralized" affirmative sharing mechanism and shared governance mechanism so that the relationship between the actual individual and the avatar becomes the internal driving force for the continuous expansion of the Metaverse [18]. However, when all the activities of individuals and the avatars under their control can be converted into machine-readable data, individuals' private data (avatars) will become a critical competing resource for service providers of the Metaverse. In the Metaverse era, the digital identity formed by personal data has changed from a static digital identity to a collection of various dynamic digital identities [19]. Privacy data about the online action trajectory, activity tendency, and shopping intention in the Metaverse, carry the identification attribute of individuals. It is one of the cornerstones of the Metaverse. Different dynamic data of individuals often form different dynamic digital identities, which are different identities that individuals intend to display on different occasions and situations. The data authority or discourse sought by the Metaverse platform involves more dynamic data and the dynamic digital identity of individuals. The reality of multiple dynamic digital identities overlapping and coexisting creates legal loopholes and technical flaws that allow powerful platforms to collect and commercially exploit personal data beyond their authority and scope. Articles 5, 6, and 7 of the Personal Information Protection Law provide for this. The Office of Network Security and Information Technology Commission will also respond with regular exposures and deadlines for rectification. In conclusion, the above situations should be included in the rule of law path of personal information protection to break the dominant position of Metaverse platforms on personal data, especially on diverse and dynamic data, and to strengthen privacy security.

4 Privacy security in the Metaverse and its challenges

The Metaverse induces users to not only hand over their lifestyle data such as hairstyle, clothing, taste, and other biometric data such as fingerprints, voice prints, and facial contours, but also hand over vital privacy data such as eye movements, electromyographic signals, brain waves, and genetic composition. In numerous Metaverse content consumption scenarios, extended reality technology and brain-computer interface technology will collect users' brain waves and other neuronal activity data to enhance user experience. All of the above pose challenges to the privacy security of privacy data in the Metaverse. The privacy security challenges of the Metaverse include the tension between the transparency of the

blockchain and privacy protection, trust fraud, data breaches, abuse, and sexual harassment. For example, one survey in 2021 showed that 87% of Americans who see Facebook's move into the Metaverse are worried about the impact in terms of privacy. For example, they are concerned about whether hackers will apply for avatars to steal data during interactions or commit deceptive acts. More than 40% of people are concerned about whether their identity is well protected and whether it will be known to the outside world.

4.1 Production and Control of privacy data in the Metaverse

The Metaverse's production and control mechanism of privacy data includes three key elements: account, data, and reputation evaluation. The account is the entrance for users to enter the Metaverse from the real world and the carrier for the ephemeral accumulation of privacy data. In the Metaverse, the identity control mechanism with account number as the core has shifted from a single centralized platform control to the coexistence of centralized and decentralized control mechanisms. The arrival of the Metaverse has given birth to several meta-architecture companies while pushing traditional technology giants to transform into meta-architecture companies like meta-rooms in the Metaverse. In the Metaverse, the centralized identity control mechanism continues, but users can gain greater access to content production and revenue distribution. As the interoperability technology in the Metaverse further matures, users can freely transfer data and its value between different metaverses. Meanwhile, the introduction of blockchain technology brings a new decentralized identity (DID) control mechanism to the Metaverse.

The data mainly contains four levels: one is the user's authentication data; the second is the content data produced by the user in the foreground of the Metaverse; the third is the user's background behavior data automatically recorded by the Metaverse; the fourth is the derivative data generated after deep mining based on the foreground content data and background behavior data, for example, the user classification and tagging data generated by the Metaverse based on various algorithms. Metaverse user data has multiple dimensions. Compared with the traditional Internet, the dimensions of user data in the Metaverse have changed in two aspects. One is the expansion of the temporal and spatial dimensions of user data. On the one hand, accumulating user data over time constitutes an essential aspect of reputation evaluation and subsequent behavior prediction.

