



RESEARCH ARTICLE

Legal Challenges of Digital Identity in Metaverse and Their Impact on Foreign Direct Investment (Descriptive-Analytical Study)

Rania S, Azab ^{1*}, HosamEldin H. Ismail ²

¹Assistant Professor of Civil Law , Department of Law, College of Business Administration, Northern Border University, Arar, Saudi Arabia.

²Assistant Professor of Economic, Department of Administrative Sciences, Applied College, Northern Border University, Arar, Saudi Arabia.

ARTICLE INFO	ABSTRACT
Received: Oct 28, 2024 Accepted: Dec 22, 2024	<p>The research will address the legal challenges related to digital identity in Metaverse and its impact on attracting foreign direct investment. In an era of increasing importance of digital spaces, Metaverse is emerging as a new environment that enhances social and economic interaction, which requires understanding the legal challenges associated with it. Several key aspects will be analyzed, including the privacy of personal data and how to protect it in a complex digital environment, as well as intellectual property issues related to content created and shared in Metaverse. Legal regulation and how it may affect the confidence of foreign investors in this space will also be addressed. By analyzing these factors, the research aims to provide practical recommendations for developing a comprehensive legal framework that enhances the attractiveness of Metaverse for foreign investment. This will contribute to creating a safe and reliable investment environment that supports innovation and economic growth.</p>
Keywords	
Metaverse	
Digital identity	
Privacy security	
Rights Security	
Intellectual	
property	
*Corresponding Author: ranias2010@gmail.com hhismail24@gmail.com	

INTRODUCTION

Digital identity and Metaverse

Evolving concepts in the digital age, Digital identity represents the virtual presence of an individual or entity in the digital world, as it reflects a set of personal information such as name, photo, and data that is used in online interaction. Since the advent of the Internet, digital identity has become an integral part of how individuals communicate with each other and with institutions, contributing to shaping social and economic relationships (Petar Radanliev, 2024), As for Metaverse, it is an integrated virtual world that allows people to interact in three-dimensional environments, providing immersive experiences through technologies such as virtual reality (Zhang & Wu, 2023) and

augmented reality. This concept has developed significantly in recent years, becoming part of discussions about the future of the Internet and how to integrate digital life with everyday life. With increasing reliance on technology, digital identity and Metaverse are becoming more important, (Ruiu et al., 2024), requiring the development of effective strategies to protect privacy and ensure the security of individuals in these new environments. These developments reflect a fundamental shift in how we understand social and economic interaction in the digital age.

Historical background on the emergence of Metaverse and its importance in the digital economy

Metaverse concept emerged as a new digital space with the advancement of digital technology (Cheng et al., 2022), tracing its origins to the 1992 science fiction novel (Snow Crash) by Neal Stephenson, which imagined a virtual world where individuals interacted through digital avatars. Since then, this idea has seen significant development, especially with the emergence of technologies such as virtual reality (VR) and augmented reality (AR), (McKinsey & Company, 2022) allowing people to experience immersive interactions in 3D environments. In recent years, Metaverse has become an integral part of the digital economy, providing a new platform for commerce and social interaction. (Falchuk, et al., 2018), With increasing reliance on technology, Metaverse has become a unique opportunity for companies and individuals alike, contributing to creating new markets and enhancing innovation. Metaverse is expected to contribute to increased investments and the development of new business models, making it a vital element in shaping the future of the digital economy. This new digital environment is extremely important, as it allows individuals and companies to communicate and interact in innovative ways, which enhances the user experience and increases the attractiveness of investment in this field. As technologies continue to evolve, Metaverse is expected to play a pivotal role in reshaping the digital economy, opening new horizons for growth and innovation.

Research Importance

1- The importance of digital identity in Metaverse and the impact of legal challenges on investor confidence

In Metaverse digital identity is increasingly essential, (Lucatch, 2021) as it connects individuals to a virtual world of social and economic interactions. It enhances user experience by allowing the creation of virtual personas that reflect real identities for interaction in 3D environments. However, this expansion brings legal challenges related to privacy and security, requiring a solid understanding to protect personal data.

2- The vital role of foreign direct investment in the digital economy

Foreign direct investment is vital for strengthening the digital economy (Bonner, 2022) by introducing capital and technology that drive innovation and growth. As reliance on digital solutions grows, attracting foreign investments is crucial for developing digital infrastructure and enhancing competitiveness. However, legal challenges related to digital identity can create uncertainty for investors, potentially deterring investments. Addressing these challenges is essential for fostering investor confidence and creating a stable investment environment.

3- The need for legal development that addresses digital identity issues in Metaverse

A comprehensive legal framework is urgently needed to address digital identity issues, ensuring user rights and personal data safety in interactive environments. (Creative Commons, 2016), Without appropriate laws, conflicts of interest and data breaches may arise, undermining trust in the digital space. The framework must also address identity verification, user privacy, and intellectual property rights. Strong legal protections will enhance confidence among users and investors, supporting sustainable growth in Metaverse and fostering innovation in the digital economy.

Research problem

What are the main legal challenges for digital identity in Metaverse?

- How do legal challenges affect foreign investors' confidence in Metaverse?
- What are the necessary mechanisms to protect digital identity and ensure privacy in Metaverse?
- How can these challenges impact attracting foreign direct investments to Metaverse?

Research Objective

This research aims to explore the legal challenges associated with digital identity, which include issues of privacy, security, and legal regulations governing the use of personal data in the digital space. By analyzing these challenges, we seek to understand how they impact individuals and businesses in an increasingly complex digital environment. The research analyzes the impact of digital identity on foreign direct investment, examining how related laws and policies can influence foreign investors' decisions, thereby creating a safer and more attractive investment environment. Through this analysis, we hope to provide valuable insights into how to promote foreign investments in light of current legal challenges

Previous studies and reports:

- 1- Ben Chester Cheong, "Avatars in Metaverse: Potential Legal Issues and Remedies," International Cyber security. The study emphasizes the importance of addressing the legal dimensions of Metaverse to ensure a safe and fair environment for users in light of continuous technical developments.
- 2- Safari Kasiyanto and Mustafa R. Kilinc, "The Legal Conundrums of Metaverse," The study stresses the importance of establishing clear legal frameworks to protect the rights of individuals and ensure the safe use of Metaverse technologies.
- 3- Maria KALYVAKI, "Navigating Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction," This study sheds light on the complex legal challenges faced by individuals and companies in the world of Metaverse, and emphasizes the necessity of clear legal frameworks to protect rights and ensure the safe use of this technology.
- 4- Faisal Fiaz et al., "Meta-SSI: A Framework for Personal Data Protection, Enhanced Cyber security and Privacy in Metaverse Virtual Reality Platforms." The study aims to explore how to create a digital environment that reflects the characteristics of the real world, with a focus on more stringent communication requirements, including security and data privacy.
- 5- Md. Rayhan Ahmed et al., "Block chain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey.". This study emphasizes the importance of developing innovative IDMS solutions based on block chain technology to enhance security and privacy in digital identity management.
- 6- Siwen Wang and Wei Wang, "A Review of the Application of Digital Identity in Metaverse," Security and Safety. This study highlights the challenges and opportunities associated with implementing digital identity in Metaverse, and emphasizes the importance of developing effective strategies to ensure privacy and security in this virtual space.

