LEGAL CHALLENGES OF DATA PROTECTION IN THE METAVERSE.

CHEIFA BADIAA[1], KARROUM NESRINE[2]
[1]University of Amar Telidji in Laghouat (Algeria).
[2]The University of BLIDA 2 (Algeria).
The Author's E-mail: b.cheifa@lagh_univ.dz[1], kerroum.nes@gmail.com[2]
Received: 06/2024 Published: 12/2024

Abstract:
The metaverse, a virtual world merging the physical and digital realms, presents new challenges in the field of personal data protection due to its complex interactive environment and reliance on advanced technologies such as Virtual Reality (VR) and Augmented Reality (AR). As users continuously interact in this digital space, vast amounts of data are generated, extending beyond traditional information like names and emails to include biometric data (e.g., eye and body movements) and sensitive behavioral patterns.
In light of these developments, several key legal challenges arise. This study aims to explore the concepts of the metaverse and data privacy, particularly under Algerian legislation (Law 18-07), and examine the major legal issues concerning data protection in the metaverse.
Keywords: *Metaverse, Data Protection, Privacy Laws, Digital Privacy, Virtual Reality Personal Data Security.*

INTRODUCTION:

With rapid technological advancements, the "Metaverse" has emerged as one of the futuristic domains capturing the interest of companies, governments, and individuals alike. The Metaverse is an integrated virtual environment that allows users to interact and communicate through technologies such as virtual reality and augmented reality.
The legal system now stands on the brink of a new challenge, addressing contemporary developments that encompass the virtual world, filled with imagination that often defies human comprehension.
Human beings can no longer live in isolation from the astonishing advancements in technology, which have made the virtual world one of the most significant innovations, offering individuals various options that distance them from their real lives and immerse them in the diverse realms presented by social media. These platforms have laid the foundation for new types of human relationships.
This evolution in artificial intelligence has given rise to behaviors and aspirations that drive individuals to seek lives beyond their current realities, existing in a virtual realm that straddles the line between truth and imagination.
However, this development is accompanied by legal challenges, particularly those related to **data protection and privacy**, which are among the primary concerns regarding the foundational systems of the Metaverse.

Study Problem:
Although current data protection and privacy laws are controversial in the physical world, these issues are expected to become even more concerning and prominent in the digital virtual world. Virtual reality platforms will enable organizations to collect personal data that is typically inaccessible through a smartphone app or computer screen. These platforms are anticipated to be intrusively invasive.
With the growing expansion of the Metaverse, new data privacy challenges are expected to emerge. These challenges raise numerous legal issues that necessitate legislative intervention to address them, ensuring the protection of users' rights and mitigating the potential risks associated with privacy.

Study Methodology:
The study adopts a descriptive-analytical approach, focusing on defining the concept of Metaverse technology and its characteristics, presenting the legal challenges related to data protection within the Metaverse, and addressing the legislative and regulatory issues associated with it.

Section One: The Metaverse and Data Privacy
The concept of the Metaverse traces its origins to American author Neal Stephenson, who first introduced the term in his 1992 novel, Snow Crash. In this novel, Stephenson envisioned a three-dimensional virtual world where people interact through digital avatars representing them. Since then, the idea has significantly evolved alongside advancements in virtual reality (VR) and augmented reality (AR) technologies, as well as the widespread adoption of the Internet and social networks.

First Topic: The Concept of the Metaverse
First Subtopic: Definition of the Metaverse
The Metaverse is a fully integrated three-dimensional virtual world accessible via the Internet, allowing users to interact through virtual avatars. This world is built on a combination of virtual reality (VR) and augmented reality (AR) technologies, providing an immersive experience that mimics real-life interactions. The Metaverse opens new horizons across various fields, such as social interaction, work, education, and entertainment.[1]

Second Subtopic: Characteristics of the Metaverse
1.**Dynamic and Open Environment:** Users can create their own content and explore diverse virtual worlds.
2. **Advanced Social Interaction**: Offers opportunities to build relationships and communicate in new and innovative ways.
3.**Integration of Advanced Technologies** : Employs artificial intelligence
and blockchain to ensure secure and efficient resource and data management.
Integration of Mixed Reality: Combines physical reality with virtual worlds to provide a seamless experience .that mimics everyday life
Continuity of the Metaverse: The Metaverse will persist and remain operational as long as the underlying .technology continues to exist
Decentralization of the Metaverse: This refers to the idea that technology companies cannot own or control [2].the Metaverse. Instead, it represents a collectively shared technical infrastructure

Second Topic: Defining Legal Concepts Related to Personal Data and Principles of Its Protection

The use of computers for collecting and processing personal data related to individuals' private lives has brought about significant positive impacts, particularly in enabling the state to organize its economic, social, and .scientific affairs

[1] Mohamed Gaber Ibrahim Hassan, "The Legal Framework of Metaverse Technology: A Foundational and Prospective Study," Journal of Legal and Economic Sciences, Issue 85, p. 128.