On the other hand, through the introduction of timestamps, the time of privacy data generation is verified, and the data is timestamped, in which the time series of data is emphasized. In this process, the time series of the data is emphasized and becomes one of the criteria for determining the security of the data. The spatiality of privacy data in the Metaverse is enhanced, and the 3D production and storage of privacy data have become increasingly mainstream. Both user identity data and user content data produced for the foreground will be three-dimensionalized with the help of digital twins and virtual simulation technologies. This has raised new privacy security issues while enhancing the immersion of metaverse users. Secondly, the human-machine integration of privacy data is enhanced. Metaverse user data cannot be produced without the support of metaverse front-end devices such as extended reality (XR). With motion tracking and perceptual interaction technologies, the front-end devices capture and retain the user's biometric data, such as voice, movement, eye movement, electromyography, and environmental data. The immersive interaction with the user's identity image and foreground scenes in the Metaverse is generated [20].

Finally, centralized and decentralized reputation evaluation mechanisms coexist. Under the centralized reputation evaluation mechanism, user behavior in the Metaverse will still be regulated. Accordingly, the control of privacy data will also be constrained by the Metaverse. At the same time, a new decentralized reputation evaluation mechanism is being bred and formed in the Metaverse by relying on blockchain technology. Decentralization means that traditional Internet technology giants no longer strongly dominate the process of user personal data collection, storage, transmission and analysis, and decentralized autonomous organizations (DAOs) or specialized privacy data service companies will take over their roles. The difference between the two is that users no longer only nominally own their data but acquire ownership and disposal rights of their data through the corresponding technical implementation and governance mechanisms. The balance of personal data assets of users is further tilted from the Metaverse to the individual. Specifically, under the decentralized reputation evaluation mechanism, the trend of users' self-quantification will be further deepened, and their biometric data, transaction records, and behavioral

data accumulated on the blockchain will be thoroughly mined to generate user reputation credentials. The user reputation evaluation system in the Metaverse is similar to Lifelogging, which not only records what a user has done in the Metaverse but also includes a person's achievements, contributions, interests and activities, and other life records.

4.2 The conflict between blockchain transparency and privacy security

Regarding data form, 3D privacy data generated by metaverse front-end devices based on AR and MR is a new information layer superimposed on the actual space, which is more likely to trigger privacy risks. The sensitive data of users and bystanders in the natural environment, which are not related to interaction, also risk being improperly collected and exposed. In terms of data storage, if data leakage or improper application access occurs while using 3D data, it will bring about severe spatial privacy damage. The multi-user interaction scenario based on AR devices may also lead to problems such as uncontrolled access to user privacy data and infringement of ownership of virtual objects and personal physical space.

Privacy data affects the development of user personality and mind structure. Meta-architecture companies in the Metaverse use digital traces to interfere with users' intellectual activities and even manipulate their minds. In the Metaverse, meta-architectural companies have digital traces of massive amounts of users' intellectual activities. Maintaining the privacy of human intellectual activities and ensuring that the private sphere is free from surveillance and interference are essential prerequisites for individuals in modern societies to develop independent and autonomous personalities and maintain their creative energy. Researchers have conducted a large-scale experiment on Facebook to show that users' emotional states can be artificially manipulated without their knowledge. This emotional infection does not require direct interaction with people or even any non-verbal cues. Simply it controls the emotional expressions of friends' posts that users can access on Facebook is enough to infect them with specific emotions [21]. Socialization remains an essential and fundamental need in the Metaverse. The collection of privacy data by technology companies in the Metaverse is more significant in volume and depth than in the traditional Internet era.

4.3 Metaverse trust scams, data misuse, leakage of personal data

Metaverse hardware and devices can collect and analyze bodily information such as facial expressions, eye movements, hand posture, body temperature, and heartbeat to know the user's personality and interests for precision marketing. There are NFT Scams and catfishing in the Metaverse. For example, in the case of an online trust scam, some users registered their accounts to apply for avatars and then registered some famous brands for scamming. The brands and companies then issued statements saying they should not fall for the scam and were not authorized to commit it by applying for an avatar [22].