RESEARCH METHODOLOGY:

The descriptive analytical approach will be used through:

1. Review of literature and previous studies related to digital identity and legal challenges in Metaverse.
2. Analyze current laws and evaluate their effectiveness in facing new challenges
3. Analyze the relationship between the legal challenges of digital identity and the development of the digital economy.

Research plan: The research consists of four chapters divided as follows:

Chapter One: The main legal challenges of digital identity in Metaverse

Data protection and privacy

Jurisdiction European Union

Digital rights as part of human rights

Commitment to transparency

Chapter Two: US laws and digital identity protection in Metaverse:

The legal framework for data protection in the United States:

Egyptian laws and digital identity protection in Metaverse:

Chapter Three: The impact of legal challenges on foreign investors' confidence in Metaverse:

Investors use technology to improve their legal and administrative processes

Copyright violations in games

Trademark issues in Metaverse

Technological innovations in the field of virtual reality

Mechanisms for protecting digital identity and privacy

Spending on research and development

Chapter Four: The relationship between research and development and foreign direct investment are evident in several aspects

Increasing competitiveness

Developing human skills

Enhancing transparency and trust

Conclusion: It contains the most important results and recommendations.

Chapter One: The main legal challenges of digital identity in Metaverse

The concept of the "right to digital identity" has emerged as one of the basic rights of individuals. Digital identity and ownership of digital assets are closely intertwined in Metaverse, with each representing an essential element of users' digital experience. The right to digital identity refers to the ability of individuals to control their digital identity (Arcia et al., 2023) including the personal information and data collected about them. In Metaverse, digital identity is crucial for user interaction within the virtual environment, enabling the creation and exchange of digital assets. Ownership of these assets, such as non-fungible tokens (NFTs) and real estate, is tied to the legal rights individuals hold over the assets they create or engage with. Virtually, this relationship presents challenges, including:

Data protection and privacy

These are vital issues in Metaverse, as these concepts are closely intertwined with the right to digital identity. In this context, digital identity plays a pivotal role in how individuals interact (Latifzadeh & Mahdi, 2023), with the virtual environment, raising questions about how to protect personal information and ensure privacy. The right to a digital identity allows individuals to control their personal data, which enhances their ability to manage their identity in the digital space. However, this right faces significant challenges in Metaverse, where huge amounts of personal data are collected by various platforms. This data can include sensitive information, making it a target for breaches and hacks. In Metaverse, platforms ask to collect user data to improve the virtual experience. However, this raises concerns about how this data is used, and whether it is processed in

a privacy-respecting manner. (Di Pietro & Cresci, 2021), which threatens the privacy of individuals and leads to a loss of trust in the platforms. It is therefore essential that there is transparency about how data is collected and used. Users should receive clear information about what is collected and how it is used, as well as obtain their informed consent. There is a demand for a balance between security and privacy as security measures may necessitate collecting additional user data, potentially conflicting with individuals' privacy rights, which have evolved with technological advancements. Privacy in Metaverse is not merely a technical issue (Chen et al., 2022), but a social and legal one that necessitates a thorough understanding of the challenges individuals face in this digital space, requiring a re-evaluation of how to protect personal data. This is due to the huge amounts of data that are collected about users' behavior, including their interactions, interests, and even feelings. This unlimited collection of data raises significant concerns about how this information is used. Users also lack control over their personal data in many cases, and the data is used for commercial purposes. Without clear consent from individuals, which leads to privacy violations. With the increase in electronic attacks, (Zhao et al., 2023), individuals become more vulnerable to risks such as identity theft and fraud. These threats require new data protection strategies. For all of this, privacy in Metaverse goes beyond simply protecting personal information. It relates to individuals' ability to control their representation and interactions in virtual spaces. Current laws struggle to keep pace with rapid technological developments, as much existing legislation does not address the complexities of Metaverse, making individuals vulnerable to privacy violations. Therefore, the developed legal framework must include clear definitions of privacy in the context of Metaverse, including the rights of individuals to control their data. It must also enhance those rights effective protection mechanisms. Laws must include preventive guarantees. New standards such as encryption techniques to protect data from unauthorized use. New standards must also be adopted to protect that data are appropriate to the nature of interactions in Metaverse, such as using artificial intelligence techniques to analyze data securely. On the one hand, other: Companies must commit to providing clear information about how to collect and use data, which gives users the ability to make informed decisions. Legal development is completed by strengthening the rights of individuals to access, modify, and delete their data, which ensures that they have control over their personal information.

Jurisdiction

Geographic boundaries, raising important legal questions about who has jurisdiction in disputes related to digital identity and asset ownership. (Valente, 2024), this discussion addresses several key aspects:

In Metaverse, if a dispute arises over ownership of a digital asset or a breach of digital identity, it can be difficult to determine which legal regime should apply, especially if the parties involved are located in different countries. Current laws may not cover all aspects related to digital identity and ownership of digital assets, which calls for thinking about developing new international laws to solve the problem of multiple jurisdictions.

Even if jurisdiction is determined, implementing judicial rulings in Metaverse is a challenge (Jesse, 2024). It may be difficult to apply national laws to actions that occur in a virtual environment, requiring the development of new mechanisms to ensure enforcement of judgments. (Aurora Jillena Meliala & Akbar Kurnia Putra, 2024), Arbitration and mediation mechanisms may be an effective option for resolving disputes in Metaverse. These mechanisms can provide quick and flexible resolution of disputes, but they also require consensus between the parties on the laws to be applied. This facilitates dealing with legal disputes and ensures the protection of the rights of individuals across borders.