[2] _ Khaled Mamdouh Ibrahim, *The Legal Regulation of Metaverse Technology*, Dar Al-Fikr Al-Jami'i, Alexandria, 1st Edition, 2023, p. 75.

However, this development necessitated the establishment of an effective protective system to ensure the .legitimate objectives of data collection are met

The Algerian legislator, through the **Law on the Protection of Natural Persons in the Processing of Personal Data**, introduced a series of provisions aimed at safeguarding the right to privacy, especially in light of rapid technological and scientific advancements that increase the risk of violations. These provisions include defining the legal concepts for all parties involved in personal data processing, setting forth the fundamental principles [3] .required to ensure adequate legal protection, and clarifying legal responsibilities in cases of breaches

First Subsection: The Concept of Personal Data and Its Automated Processing

The Law on the Protection of Natural Persons in Algeria defines personal data as **any information relating to an identified or identifiable individual, whether directly or indirectly, such as a name, identification number, or any attribute related to their physical, physiological, genetic, biometric, psychological, economic, cultural, or .social characteristics

Article 03/1, Law No. 18-07 of June 10, 2018, on the Protection of Natural Persons in the Processing of) (.Personal Data, Official Gazette, Issue 34

With the advent of the Internet, available data is no longer limited to names, surnames, and addresses. It has .**expanded to include **a person's image, voice, financial status, habits, preferences, and biometric data

(Such as fingerprints or iris scans). These sensitive pieces of information have become an integral part of .personal data that must be protected

Due to the sensitivity of such data, its processing requires strict adherence to rules to ensure the **privacy of individuals** is not violated. This is particularly important as this type of information can reveal intricate details about a person's private life, health, or personal behaviors, underscoring the necessity for a clear legal .framework to safeguard it against any misuse

Second Subsection: Fundamental Principles for the Protection of Personal Data

Law No. 07-18, in its second chapter, outlines the fundamental principles governing the protection of personal data. Adhering to and upholding these principles provides a crucial legal safeguard for preserving this right. :From an analysis of the provisions in this chapter, the key principles can be summarized as follows

First: The Principle of Prior and Explicit Consent of the Data Subject

According to the Personal Data Protection Law, **the processing of personal data is prohibited unless explicit consent is obtained from the individual concerned**. The data subject also has the right to withdraw their consent at any time. The law further specifies instances where data processing is deemed necessary, and in such .(07-[4]cases, consent may not be required (Article 7/5 of Law No. 18

The disclosure of personal data under processing to third parties is **prohibited unless it directly serves the purposes related to the responsibilities of the data processor and the recipient, and only after obtaining the individual's consent. Therefore, any processing conducted without prior consent is considered unlawful. Consent acts as a vital legal tool to prevent potential disputes between the data processor and the individual

[3] _Article 03/1 of Law No. 18-07 dated June 10, 2018, concerning the protection of natural persons in the processing of personal data, Official Gazette No. 34.

[4] _Article 7/5 of Law No. 18/07.

concerned, ensuring that both parties adhere to their respective rights and obligations as per the terms of consent .(Article 7/4 of Law No. 18-07)

Second: The Principle of Legality

The Algerian legislator mandates that personal data must be processed in a lawful and fair manner, respecting all relevant legal provisions and procedures. The data must be collected for a specific, clear, and legitimate purpose, and it cannot be used subsequently for purposes that are inconsistent with the objectives for which it was initially collected [5]

Third: The Principle of Proportionality

This principle requires that personal data be appropriate, relevant, and not excessive in relation to the purposes for which it is collected. The data must be necessary and directly related to those purposes, ensuring that only [6].the information essential for achieving the legitimate objective is collected

Moreover, the collection of unnecessary or excessive data in comparison to the defined purposes of processing is strictly prohibited. This ensures the protection of individuals' privacy and prevents the misuse of their .personal information