In the Metaverse, the intelligent terminal platform, cloud service platform, and application platform control the process of collecting, storing, sharing, and opening personal data. Users first log into the Metaverse platform to submit and produce privacy data. The platform opens interfaces to third-party enterprises, such as third-party application providers of games and music. Advertisers of third-party enterprises will obtain privacy data and push advertisements to users. In the above process, the privacy data owner almost loses control of his data. In the Metaverse, personal data misuse and leakage risk are massive. First, the Metaverse application platform misuses the personal data it collects. While metaverse platforms can aggregate massive amounts of privacy data, they may also break their promises and fail to use the privacy data they acquire strictly with the individual user's permission and authorization. Misuse of personal data may occur, posing a direct threat to the security of personal data. For example, Facebook has allowed more than a dozen companies broad access to the privacy data of its 2.2 billion users, including private information, names and contact information of friends, without consent. Another example is Facefirst which can provide users with facial expression services, age and identification services and in-store pickup services. It can enable faster and more secure transactions at kiosks, ATMs, and online applications [23]. Nevertheless, the process is highly complex, and it is difficult for individual users to know how the application platform will use the privacy data it collects.

Second, there is a risk of compromising the privacy security of the Metaverse as an infrastructure for personal data storage [24]. Based on personal data, metaverse applications can comprehensively understand a person's health and financial status and tap into a user's behavioral habits; they can also detect

and reveal changes in people's routines and displays of abnormal behavior. For example, Facebook analyzes and builds user networks, preferences, interests, and activities based on data from users and third parties. Their interactions in its platform, other users, places, and things with which they are connected, to customize their Facebook and Instagram profiles. Once a user's identity is stolen, intruders may be able to take control of the various end devices associated with the individual's identity, with severe and unpredictable consequences for the individual. Metaverse end devices are in the perception layer of the Metaverse. Suppose the metaverse platform does not deploy advanced security mechanisms, *e.g.*, complex encryption algorithms. In that case, they can not only be connected by the owner but may also be intercepted by an attacker. In this case, these things are highly vulnerable to reprogramming by an intruder in order to allow it to send data to the intruder's database server. An attacker could gain access and control of the computing device, possibly manipulating or extracting data and controlling or interrupting services. For example, the database of Fitbit, a provider of wearable devices used to assess health conditions, *e.g.*, sleep disorders, was hacked in January 2018, exposing the personal privacy data of more than 25 million users [25].

The Metaverse opens privacy data to third parties, which is also prone to personal data leakage [26]. Metaverse platform can provide rich interfaces for third parties. Any third-party developers who register, apply, and pass the examination can realize the relevant functions of their products or services through the open platform. In this process, the third party can get part of the user's data based on user authorization. Moreover, how these privacy data will be used by the third party or even continue to flow, in addition to the detailed specification requirements, the metaverse platform may not implement concrete regulatory measures.

4.4 Privacy security and sexual harassment in the Metaverse

The three features of Second Life are avatar, land and virtual objects, and currency. In addition to applying for an account to interact with others in the form of avatars, users can also buy land, build houses, and trade with tokens. Second Life's three main issues exposed are online harassment, data breach, and financial loss. A case study on online harassment is that of Miss Chung, a Second Life user who founded a company in Hubei. The company started in the Metaverse, and the income she earned in the virtual world was converted into real property, which many media outlets covered. During the media visits, some men used their avatars to enter and interact with her, using animations of sexual organs to attack her in a highly insulting way. In her husband's opinion, she was a successful woman who received media coverage and was discussed together through the Metaverse but was attacked unpleasantly. The photos of the attack were screenshotted by others and published on Youtube to be reported by other media. She used the concept of communication law to file a complaint against the media for copyright infringement, while the media argued that it was fair use to implement the story. Sexual harassment also occurred in Meta. Meta established a personal boundary in crisis management to keep the users' avatars at a distance when interacting with each other through gestures to avoid similar situations [27].