Digital rights as part of human rights

Protection of personal data and privacy is part of basic human rights. (Dr.Veerabhadraiah C & Bai, 2024)

This requires countries to commit to promoting these rights through effective legislation, reflecting the importance of protecting digital identity in the modern era.

Commitment to transparency

The new legal framework must include requirements for transparency and accountability, so that organizations are obligated to inform users about how their data is collected and used. This enhances individuals' rights to control their personal information. Concerns related to information security are increasing in light of the rapid developments witnessed in Metaverse, as cybercrime emerges as one of the most prominent challenges facing users. The chances of committing cybercrime (Bolaji David Oladokun et al., 2024), such as fraud, identity theft, and cyberbullying, increase. These criminal activities cross traditional boundaries, making it difficult to determine legal responsibility and enforce laws effectively. Therefore, it is necessary to develop new legal strategies to confront these challenges. This requires coordinating efforts between countries to exchange information and experiences, and developing joint legal mechanisms to combat these crimes. (Cao, 2024), this cooperation can contribute to enhancing information security and protecting users. To propose developing current laws to keep pace with rapid advancements in Metaverse, it is essential first to review the existing laws in Egypt and the United States related to digital identity. This monitoring aims to clarify the shortcomings that these laws suffer from in the face of emerging challenges. Egypt and the United States are two countries with great influence in the fields of technology and innovation. The United States, being home to many major technology companies, plays a leading role in the development of Metaverse. While Egypt seeks, through its digital strategies, to enhance technological innovation and provide an appropriate legal environment to attract investments. Analysis of current laws will enable us to identify points that need to be amended or updated, which will facilitate the formulation of new legislation that suits the nature of Metaverse and its unique challenges.

Chapter Two: US laws and digital identity protection in Metaverse

A legal analysis

The United States is considered a leading country in the field of technological innovation, which places protecting digital identity and ensuring privacy in Metaverse at the heart of contemporary legal debates. This analysis examines the legal framework governing data protection in the United States, focusing on the challenges facing this framework and its impact on attracting foreign investment.

The legal framework for data protection in the United States

The United States lacks a comprehensive law regulating personal data protection at the federal level, complicating the legal landscape. Rather than having uniform legislation, the United States relies on a patchwork of federal and state laws that address different aspects of data protection. The most prominent of these laws are:

The Children's Online Privacy Protection Act (COPPA) (Federal Trade Commission, 2013) is a US law aimed at protecting the data of children under the age of 13, and requires websites to obtain parental consent before collecting any personal information. (Adrija Guhathakurta, 2024), (Benjamin et al., 2016), Despite the importance of this law, it faces several limitations in meeting the challenges of metaphysics.

Limited scope of application: (Children's Online Privacy Act (COPPA) - an Overview, n.d.), COPPA only focuses on children under 13, meaning that older children, who may also be vulnerable in Metaverse environments, do not have the same level of protection. This leaves a gap in legal protection for children aged 13 to 18, who may be exposed to risks such as cyberbullying or exploitation.

Challenges in parental consent: The law requires parental consent before information is collected, but in Metaverse environments, it can be difficult to ensure that this consent has been properly

obtained. Parents may not have the ability to monitor all of their children's activities in these virtual environments, which increases the risk that children will be exposed to inappropriate content or other risks. Not adapting to modern technology: Enacted in 1998 COPPA, (Fruhlinger, 2021), does not reflect the rapid changes in technology and ways of interacting online. Metaverse represents an interactive, three-dimensional environment that requires new strategies to protect children, which current law may not adequately cover.

Difficulty in applying laws across borders

Many platforms in Metaverse operate globally, making it difficult to enforce local laws like COPPA. Children may interact with content or platforms outside the scope of US law, which limits the effectiveness of the protections it provides. While COPPA represents an important step toward protecting children's online privacy, it faces significant challenges in the face of Metaverse (Krishnaa, 2023). It is essential to update laws to meet the protection needs of modern digital environments, and to ensure the safety of all children, regardless of their age.

Health Information Protection Act (HIPAA)

Regulates how personal health information is handled, ensuring that patients' privacy is protected. Although it is a role model in protecting sensitive data, it has significant limitations in meeting the challenges of Metaverse.

Not adapting to virtual environments

HIPAA was originally designed to handle health information in traditional contexts, such as hospitals and clinics. (Lutkevich, 2020), with the emergence of Metaverse, where it is assumed that health information can be exchanged in interactive virtual environments, it becomes difficult to apply the same standards. Metaverse requires new strategies to protect health data that may be collected or used in these environments.

Difficulty in determining responsibility

In Metaverse, multiple entities (such as developers, service providers, and users) may be involved in the collection and use of health information. (Mehdi Letafati & Safa Otoum, 2023), this complexity makes it difficult to determine who is responsible for data protection, which can lead to gaps in HIPAA compliance.

Challenges in data protection (HIPAA) requires specific security measures to protect health information, but in Metaverse environments, these measures may be insufficient. Cyber threats such as hacks and malware may

Be more common in virtual spaces, requiring advanced security strategies beyond what HIPAA mandates.

Lack of a comprehensive legal framework

HIPAA primarily focuses on health information, (UC Berkeley, 2019), but does not address other issues that may be relevant in Metaverse, such as intellectual property rights or personal data protection in general. This lack of comprehensiveness can lead to inadequate protection of sensitive data.

State laws

Many states, such as California, have passed data protection laws, the California Consumer Privacy Act (CCPA), (State of California Department of Justice, 2024), that give consumers additional rights over their personal data, including the right to know how their data is used and sold. The California Consumer Privacy Act (CCPA) is a law intended to give consumers additional rights over their personal data, including the right to know how their data is used and sold. Although this law

represents an important step toward protecting privacy, it faces significant limitations in the face of Metaverse challenges.

Limited scope of application

The CCPA only applies to companies that handle California residents' data, (Comprehensive FAQs on the CCPA, 2018), which means that companies that operate in Metaverse but are not based in California may not be required to comply with the law. This creates a gap in protection, as consumers can be exposed to risks from companies that are not subject to the law.

Challenges in identifying

In Metaverse environments, it can be difficult to accurately identify users, making it difficult to enforce consumer rights under the CCPA. For example, it can be difficult for users to know who is collecting their data and how it is being used, especially in complex virtual environments.

Insufficient protection for sensitive data

While the CCPA focuses on personal data, it may not adequately address sensitive data that may be collected in Metaverse, such as health information or biometric data. This lack of comprehensiveness can result in consumers (UC Berkeley, 2019), being exposed to greater risks.