Fourth: The Principle of Accuracy and Correctness

personal data be accurate and, where necessary, kept up to date. Measures must be This principle requires that taken to erase or correct any incorrect or incomplete information. This ensures the transparency of data processing and guarantees confidentiality and security in the automated processing of this data, in accordance with the provisions of Law No18_07 , thus effectively protecting individuals [7]

Fifth: The Principle of Data Retention Limitation

This principle mandates that personal data be retained only for as long as necessary to fulfill the purposes for which it was collected. It is prohibited to keep this data indefinitely or permanently in automated files, unless special permission is granted by the relevant authority. The retention period may be extended for historical, statistical, or scientific purposes based on a request from the data processor and within the scope of a , [8].legitimate interest

Sixth: The Principle of Prior Formalities Before Processing

This principle requires the data controller to comply with formal procedures prior to the processing of personal data. This includes ensuring that all necessary legal and procedural steps are taken before data processing

[5] _Article 7/4 of Law No. 18/07.

_**Article 9 of Law No. 18/07**[6]

[7] Yahya Toumi, *The Legal Protection of Personal Data in Light of Law No. 18-07: An Analytical Study, Professor Researcher Journal of Legal and Political Studies,* Mohamed Boudiaf University, M'sila, Vol. 04, No. 02, 2019, pp. 1521–1554.

[8] _ *International and National Legal Protection of Personal Data in Cyberspace, Journal of Legal and Political Sciences,* University of El-Oued, Vol. 10, No. 1, April 2019, pp. 1304–1325, with reference to p. 1310 (adapted).

begins, in order to guarantee the protection of individuals' rights and ensure compliance with data protection [9].regulations

This principle requires the data controller to adhere toformal procedures prior to the processing in order to ensure the protection of the rights and freedoms of the data subject. The controller is required to obtain prior authorization from the national authority for the protection of personal data if the assessment indicates that the processing poses a clear risk to privacy or fundamental rights and freedoms. The authority has the right to refuse [10].the authorization or request modifications to the processing to ensure compliance with the legal framework

Chapter Two: The Impact of the Metaverse on Data and Privacy

The metaverse, a rapidly evolving digital ecosystem, introduces unprecedented opportunities for interaction and innovation. However, its reliance on extensive data collection and processing raises critical concerns regarding privacy and the protection of personal information. This chapter explores how the metaverse reshapes the landscape of data usage and privacy, highlighting potential risks, legal challenges, and the need for robust regulatory frameworks to ensure the ethical and secure handling of user data in this immersive virtual environment.

Section One: The Relationship Between the Metaverse and Data Privacy

The Metaverse intersects closely with data privacy, as the virtual environment requires the processing of vast amounts of personal data, presenting legal and ethical challenges related to safeguarding user privacy. Below is :an explanation of the relationship between the metaverse and data privacy

Subsection One: Collecting Vast Amounts of Personal Data

The Metaverse relies on technologies such asvirtual reality (VR) and *augmented reality (AR)**, which collect :precise data about users, such as

.Biometric data (eye movements, facial expressions, body features)** -

.Location and activity data (user behaviors in the virtual world)** -

.Social interactions (chats and participation in virtual events)** -

This wide range of data collection increases the likelihood of **privacy violations if strict controls are not [11].applied on how this data is used

The Risk of Data Breach and Misuse .

In the Metaverse, there are significant*risks of data breaches** or the unlawful use of personal data for commercial** purposes (such as targeted advertising) or **illegal** activities (such as spying or ** psychological manipulation). Because users interact through **digital avatars** in a reality-like environment, the data collected can reveal **personal secrets or behavioral patterns with greater precision than what is typically found on traditional internet platforms

Second Requirement: Legal Challenges Related to Data and Privacy

Adopting Clear and Transparent Privacy Policies** that define the nature of the data collected and the ** -
.purposes for its use

.Developing New Legal Frameworks that align with the specific characteristics imposed by the virtual world -

.Enhancing Digital Awareness among users about the risks of sharing personal data in the metaverse** -

[9] _Yahya Toumi, *The Legal Protection of Personal Data in Light of Law No. 18-07: An Analytical Study, Professor Researcher Journal of Legal and Political Studies,* Mohamed Boudiaf University, M'sila, Vol. 04, No. 02, 2019, pp. 1521

[10] _Giles Hogben,virtul Word:Real Money,European Network and Information Security Agency ,Heraklion,2008,p83

[11] _Giles Hogben,virtul Word:Real Money,European Network and Information Security Agency ,Heraklion,p83

In summary, the metaverse is a promising field but is fraught with risks related to privacy violations, which .requires a combination of legal and technological efforts** to ensure the protection of personal data for users

Subsection One: Legal Issues Related to Data Protection in the Metaverse

The challenges of data privacy in the metaverse are similar to those posed by traditional social media platforms. However, it is important to consider the nature of the underlying technology of the metaverse, where users interact more deeply and extensively with their virtual environment, thus generating more personal data from :their activities. This data raises several legal issues, which are outlined as follows

Data Privacy in a Large-Scale Virtual Environment .