5 Legal safeguards for digital identity and privacy security in the Metaverse

According to Professor Zhang Wenxian, the legal order of an intelligent society has five elements, including science and shared governance. In terms of the Metaverse, scholar Li Jing proposed the idea of "law + technology" regulation to match the legal rules of the natural world with the rules of autonomy in the digital world [28]. According to Zheng Ge, the rule of law is a trust mechanism that relies on various state-led intermediaries to maintain social order and predictable interpersonal relationships [29]. The Metaverse is constructed almost entirely out of computer hardware and software code. In his book "Code 2.0: Law in Cyberspace", Professor Laurence Lessig proposes the idea of "code as law" [30]. Although the systems of the Metaverse, with blockchain as the underlying technology, can create increasingly autonomous and distinct systems from customary law, they are still ultimately controlled by real persons. In the book "On the Spirit of Law", Montesquieu pointed out that law is a necessary relation arising from the nature of things [31]. With the Metaverse boom, Montesquieu's ideal can be reflected in the evolution of human society in a new, purer, and more comprehensive way with blockchain technology. Even if blockchain does achieve extensive disintermediation, the law of people's consensus will still be needed to guarantee the

orderly operation of the Metaverse [32]. The healthy development of the Metaverse in the context of the digital economy urgently needs the legal safeguard of digital identity and privacy security, especially the personal information protection legal system and the Metaverse's unified digital identity authentication system.

5.1 Personal information protection legal system to protect the Metaverse privacy security

In the Metaverse, the behavior of the active subjects must comply with the rule of law. The current personal information protection legal system applies to the Metaverse scenario. China initially constructed a comprehensive system of personal information protection law, and it is based on the constitutional obligation of the state to protect. For the protection of personal information, the Personal Information Protection Law, the Civil Code, the Data Security Law, the Criminal Law, and other relevant laws have provided the primary legal basis for the protection system from both public and private law perspectives. In addition, there are also regulations and local legislation related to personal information. The laws mentioned above and regulations have been interlinked through legislative techniques such as "referral clauses" and "lead-in clauses" to achieve a systematization of norms through the interchange of various legal provisions on personal information protection.

The Personal Information Protection Law, characterized by the integration of public and private laws, defines, protects, and regulates almost all digital economic and social activities and behaviors and is a fundamental law that regulates almost all digital information society relations. This law is a milestone for the protection of the fundamental human rights of our citizens. Article 1 clearly states the purpose of the legislation, which is "to protect the rights and interests of personal information, regulate personal information processing activities, and promote the reasonable use of personal information". The law also establishes the "five principles" of personal information handling. Further, it clarifies the obligations of personal information handlers, which provides the primary legal basis for the construction of the management mechanism. The Civil Code is the fundamental law of private law. In Part IV, the essential protection of personal information is clarified in several aspects, such as regulating access to information, determining the scope of information protection, establishing the fundamental remedial rights of information subjects, and regulating the responsibility of information processors and administrative access to information. Starting from the scope of protection and fundamental remedy rights established by the Civil Code, the protection of personal information has gradually developed to improve the judicial remedy system by starting from the protection of legal interests of personality rights. In addition, the private law norms in the Civil Code and the Personal Information Protection Law constitute the relationship between the general law and the specialized law. When the latter has explicit provisions, the latter should be applied in priority. The interpretation should be based on the Civil Code when the latter has unclear and ambiguous situations. For example, the Personal Information Protection Law adds the principle of "good faith", but the meaning of "good faith" should be interpreted in accordance with Article 7 of the Civil Code. Considering the limitations of the protection model of personal information as a proper private object in terms of normative logic and institutional function, the Data Security Law, a technical public law standard, explicitly regulates the technical aspects of the use and protection of personal information from the government's perspective. In Chapter 3, the law establishes the basic system of classifying and grading the protection of various data types. Chapter 4 specifies the primary data security protection obligations of data processors. As for the protection of personal information under criminal law, the Supreme Court and the Supreme Prosecutor have issued several judicial interpretations on the protection of personal information. For example, the "Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Illegal Use of Information Network to Help Information Network Criminal Activities", promulgated in 2019, provides a comprehensive and systematic legal interpretation of the conviction and sentencing standards and legal application of personal information crimes.