Difficulty enforcing laws across borders

Many platforms in Metaverse operate globally, making it difficult to enforce local laws like the CCPA. Users may interact with content or platforms outside the scope of the law, limiting the effectiveness of the protection it provides. Legal liability in Metaverse is a major challenge in the event of violations or crimes. It is difficult to determine the responsible party, whether it is the companies that manage the platforms or the users themselves. This legal ambiguity can lead to difficulties in applying justice. Comment on the legal challenges facing American laws in the face of Metaverse, although a body of laws exists, the United States faces several challenges in applying them effectively in the context of Metaverse

The lack of a uniform federal data protection law

Makes it difficult for companies to comply with diverse requirements across states, leading to legal uncertainty (greggwirth, 2022), Differences in laws between states may create legal complexities for companies operating on a national level, affecting their ability to innovate and increasing compliance costs.

Enforcement of the laws requires effective mechanisms to monitor compliance, which calls for the establishment of regulatory bodies capable of imposing penalties on violators. This requires significant investments in legal and regulatory infrastructure.

Egyptian laws and digital identity protection in Metaverse:

A legal analysis: In light of the rapid technological developments that the world is witnessing, Metaverse has become a new platform that requires special attention from a legal standpoint, especially with regard to protecting the digital identity and privacy of users. In this context, we need to explore the extent to which Egyptian laws accommodate these challenges and how they may affect the attraction of foreign direct investment.

Legal framework for data protection in Egypt Egypt's Personal Data Protection Law (Law No. 151 of 2020) represents an important step towards regulating how collect (NATLEX - Egypt - Law 151/2020 on the Protection of Personal Data., 2020), use and protect personal data. However, this law faces significant challenges in the context of protecting digital identity in Metaverse, a virtual world characterized by complex social and economic interaction.

Main challenges

The complex nature of Metaverse

Metaverse is an interactive digital environment that involves multidimensional interactions between users, making it difficult to determine how data is collected and used. In this environment, digital identities can become intertwined, making it difficult to apply the protection standards set by law. For example, individuals may use multiple identities or virtual personas, (Chawki et al., 2024), making it difficult to track personal data associated with each identity.

Difficulty in obtaining approval:

The law requires individuals' consent to be obtained before their data is collected, (LI & white, 2023) but in Metaverse, it can be difficult to ensure that this consent has been properly obtained. Users may not be fully aware of how their data is used, or they may agree to the terms of use without fully understanding the consequences. This can lead to unauthorized data being collected or used in unexpected ways.

Cyber Threats

Cyber threats are increasing in Metaverse, (Chaudhari et al., 2024), where personal data can be hacked or stolen. The Personal Data Protection Law may not include sufficient measures to confront these threats, which puts individuals' digital identity at risk. In a Metaverse environment, cyber-attacks can be more complex, requiring advanced security strategies.

Lack of effective implementation mechanisms

Although there are legal provisions, implementing them in Metaverse can be a challenge. Stakeholders may lack the resources or expertise to monitor compliance with the law in complex digital environments. This lack of enforcement capacity can lead to non-compliance by companies or individuals.

Non-inclusiveness

Personal data protection law may not adequately address issues such as biometric data or other sensitive information (Garg, 2024), that may be collected in Metaverse. This lack of comprehensiveness can result in individuals being exposed to greater risks, as sensitive data may be collected without adequate protection. While the Personal Data Protection Act represents an important step towards protecting digital identity, it faces significant challenges in the face of Metaverse. . The challenges posed by virtual reality environments require the development of additional legislation commensurate with the nature of this technology, such as regulating the use of artificial intelligence techniques and big data analysis. This calls for updating laws and developing new legal frameworks that match technological innovations to ensure effective protection of personal data in modern digital environments. This requires cooperation between governments, companies, and civil society to ensure the safety of individuals' digital identities in this evolving virtual world.

Comment on the legal challenges faced by Egyptian laws in face of Metaverse:

Despite the existence of a legal framework, Egypt faces several challenges in implementing it effectively. The most prominent of these challenges are: Current Egyptian laws do not contain clear legal texts related to Metaverse. This absence makes it difficult to organize the economic and social activities that occur in this virtual environment. For example, there are no laws governing intellectual property or user rights in Metaverse, leading to issues related to fraud or invasion of privacy. With the increase in commercial activities in Metaverse, there is an urgent need to develop laws regulating e-commerce. Current laws may not cover all aspects of virtual commerce, (Yadav, 2024), leaving loopholes that can be exploited by fraudsters. Determining legal liability in Metaverse is a major challenge. If abuses or crimes occur, it is difficult to determine who is responsible, whether it is the

companies running the platforms or the users themselves. This legal ambiguity can lead to difficulties in administering justice. There is an urgent need to educate companies and users about their rights and duties under data protection law. It also requires training legal and administrative personnel on how to comply with legal requirements. Law enforcement also requires effective mechanisms to monitor compliance, which requires imposing penalties on violators. Current laws may not sufficiently protect individuals or organizations in virtual environments, necessitating a reevaluation of the legal framework for better effectiveness and relevance. Implications of digital identity protection on foreign direct investment Protecting digital identity and ensuring privacy are key factors affecting the attraction of foreign investments. Investors are looking for safe and stable environments, where their data and personal information are protected. If Egypt can strengthen its legal framework and implement it effectively, this will enhance investor confidence and attract more investments in the technology and Metaverse sector.

Chapter Three: The impact of legal challenges on foreign investors' confidence in Metaverse

The legal challenges associated with Metaverse (Saridakis et al., 2024), are critical factors affecting foreign investors' confidence in this emerging field. The impact of these challenges is evident in several key aspects: When multiple legal systems exist, (Zou & Hu, 2024), investors face uncertainty about which laws they must adhere to. This ambiguity can cause investors to be hesitant to make investment decisions, as they fear exposure to unexpected legal risks. Lack of clarity in laws may discourage investors from entering new markets, which negatively impacts the flow of investments. (Matytsin et al., 2024), the multiplicity of legal systems requires investors to deal with a variety of laws and regulations, which increases the complexity of the compliance process. This complexity can lead to increased legal and administrative costs, making investment in those markets less attractive. Investors prefer legal environments that provide clarity and ease of compliance.