In the metaverse, a wide variety of data is collected, such as physical movements, gestures, biometric data, .geographical location, as well as interactive and social activities of users

The legal challenge lies in how to apply traditional data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union or the California Privacy Protection Law, to a global virtual .environment where servers and users may be distributed across multiple countries with different regulations

Ownership and Control of Data

In the metaverse, questions arise regarding who owns the collected data: Is it owned by the user, the platform ?provider, or the third-party developers

Some companies may resort to complex, long-term licensing agreements that make it difficult for users to understand their rights regarding their data. This issue becomes more complex with the involvement of multiple .parties in platform management

Explicit Consent for Data Collection .

The metaverse requires explicit consent from users to collect personal data. However, in this virtual environment, it may be difficult to ensure that users have given their consent in a thoughtful and comprehensive manner. Moreover, the variety of data being collected raises questions about the clarity and transparency of such consent

In the virtual world, it is difficult to ensure that users have given informed and explicit consent for the collection .of their data, as consent is often provided through quick clicks on complex and unclear terms of use

This presents a challenge in relation to the principle of "free consent," which is one of the cornerstones of data .protection laws, such as the GDPR

****Cybersecurity and Potential Leaks**** .4

Protecting data in the metaverse requires strong security strategies due to the sensitive data being collected. Any security breach could expose sensitive information about users, including their biometric data, putting them :at risk for issues such as

Identity Theft and Avatar Theft

Another privacy concern is the theft of the user's virtual identity, or "avatar." This could be problematic in immersive virtual spaces that allow users to create realistic avatars. For instance, deepfake technology has already been misused to produce pornographic material involving users, and realistic avatars could also be used .to create simulated pornographic images showing the victim

.The key point is that this form of identity theft can be an issue even if no one is deceived

:Ease of Access to User Data[12] -

[12] Liska Strikwerda ,A philosophical Legal Analysis of Virtual Cy bererime,faculty of Behavioral,Adminstrative and Sociel Seiences,University of twente ,Dissertation,Doctoral THESIS,2021.

As a result of Facebook's heavy investment in virtual reality technology, being one of the largest tech investors, and with the upcoming release of its virtual reality headset, Facebook has required users to log into their Facebook accounts to access the virtual reality device. This raises several privacy issues, as accessing the Facebook virtual reality device inevitably involves registering and collecting data. The amount of personal information collected about users in the metaverse is far beyond what has been collected in the flat-screen .world

Furthermore, data collection allows advanced virtual reality technologies for applications and service providers .to access this information in order to develop targeted advertisements based on better inference techniques

.However, with laws and regulations concerning data protection, user data privacy and security can be ensured

:Using Metadata to Influence Users' Minds -

Manipulating personal data and controlling behaviors by collecting detailed information about users' actions, operators of platforms may use algorithms to influence individuals' behaviors and guide them toward specific decisions. Metadata can be used to influence the minds of voters toward a particular party, ideology, or leader [13]by regularly showing them content that serves that cause

Difficulty in Identifying Users within the Metaverse -

Another interesting issue is that individuals in the metaverse will have multiple and different identities, whether it's their real identity in a professional context, their identity with friends and family, or fictional characters they don't want to be linked to their real life. This identity is called a decentralized identity or self-sovereign identity, .where individuals control their identity through blockchain technology

When someone has multiple identities and personas within the metaverse, there is a legal challenge in determining the true identity of the person you're interacting with—whether they are a man or woman, an adult or a minor. This certainly impacts the validity of contracts and electronic transactions, as well as determining the [14]appropriate jurisdiction in case of a legal dispute

****Subsection Two: Regulatory and Legislative Challenges for Data Protection in the Metaverse**

1 Difficulty in Determining Legal Responsibility

From a data protection and privacy perspective, the development of metaverse platforms raises many unanswered questions. For example, who is responsible for processing the data? Who will be accountable for lost, stolen, or manipulated data? How and when will users provide consent for data processing? These are just .some of the legal questions that need to be addressed

Another legal issue related to data privacy is whether this data will be stored by multinational companies or a separate data agency, and whether the data will be retained in the local country or exported to another country. Who will be responsible in cases of data breaches or privacy violations? And most importantly, do multinational ?companies face any restrictions on the types of data they are allowed to collect

Subsection Two: Regulatory and Legislative Challenges for Data Protection in the Metaverse

_ Absence of a Unified Global Legal Framework .