5.2 Defining and classifying personal data in the Metaverse

Personal information is defined in Article 1034 of the Civil Code and Article 4 of the Personal Information Protection Act. The Civil Code emphasizes the difference in identification methods, distinguishing between direct and indirect identification of privacy data. On the other hand, the Personal Information

Protection Law distinguishes between identified and identifiable personal information and emphasizes the difference in the degree of identification of individuals. In the context of identity construction, privacy data reflects various ways of presenting an individual's identity. Both static identities (*i.e.*, identity markers) and dynamic identities (*i.e.*, social mirrors) can be used to identify a particular individual. However, the normative model of privacy security focuses not on the protection of identity as a result but on regulating the behavior of the process of identity generation. This means that, on the one hand, any data that affects the construction of personal identity, whether direct or indirect, identified or identifiable, should be included in the protection of personal identity. In other words, data in the Metaverse that is specific to an individual's physical, physiological, genetic, psychological, economic, cultural, or social identity, including data that evaluates an individual, de-identified data, theoretically falls within the scope of privacy data.

On the other hand, the key to privacy security is not to statically determine whether specific data belongs or does not belong to privacy data but to focus on how personal identity is generated in different contexts for more targeted behavioral regulation. With the development of digital technology, identification methods are becoming more and more diverse. In addition to inherent personality traits such as name and portrait, skin color, vein shape, genetic arrangement, walking posture, voice, fingerprints, palm prints, and other physical characteristics of a person in the Metaverse can be used as identifiers to identify a specific person. Behavioral traces and location information in the Metaverse can be used for identity verification and identification. Different paths of specification exist for these privacy data. Suppose an inherent element of personality characterizes personal identity, such as name and portrait. In that case, there is room for interpretation to expand the protection of name and portrait rights. From the perspective of personal identity construction, the types above of data all contain, to a certain extent, the identity code of a particular person. Distinguishing the significance of different identifiers in the generation of personal identity and imposing different levels of behavioral regulation on data processing may better balance the relationship between personal privacy and digital identity protection and data exploitation in the Metaverse. In privacy data, there is room for further exploration of what data is processed, what kind of processing may affect the correct perception of personal identity, and whether typological regulation is still needed. For example, there is a lack of clear thinking on whether the various evaluation data of individuals in the Metaverse need to be regulated in a focused and differentiated manner.

5.3 Rules of consent in the Metaverse

Concerning the consent rule, the Civil Code provides for it in Articles 1035, 1036, and 1038. Article 13 of the Personal Information Protection Act also stipulates that the individual's consent shall be obtained for processing privacy data, except for the cases specified in paragraph 1, items 2 to 7 of the same article. In the context of identity construction, identity is formed and developed due to interpersonal interaction in social relations. Therefore, consent to processing various privacy data in the Metaverse is not so much permission for others to dispose of elements of their personality as it is an attempt to show that the personal identity established through the processing of privacy data must, in principle, involve the person. In the Metaverse where the territorial boundaries of interpersonal interactions are broken, the distortion and inauthenticity of identity become a legal challenge. However, they can also create a huge obstacle to the autonomous construction of personal identity. Therefore, the Personal Information Protection Law emphasizes the principle of privacy data processing with the individual's consent. It specifies that data processing should have a clear and reasonable purpose and should be directly related to the purpose of processing.

Further, it adopts a way that has the most negligible impact on the rights and interests of the individual. It requires that data processing should be open and transparent. The individual's consent must be obtained once the purpose of processing, the way of processing and the type of privacy data processed are changed. In essence, the parties withdraw their consent on their own, emphasizing the individual's autonomous participation in constructing his identity in different contexts. Covering the mirror image of the self presented by the individual's participation in social life is necessarily a scenario-based construction process. In different contexts of social relations, individuals can form multiple social identities through conscious activities, thus fully expressing themselves and developing their personalities.