In a diverse legal environment, investors may be reluctant to enter into partnerships with local or international companies. Partnerships require a high level of trust, and when laws are unclear or inconsistent, this can lead to a decline in trust between the parties involved. This decline can hinder cooperation and reduce growth opportunities. The multiplicity of legal systems may hinder innovation, as investors may avoid investing money in new or innovative projects due to potential legal risks. (Xu et al., 2024), When investors feel that the legal environment is unfavorable, they may prefer to keep their money in more stable markets. In a globalized world, countries seek to attract foreign investments by offering stable and attractive legal environments. If a country suffers from multiple legal systems, this may negatively affect its competitiveness compared to other countries that provide clearer and more stable legal environments. However, there are several strategies these investors adapt to deal with this situation: Investors can conduct comprehensive studies on the laws and regulations in force in the countries in which they intend to invest. (Ahmet Faruk Aysan et al., 2024) This includes analyzing legal frameworks related to Metaverse, such as data protection laws, intellectual property rights, and regulatory compliance. This research helps them understand potential risks and identify opportunities. Investors rely on legal advisors and local experts to better understand the legal environment. These experts can provide valuable insights on how to navigate complex legal systems and advise on best practices for compliance. To reduce the risks associated with legal uncertainty, investors may diversify their investment portfolio across several projects or geographic regions. This diversification helps reduce the negative impact of any legal changes that may occur in a particular area.

Some investors participate in public discussions about developing laws and regulations related to Metaverse. By engaging in these dialogues, they can influence future policies and ensure that laws are appropriate to support innovation and investment.

Investors develop comprehensive risk management strategies, (Egliston & Carter, 2022), including assessing potential legal risks and developing plans to deal with them. These strategies help them respond quickly to any legal changes that may affect their investments. Investors use technology to

improve their legal and administrative processes. Legal analysis tools and specialized software can help track legal changes and provide accurate reporting, making it easier to make informed decisions. Facing uncertainty about laws and regulations in Metaverse requires foreign investors to adopt multidimensional strategies. Through careful research, collaboration with experts, and diversification of investments, they can reduce risks and enhance their confidence in this promising field. Metaverse operates as a global space that transcends national borders, creating challenges related to law enforcement. Investors may have difficulty understanding which legal regime they should follow, which increases the complexity of the investment process and reduces the attractiveness of the market, intellectual property protection is one of the main issues of concern to investors. In a Metaverse environment, where content can be easily copied and distributed, it becomes necessary to have a strong legal framework to protect intellectual property rights. The lack of such a framework may lead to a loss of confidence in investing in innovative projects. The lack of a strong legal framework to protect intellectual property in Metaverse has noticeably worried investors, and there are several actual examples that illustrate this effect:

The “Roblox” issue and intellectual property rights: In 2021, the “Roblox” platform (Ghaffar, 2024)

Faced legal challenges related to intellectual property, as it was accused of facilitating violations of intellectual property rights by its users. This has investors concerned about how to protect their innovations and ideas in a legally unprotected environment. Investors were afraid that the lack of adequate protection could lead to them losing their rights to the content they develop. (Mezei & Chawla Aror, 2019)

Copyright violations in games: In recent years, gaming industry has witnessed many cases of copyright violation, where popular games were cloned without permission from the original developers. For example, the game “Fortnite” was illegally cloned on several platforms, (Pedraça, 2024), causing investors to worry about their investments in developing new games. This type of violation creates an unsafe environment for investors, as they fear that their efforts may be in vain due to the lack of effective legal protection.

Trademark issues in Metaverse: In 2022, trademark issues emerged in Metaverse, (Bonadio & Mohnot, 2024), where well-known brands were used in virtual environments without permission. (Jaloliddin Abdusatarov & Muhammad Ali Turdialiev, 2024), this matter raised concerns among major companies, such as Nike and Adidas, which began taking legal steps to protect their trademarks. Investors in these companies were concerned that the lack of adequate protection might affect the value of the brand and reduce investment attractiveness.

Technological innovations in the field of virtual reality:

New technologies related to user experiences have been developed. (Raji et al., 2024), However, the lack of strong legal protection has made some companies reluctant to invest in these innovations. For example, there have been concerns that companies might be hacked or have their technology copied, making them avoid investing money in developing new ideas. There are lawsuits related to digital identity and privacy, including the issue of Facebook, and user data Lawsuits, have been filed against Facebook for privacy violations, related to data collection, and use. In 2019, a class action lawsuit was filed against the company for leaking user data, and using it for targeted advertising, without clear consent from users. This case sparked widespread debate, about how to protect personal data on social platforms. This case greatly impacted Facebook's reputation, as it raised awareness, about digital privacy issues, and the importance of protecting personal data. It has also prompted, many users to re-evaluate their use of social platforms. Following this case, many countries began to review their data protection laws, leading to strengthening laws, such as the General Data Protection Regulation (GDPR) in the European Union. (Bakare et al., 2024), as companies recognize the importance of user data protection and transparency, the Facebook data issue marks a pivotal moment, in how businesses handle personal data. This case highlighted the importance of digital privacy, and influenced legal, and business

Policies, around the world, making it one of the most prominent cases of the modern technology era.

Cambridge Analytical case: This case relates to the use of Cambridge Analytical, (Anna-Verena Nosthoff & Maschewski, 2023), which was founded in 2013 and was engaged in data analysis and political consulting. The company used advanced technologies to collect and analyze data from Facebook users, obtaining personal information from more than 87 million users without their permission. This was done through apps that looked like academic research tools, but were actually collecting data from millions of Facebook users without their permission. Claims have been brought against Facebook for not adequately protecting user data, leading to legal investigations in the US and UK. This case has significantly affected policies related to data protection. It has prompted governments to review privacy laws, leading to strengthening laws such as the General Data Protection Regulation (GDPR) in the European Union. It also increased public awareness about the importance of protecting personal data and user rights. The Cambridge Analytical case represents a turning point in how companies handle personal data, and has significantly impacted privacy policies around the world. This case highlighted the importance of data protection and the rights of individuals in the digital space, making it one of the most prominent cases of the modern technology era.