Since the metaverse does not adhere to specific geographical boundaries, the application of national and regional legislations can become complex. There is a need to establish a coordinated international legal [15].framework that regulates data protection in this virtual world

_ Liska Strikwerda.op.98[13]

[14]Khaled Mahmoud Ibrahim, *Op. cit.*, p. 184.

Khaled Mahmoud Ibrahim, *Op. cit.*, p. 184.[15]

_Challenges in Law Enforcemen

Regulatory authorities may face difficulties monitoring compliance with data protection laws due to the decentralized nature of the metaverse. Additionally, the lack of effective mechanisms for cooperation between .countries complicates the enforcement of penalties against violators

: Conclusion

In conclusion, this study shows that the emergence of the metaverse presents multiple legal challenges related to the protection of personal data and user privacy. As reliance on this virtual world increases, the need for a cohesive legal framework to regulate data handling and ensure individuals' rights in this unconventional digital :environment becomes more pressing. Among the main issues discussed

- Unclear Jurisdiction: Due to the global nature of the metaverse, it becomes difficult to determine the .appropriate legal authority in case of a dispute
- Weak Existing Legal Frameworks**: Most current data protection laws were designed for the traditional .internet world, making them inadequate to cover all aspects of the metaverse
- Balancing Innovation and Privacy: Rapid technological development may conflict with privacy laws that .impose restrictions on data collection and processing
- Managing Biometric Data: Since the metaverse may require the collection of sensitive data (such as facial .features or movements), specific laws are needed to protect this data from misuse

:Recommendations

- Issuing New Specialized Legislation: Countries and international organizations must develop legislation that .considers the unique nature of the metaverse and the privacy risks it entails
- Harmonizing Legal Frameworks Globally**: To avoid legal conflicts between countries, international .agreements should be pursued to regulate data protection in virtual environments
- Companies operating in the metaverse should be required to disclose how they : Enhancing Transparency .collect and process data, ensuring users have the right to consent or opt out
- Strengthening Enforcement Mechanisms and Accountability: To ensure effective law enforcement, monitoring .and penalties for violations should be enhanced
- Raising Awareness and Building Capacity: It is crucial to educate users about the risks associated with the .metaverse and their legal rights, as well as to train legislators on the technical aspects of this environment

In the end, finding comprehensive legal solutions to protect data in the **metaverse** is critical to maintaining user trust in this virtual world. Achieving this requires a combination of legislative efforts, international cooperation, .and ethical commitment from the developing companies

REFERENCES AND PUBLICATIONS

1. Mohamed Jibril Ibrahim Hassan, *The Legal Framework of the Metaverse Technology: A Pioneering and Foresight Study*, Article in *Journal of Legal and Economic Sciences*, Issue 85,
2. Khaled Mamdouh Ibrahim, *The Legal Regulation of Metaverse Technology*, Dar al-Fikr al-Jami'i, Alexandria, 1st Edition, 2023,
3. Law No. 18-07 of June 10, 2018, concerning the protection of natural persons in the processing of personal data, Official Journal, Issue 34.
4. Tumi Yahya, *Legal Protection of Personal Data under Law No. 18-07: An Analytical Study*, *Professor Research Journal of Legal and Political Studies*, Mohamed Boudiaf University, M'sila, Volume 04, Issue 02, 2019, 1554.
5. *The International and National Legal Protection of Personal Data in the Legal Sphere*, *Journal of Legal and Political Sciences*, University of El-Oued, Volume 10, Issue 1, April 2019, pp. 1304-1325, p. 1310, with modifications, Algeria.

6. Giles Hogben, *Virtual World: Real Money*, European Network and Information Security Agency, Heraklion, 2008,
7. Liska Strikwerda, *A Philosophical Legal Analysis of Virtual Cybercrime*, Faculty of Behavioral, Administrative, and Social Sciences, University of Twente, Dissertation, Doctoral Thesis, 2021.