5.4 Metaverse unified digital identity and privacy security protection

With the expansion of the scope of socio-economic activities in the Metaverse, there is an objective need to establish a unified system of official subject qualification. Identity information will be stored in a unified encrypted system of government departments to provide personal identity data that matches the real physical world. This may effectively solve the problem of false identity information to gain the general trust of society. By establishing a unified identification platform and standards, the state can centralize the management of various identity data and achieve technical and legal isomorphism. When a real user enters an app with specific functions in the Metaverse, he has to provide accurate information in the official registration and identification system. After identity matching with the public security system, he will be qualified for access and given a personal digital badge through the digital encryption technology mechanism, enjoying a permanent and independent metaverse ID. To be homogeneous with the law, each Metaverse should set up a certified identity interface at the technical level. The interface layer is to provide basic operational interfaces, not only for users and merchants but also for regulators. The interface layer can provide essential identity authentication services; realize initial identity identification; provide a unified trust model for the whole network; support common access of multiple identity providers; secure authentication of multiple identity formats; and integrate and unify multiple identity information sources authentications. It also automatically completes predefined conditions by embedding predefined authentication rules in the blockchain. In this way, the authenticity of the identity can be determined, which is convenient for inquiry and comparison, and the relevant privacy data can be appropriately corrected through the flexible control and management of remote nodes to overcome the severe drawbacks of blockchain technology. Officials can use the NFT, which can be applied to identity proof, record, and native digital asset confirmation. This unique and indelible identity and ownership record can provide digital assets and identity security.

Metaverse is an online digital virtual world that maps the real world. The digital twin technology creates the same avatar as the natural body for companies and users. The personal digital badge is the qualification to engage in socio-economic behavior in the Metaverse. In order to better identify the relevant subjects in the virtual world and increase the sense of trust, a subject identification mechanism can be established. The amount and degree of subject identification information can be decided by oneself, either anonymously or conspicuously, following the orientation of liberal values and realizing the principle of selective display. To identify the subject by name, we can establish a highlighting identification mechanism, *i.e.*, the relevant subject can display the basic personal information of the other party, such as name, gender, and integrity data, by highlighting. However, users can only simultaneously enjoy one corresponding virtual digital identity in the Metaverse. For example, a female digital model cannot be selected if a male data model is selected. A minor digital accessory cannot be selected if an adult digital accessory is selected. At the same time, multiple digital person types cannot be selected. Otherwise, it will lead to difficulties or even confusion in identification. The data person of the Metaverse can be anonymized. However, when it comes to the fundamental rights and obligations relationship, it should be oriented to the value of the order and be visible through specific lighting rules, taking into account the transaction security and the realization of the value of personal privacy data protection.

5.5 Civil liability for wrongful infringement of digital identity and privacy security in the Metaverse

The Civil Code does not specify the liability for wrongful handling of digital identity and privacy data in the chapter on "Protection of Privacy and Personal Information" but only provides for the exemption from civil liability in Article 1036. Theoretically, it is necessary to explain whether the remedies for infringement of personality rights in Articles 995 to 1000 of the Civil Code can be applied to the scenario of unlawful infringement of digital identity and privacy security. There are two different possible interpretative options for this. One is to interpret the relevant digital identity and privacy security provisions as an *ex-ante* remedy to protect individuals' specific personality or property rights. The unlawful collection, leakage, sale, or exploitation of digital identity and privacy information may lead to the infringement of personal property rights or the impairment of human dignity and personal freedom. Logically, it appears that victims must still seek relief under Sections 995 through 1000 based on various specific personality rights and interests that may be violated due to the criminal violation of digital identity and privacy security. For example, suppose the perpetrator improperly discloses the victim's privacy data, ultimately damaging