The case of “Apple” and “Fortnite” case is a prominent legal dispute between Epic Games, the developer of the game “Fortnite”, and Apple, over App Store policies and market monopoly. (Cheremnykh, 2024), this case began in 2020, when Epic Games introduced its own payment system into Fortnite, violating Apple's App Store policies. Epic Games, the developer of Fortnite, filed a lawsuit against Apple over its restrictions on the App Store. The issue concerns how users' digital identity and rights to access content are managed. This case highlights the legal challenges related to controlling digital identity in gaming environments. In September 2021, the court issued a mixed ruling. The court ruled that Apple cannot prevent developers from directing users to third-party payment methods, a victory for Epic. However, the court did not find that Apple had an illegal monopoly on the market, which was a partial victory for Apple. This issue has greatly affected how companies handle in-app payment policies. After the ruling, Apple began amending some of its policies, allowing developers to direct users to third-party payment options, but still reserves the right to charge a commission on sales made through the App Store. The case of “Apple” and “Fortnite” represents a major conflict over payment policies and market monopoly in the world of applications. This case highlighted the challenges facing developers in dealing with major technology platforms, and influenced how the application market is regulated in the future. Lawsuits against virtual reality applications Cases have been filed against some VR apps for illegally collecting user data. For example, some apps have been accused of collecting sensitive information such as geolocation and usage behaviors without adequately informing users.

Horizon Worlds Privacy Lawsuits (Meta's Horizon Worlds app) has faced criticism and lawsuits over privacy issues. In 2021, there were reported cases of users experiencing harassment or inappropriate behavior while using the app. As a result, claims have been filed against Meta for failing to provide a safe environment for users, raising questions about how privacy and safety of users are protected in VR environments. Legal cases clearly show that lack of intellectual property protection can lead to a loss of confidence in investing in innovative projects. Providing a strong legal framework to protect intellectual property is vital to attract investment and foster innovation, especially in evolving digital environments such as Metaverse. Despite the importance of legal regulation, when discussing the regulation of an advanced digital environment such as Metaverse, it is necessary to integrate technical regulation with the legal framework and privacy policies. Therefore, it is important to review the protection mechanisms that have proven relatively successful as a form of regulation of the digital environment. Strengthening these Technical mechanisms not only contribute to protecting innovations, but also enhance investor confidence in the digital business environment, which contributes to driving innovation and economic growth.

Mechanisms for protecting digital identity and privacy

Encryption

It is one of the basic tools for protecting data. By encrypting the information exchanged between users, the confidentiality of data can be guaranteed and protected from hacking. (Binhammad et al., 2024). This enhances users' trust in virtual platforms.

Access Control

Allows users to decide who can see their information and interact with them. Through privacy settings, users can customize their experience to suit their needs, enhancing their sense of security.

Transparency in data collection

It plays an important role in building trust. Companies need to be clear about how they collect and use data, which helps users understand how their information is protected. (Tekla Berozashvili, 2024).

Strong privacy policies

It is essential to ensure data protection. These policies must be consistent with local and international laws, and explain how personal data will be handled. Protecting digital identity and ensuring privacy are among the basic factors that affect attracting foreign direct investment. When there are strong data protection mechanisms, it enhances investors' confidence in digital platforms. Investors tend to choose secure environments where their data and personal information are protected. Moreover, having strong privacy protection policies could attract major technology companies to invest in developing new technologies in Metaverse. Reducing the legal risks resulting from privacy violations also enhances the attractiveness of investment, as it reduces the possibility of exposure to lawsuits. Markets that place privacy protection at the top of their priorities enjoy a better reputation internationally, which contributes to an increase in foreign direct investment. The legal challenges associated with Metaverse play a crucial role in shaping foreign investor confidence. By addressing these challenges and developing clear and effective legal frameworks, a safer and more attractive investment environment can be promoted, which contributes to attracting more investments to this promising field. Among these treatments is spending on research and development to reach the best legal and economic reforms.

Spending on research and development (R&D)

It represents one of the basic pillars that support innovation and economic growth in any country. (Ugur Korkut Pata et al., 2024), this type of spending is considered a long-term investment, as it contributes to the development of new technologies and the improvement of products and services, which enhances the competitiveness of countries in global markets. The relationship between R&D spending and digital identity in Metaverse is complementary. By investing in innovation, security can be improved, user experience enhanced, and richer social interactions developed. In an increasingly digital world, research and development is key to ensuring that digital identity properly reflects individuals and meets their needs in virtual environments.

Chapter Four: The relationship between research, development and foreign direct investment

Improving the investment environment

Countries that invest in research and development create a favorable business environment, as they provide modern technologies and innovations that facilitate production and distribution processes. This makes it an attractive destination for foreign investors seeking high returns.

Increasing competitiveness

Companies that focus on research and development have a competitive advantage, as they can provide innovative products and services that better meet market needs. This innovation attracts foreign investment, as investors seek to take advantage of these advantages.

Developing human skills

Spending on research and development enhances the skills of the workforce, which leads to improving the quality of products, and services. A well-trained workforce is a major attraction, for foreign investments, as it guarantees investors the presence of highly qualified employees.

Enhancing transparency and trust

Applying strict international accounting standards in countries that invest in research and development enhances transparency and credibility. This increases the confidence of foreign investors, making it easier to attract investments. Legal challenges in Metaverse significantly impact foreign investor confidence. Uncertainty surrounding laws and regulations can deter foreign investment, adversely affecting economic growth and innovation. This analysis focuses on foreign direct investment flows in the USA and Egypt from 2010 to 2022, examining their effects on GDP and research and development spending. Data indicate a noticeable increase in foreign investments in both countries, which reflects economic reform efforts and the trend towards innovation and development.

Gross domestic product EGYPT Billion dollars	Spending on research and development of GDP EGYPT Billion dollars	Foreign direct investment flows EGYPT billion dollars	USA GDP Trillion dollars	Percentage of spending on research and development as a percentage of USA's GDP Billion dollars	USA foreign direct investment flows Billion dollars	Statement Year
218.98	0.43	6.39	15.05	2.71	264.04	2010
235.99	0.53	0.483	15.60	2.74	263.50	2011
279.12	0.51	2.80	16.25	2.67	250.34	2012
288.43	0.64	4.19	16.88	2.70	288.13	2013
305.60	0.64	4.61	17.61	2.72	251.86	2014
329.37	0.72	6.93	18.30	2.79	511.43	2015
332.44	0.71	8.11	18.80	2.85	474.39	2016
248.36	0.64	7.41	19.61	2.90	380.82	2017
262.59	0.69	8.14	20.66	3.01	214.72	2018
318.68	0.80	9.01	21.52	3.17	315.98	2019
383.82	0.92	5.85	21.32	3.47	137.07	2020
424.67	0.91	5.12	23.59	3.46	475.81	2021
476.75	1.02	11.40	25.74	3.45	408.98	2022

Source: World Bank database <https://databank.worldbank.org/>

The table indicates that foreign direct investment flows in the United States increased from approximately \$264 billion to \$409 billion between 2010 and 2022, representing a 55% rise. The peak occurred in 2015, with flows reaching about \$511 billion. While the lowest value of these flows was recorded in 2020, amounting to about \$137 billion, as a result of the negative repercussions of the Corona pandemic. The epidemic had negative effects on the flow of foreign investments to all regions of the world, and the epidemic even contributed to increasing the economic gap between developed and developing countries (UN.ESCAP, 2021)

The percentage of spending on research and development as a percentage of GDP has also increased steadily, rising from 2.71% to 3.45% during the same period, which indicates the United States' keenness to pay attention to spending on research and development. Rather, the average growth in spending on research and development recorded higher rates than the gross domestic product, reaching 2.7% and 2.2%, respectively, during the period (2010-2017), and the United States accounted for about 25% of the total global research and development (Borouh, 2020). The gross domestic product also rose steadily, rising from \$15.05 to \$25.74 trillion, an increase estimated at about 71% during the same period. The lowest value of the gross domestic product was recorded in 2017, when it amounted to about \$248 trillion. This is a result of the financial crisis, which had a negative impact on the components of the gross domestic product, as exports decreased by about 14% and investment decreased by about 11% during the financial crisis (Inekwe & Valenzuela, 2018). However, the strength of the American economy enabled it to overcome this crisis and returned to rising from about 263 to 477 trillion dollars during the period 2019-2022). The table also shows an increase in foreign direct investment flows from 6.39 to 11.40 billion dollars during Egypt, an increase estimated at about 78% during the same period. The lowest value of these flows was recorded in 2011, when it amounted to less than half a billion dollars, as a result of the political repercussions of the January 25, 2011 revolution. While the highest value of these flows was recorded in 2022, amounting to about \$11.4 billion, the state's efforts in economic reform have contributed to attracting more foreign direct investment. Which contributed to advancing the economic development process, by attracting and developing technology, transferring knowledge, improving productivity, increasing competitiveness, and then increasing exports (Ghorab 2022). The percentage of spending on research and development of the gross domestic product in Egypt also increased from 0.41% to 1.02% during the same period, which indicates the Egyptian government's interest in this sector, especially since 2019, and especially since the beginning of the Corona pandemic, and the study (Attala & Zaki, (2023) indicates that there is a complementary and unidirectional relationship between spending on research and development on the one hand, the number of researchers per million citizens, and patents on the other hand, especially in the agricultural field,

The table shows that GDP increased from \$218.98 billion to \$476.75 billion during the same period, a rise of about 118%. However, GDP declined from \$332 billion to \$262 billion in 2016 and 2017 due to reduced capital accumulation. As a result of the decrease in foreign direct investment, in addition to the decrease in the savings rate and the increase in the population growth rate (Kamal, A. L. M., & AboElsoud, M. E. (2023)

Data indicated that increased spending on research and development reflects governments' commitment to innovation and helps develop technical solutions that increase identity security. Improving digital identity also facilitates commercial transactions and enhances competitiveness, which contributes to increasing foreign direct investment flows. In conclusion, research, and development in digital identity is essential for achieving sustainable economic development.

CONCLUSION AND RECOMMENDATIONS:

The research examined the impact of laws related to digital identity, and data protection in Metaverse on innovation, and foreign direct investment. It emphasizes that clear legal frameworks foster innovation by providing a safe environment for developers, and they also attract foreign direct investment by offering strong legal protection. However, strict regulations may pose challenges that may lead to innovation projects being postponed or cancelled. The importance of legal transparency stands out as an attractive factor for investors, as it helps them make informed decisions. Also, these laws require companies to develop innovative solutions to adapt to them. Overall, laws can enhance the attractiveness of countries in this growing sector if a balance is struck between stimulating innovation and legal compliance.

The following are the results and recommendations of the research: To address the legal challenges related to digital identity in Metaverse and enhance the market's attractiveness for foreign direct investment in Egypt, the following steps can be taken:

The Egyptian government must develop a legal framework that addresses all aspects of digital identity, including data protection and user rights, while establishing clear compliance mechanisms that make it easier for companies to understand legal requirements.

Laws should be flexible and adaptable to rapid technological developments. This can be achieved by periodically reviewing and updating the laws based on new innovations in Metaverse.

Encouraging partnerships between the government and private companies to develop effective policies.

Joint committees could be established that include representatives from both sectors to discuss legal challenges and provide innovative solutions.

The government can provide financial or tax incentives to companies that invest in developing new technologies to protect data and comply with laws, which encourages innovation.

Developing awareness programs for investors and companies about laws related to digital identity, including workshops and training courses to enhance legal awareness and reduce compliance concerns. Laws must be clear and easy to understand, with legal information published in a simplified manner, making it easier for companies and investors to understand the legal requirements.

Periodic assessments of the legal impact of current laws on innovation and investment must be conducted, to ensure that they do not negatively impact economic growth. Encouraging research and development in the field of digital identity by providing grants or financial support to academic institutions and startup companies, which helps in developing innovative solutions that enhance data protection.

ACKNOWLEDGEMENTS

The authors gratefully acknowledges the approval and the support of this research study by Grant No.NBU-FFR-2024-2539-02 from Northern Border University, Arar, KSA

REFERENCES

- Adrija Guhathakurta. (2024). Data Privacy, Data Protection and User Rights in the World of Metaverse: Addressing the Legal Challenges in the EU, the US and India. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.4994031>
- Ahmed, Md. R., Islam, A. K. M. M., Shatabda, S., & Islam, S. (2022). Block chain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey. IEEE Access, 10(VOLUME 10, 2022), 113436–113481. <https://doi.org/10.1109/access.2022.3216643>
- Ahmet Faruk Aysan, Batten, J., Giray Gozgor, Rabeh Khalfaoui, & Zhamal Nanaeva. (2024). Metaverse and Financial Markets: A Quantile-Time-Frequency Connectedness Analysis. Research in International Business and Finance, 72(72), 102527–102527. <https://doi.org/10.1016/j.ribaf.2024.102527>
- Anna-Verena Nosthoff, & Maschewski, F. (2023). The platform economy's infrastructural transformation of the public sphere: Facebook and Cambridge Analytical revisited. Philosophy & Social Criticism, 50(1). <https://doi.org/10.1177/01914537231203536>
- Arcia, P., Fuentealba, A., César Retamal, Lara, S., Mardones, E., Mascaró, T., Fuentes, P., & Centeno, M. (2023). ETHICAL ISSUES OF DIGITAL IDENTITY IN METAVERSE. ICERI Proceedings, 1, 2434–2439. <https://doi.org/10.21125/iceri.2023.0665>