the latter's reputation. In that case, the perpetrator is not subject to civil liability for improper handling of privacy data but rather for infringement of the right to reputation. Another interpretation option is to broadly interpret the personality rights in Articles 995 to 1000 to include rights to privacy data so that the person concerned can wrongfully infringe on digital identity and privacy security. In this way, a person may directly claim the remedies under Articles 995 to 1000 because his personal identity rights and interests have been damaged due to unlawful infringement of digital identity and privacy security. The personal identity rights and interests carried on privacy data fall within the scope of other personal rights and interests of natural persons based on personal freedom and human dignity, as stated in Article 990, Paragraph 2 of the Civil Code. Therefore, if the perpetrator cannot claim relief for the violation of digital identity and privacy security, it is necessary to determine the liability by evaluating the impact of the relevant privacy data processing behavior on the freedom of personal identity construction. Article 69 of the Personal Information Protection Law expressly provides compensation for damages for infringement of digital identity and privacy security. The provision considers the information asymmetry in privacy data processing and clarifies the rule of reversing the burden of proof in determining the fault of privacy processors. Both property damage and moral damage need to be judiciously judged in the context of the specific scenario of digital identity construction.

6 Conclusion

In our human history, we have never stopped searching for our inner selves. However, it is only in the last hundred years that we as human beings have come to realize that our identity is not an immutable core hidden in the depths of our existence but a collection of ideas inscribed on our bodies from the outside. However, this modern notion of human identity is, in a certain sense, the original face of personality. Protecting rights to personality has never deviated from the main line of protecting our personal identity. Behind the continuous expansion of this protection as society changes, it reflects our increasingly profound knowledge and reflection on self, human identity, and dignity. In the era of the Metaverse, digital identities are formed by the digital presentation of the individual self. There are all kinds of new problems caused by the pluralism, fragmentation, and contextualization of digital identity. There is a massive risk to privacy security behind digital identity. Therefore, if we reinterpret the normative meaning of privacy security protection in the context of identity construction, we can find that the object of privacy security is never privacy data itself but precisely the autonomy and integrity of our digital identity construction in the Metaverse era. Is the existing privacy security protection sufficient to cope with the personal identity crisis in the Metaverse era? The digital identity carried on top of the privacy data is the only bridge that genuinely connects human beings' physical world and the Metaverse. Perhaps, it is not far for us to reconstruct the new order of human relationships in the Metaverse era with digital identity and privacy security as the center.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability

No data are associated with this article.

Authors' Contributions

Both authors have equal contributions.

Acknowledgements

No acknowledgments.

Funding

This work was supported by the 2021 National Social Science Foundation Project titled "Research on the Legal Risks and Prevention of China's Social Media Platforms Operating in the United States" (21BXW040).

References

[1] Sun Y. On the Adjustment of the Metaverse and the Intelligent Socio-Legal Order, 2022, Legal Research.
[2] David L. 'Digital Identity in the Metaverse'. Forbes, 2021, https://www.forbes.com/sites/forbesbusinesscouncil/2021/12/28/digital-identity-in-%0D%0Athe-metaverse/?sh=737835831fb6%0D%0A.

[3] Zhaowang L. 'The Order and Rules of the Metaverse'. ACADEMICS, 2022.
[4] Stephenson N. Avalanche. Sichuan Science and Technology Press, 2018.
[5] Zhu JM. Metaverse and Post-Human Society. Economic Observer, 2021.
[6] Xiao C. Spatial Reconstruction Analysis of the "Metaverse". Geography and Geographic Information Science, 2022.
[7] Qin X. The First Campus Metaverse Model "CUHKSZ Metaverse" Was Born in Hong Kong Central University (Shenzhen), In-Depth Interview With Designer Prof. Cai Wei. Daily Daily Planet, 2021.
[8] Yu G. The Future of Media: Iteration, Restructuring and Sublimation of "Human Connection" – From "Scene Era" to "Metaverse" to "Heart World", 2021.
[9] Yu J. Metaverse: Political Order Reconstruction and Challenges in a Changing World. Exploration and Controversy, 2021.
[10] CoinYuppie. Metaverse and Self Sovereign Identity (SSI): The New Superpower? In: Lessig L, editor, Code 2.0: Law in Cyberspace, Tsinghua University Press, 2018. https://coinyuppie.com/metaverse-and-self-sovereign-identity-ssi-the-new-superpower
[11] Wang W and Dong S. Identifying digital identities in a Metaverse environment. China Soc. Sci. J. 2022. http://ex.cssn.cn/zx/bwyc/202207/t20220721_5418801.shtml
[12] Chen J. Beyond the Metaverse: Digital Identity, NFT and Plural Regulation NFT and Pluralistic Regulation. Legal Research, 2022.
[13] Miller V. The Essence of Digital Culture. Tsinghua University Press, 2017.
[14] Wang W and Dong S. Identifying Digital Identities in a Metaverse environment. Chin Soc Sci J 2022. http://ex.cssn.cn/zx/bwyc/202207/t20220721_5418801.shtml.
[15] Luhmann N. Trust: A Simplifying Mechanism of Social Complexity. Shanghai People's Publishing House, 2005.
[16] Lee V. Freedom and Order: Value Choices of Metaverse Access and Meta-Rules of Identity Authentication. Legal Research, 2022.
[17] Chenxin R. The Legal Limits of Internet Trusted Authentication from the Perspective of Legal Benefit Measurement. Eastern Law, 2020.
[18] Jinhua C. The Rule of Law Principle of Metaverse Governance. Eastern Jurisprudence, 2022.
[19] Lu Q. Identity construction and its legal protection in the digital age: reflections on the protection of personal information. Chin J Law 2021; 43.
[20] Chen H. User data privacy in the Metaverse. J Xinjiang Normal Univ 2022, Philosophy and Social Science.
[21] Kramer ADI, Guillory JE and Hancock JT. Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks. Princeton University, 2014.
[22] Stouffer C. Online Scams: An Overview + 20 Internet Scams to Avoid in 2023, 2022. https://us.norton.com/blog/emerging-threats/internet-scams#.
[23] Facefirst. Stop In-Store Violence and Theft with Facefirst Facial Matching Software, 2022. https://www.facefirst.com.
[24] Guo X. Personal information security challenges and responses in the era of artificial intelligence. J Zhejiang Univ. Humanities and Social Sciences, 2021.
[25] More Than 200 Classified Areas around the World Leaked, US, UK, Russia, France And Netherlands Pitted by A Watch. Watchdog.com, 2018. https://www.guancha.cn/internation/2018_07_11_463658_2.shtml.
[26] Yu L and Zhou X. Technology Embedding: The Construction of Individual Privacy Security System in Cyberspace: An Analytical Framework Based on Concept, Technology and System. J Henan Norm Univ (Philos Soc Sci) 2022; 49.
[27] Sharma V. Introducing a Personal Boundary for Horizon Worlds and Venues. Meta, 2022. https://about.fb.com/news/2022/02/personal-boundary-horizon/.
[28] Jing L. On the Legal Nature of Artificial Intelligence Virtual Idols. Zhejiang Social Science, 2020.
[29] Zheng G. Blockchain and the Future Rule of Law. Eastern Jurisprudence, 2018.
[30] Wang W and Dong S. Identifying digital identities in a metaverse environment. Chin Soc Sci J 2022. http://ex.cssn.cn/zx/bwyc/202207/t20220721_5418801.shtml.
[31] Li X. Legal Governance of the Metaverse in the Perspective of Structural Changes in Network Society. Legal Research, 2022.
[32] Montesquieu B. On the Spirit of the Law (First and Second Volumes) The Commercial Press, 2009.

Hong Wu is currently an associate professor at NingboTech University. His research interests include data law, AI law, and social media law.

Wenxiang Zhang is currently a professor at NingboTech University. His research interests include cyberspace governance and media law.