- Attala, M. A. E., & Mohamed Zaki, E. (2023). The Role of Scientific Research and Government Expenditure in Achieving Sustainable Development in the Agriculture. *Alexandria Science Exchange Journal*, 44(2), 121-134.
- Aurora Jillena Meliala, & Akbar Kurnia Putra. (2024). Tacit Choice of Law in Metaverse: What Law Applies? *Uti Possidetis Journal of International Law*, 5(1), 1–37. <https://doi.org/10.22437/up.v5i1.28587>
- Bakare, S., Adekunle, N., None Chidiogo Uzoamaka Akpuokwe, & None Nkechi Emmanuella Eneh. (2024). DATA PRIVACY LAWS AND COMPLIANCE: A COMPARATIVE REVIEW OF THE EU GDPR AND USA REGULATIONS. *Computer Science & IT Research Journal*, 5(3), 528–543. <https://doi.org/10.51594/csitrj.v5i3.859>
- Benjamin, B. M., Brigagliano, J. M., & Andres, T. (2016, July 29). Complying with the Children’s Online Privacy Protection Rule; FTC’s Proposed Updates. *Ktslaw.com*. <https://ktslaw.com/en/Insights/Alert/2024/1/Complying-with-the-Childrens-Online-Privacy-Protection-Rule>
- Binhammad, M., Alqaydi, S., Othman, A., & Abuljadayel, L. H. (2024). The Role of AI in Cyber Security: Safeguarding Digital Identity. *Journal of Information Security*, 15(02), 245–278. <https://doi.org/10.4236/jis.2024.152015>
- Bolaji David Oladokun, Rexwhite Tega Enakrire, Ukubeyinje, S. E., Oyighan Diseiye, & Ajani, Y. A. (2024). Cyber security behavior in Metaverse: opportunities, challenges and future trends for libraries. *Library Hi Tech News*, Library Hi Tech News (<https://doi.org/10.1108/LHTN-09-2024-0159>). <https://doi.org/10.1108/LHTN-09-2024-0159>
- Bonadio, E., & Mohnot, R. (2024, April). Trademarks and Image Rights in Metaverse. *Ssrn.com*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4799000
- Bonner, M. (2022, December 5). Why we need to regulate digital identity in Metaverse. *World Economic Forum*. <https://www.weforum.org/stories/2022/12/digital-identity-Metaverse-why-we-need-to-regulate-it-and-how/>
- Borouh, M. (2020). Research and Development: US Trends and International Comparisons. *Science and Engineering Indicators 2020*. NSB-2020-3. National Science Foundation.
- Cao, R. (2024). Personal Information Protection Issues in Metaverse Perspective. *Advances in Economics and Management Research*, 10(1), 19–19. <https://doi.org/10.56028/aemr.10.1.19.2024>
- Chaudhari, A., Mali, Y. K., Kulkarni, A., Jain, D., Sharma, L., Mahajan, K., Kazi, F., Kar, P., & Aman Bhogle. (2024). Cyber Security Challenges in Social Metaverse and Mitigation Techniques. 2024 MIT Art, Design and Technology School of Computing International Conference (MITADTSociCon), 8(<https://doi.org/10.1109/MITADTSociCon60330.2024.10575295>), 1–7. <https://doi.org/10.1109/mitadtsocicon60330.2024.10575295>
- Chawki, M., Basu, S., & Choi, K.-S. (2024). Redefining Boundaries in Metaverse: Navigating the Challenges of Virtual Harm and User Safety. *Laws*, 13(3), 33. <https://doi.org/10.3390/laws13030033>
- Chen, Z., Wu, J., Gan, W., & Qi, Z. (2022). Metaverse Security and Privacy: An Overview. 2022 IEEE International Conference on Big Data (Big Data), 33.
- Cheng, X., Zhang, S., Fu, S., Liu, W., Guan, C., Mou, J., Ye, Q., & Huang, C. (2022). Exploring Metaverse in the digital economy: an overview and research framework. *Journal of Electronic Business & Digital Economics*, 1(1/2), 206–224. <https://doi.org/10.1108/jebde-09-2022-0036>
- Cheong, B. C. (2022). Avatars in Metaverse: potential legal issues and remedies. *International Cyber security Law Review*, 3(Volume 3, pages 467–494, (2022). <https://doi.org/10.1365/s43439-022-00056-9>
- Cheremnykh, P. (2024). Gaming Metaverse User Experience Analysis and Insights from Fortnite Bachelor of Culture and Arts Degree Programmer in Design Thesis. https://www.theseus.fi/bitstream/handle/10024/850495/Cheremnykh_Pedcharat.pdf?sequence=2

- Children's Online Privacy Act (COPPA) - An Overview. (n.d.). Consent Management Platform (CMP) Usercentrics. <https://usercentrics.com/knowledge-hub/childrens-online-protection-act-coppa/> Comprehensive FAQs on the CCPA. (2018). Fisher Phillips. <https://www.fisherphillips.com/en/news-insights/comprehensive-faqs-on-the-ccpa.html>
- Creative Commons. (2016). Creative Commons — Attribution 4.0 International — CC BY 4.0. Creativecommons.org; Creative Commons. <https://creativecommons.org/licenses/by/4.0/>
- Di Pietro, R., & Cresci, S. (2021). Metaverse: Security and Privacy Issues. 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 281–288. <https://doi.org/10.1109/tpsisa52974.2021.00032>
- Dr.Veerabhadraiah C, & Bai, G. (2024). Human Rights in the Digital Age: Balancing Privacy, Freedom, and Security. *International Journal of Commerce, Management, Leadership, and Law*, 1(1), 77–89. <https://ijcmll.com/1/article/view/10>
- Egliston, B., & Carter, M. (2022). “Metaverse and how we'll build it”: The political economy of Meta's Reality Labs. *New Media & Society*, 0(0), 146144482211197. <https://doi.org/10.1177/14614448221119785>
- Falchuk, B., Loeb, S., & Neff, R. (2018, June 4). The Social Metaverse: Battle for Privacy. *Ieeexplore.ieee.org*. <https://ieeexplore.ieee.org/abstract/document/8371577>
- Federal Trade Commission. (2013, July 25). Children's Online Privacy Protection Rule (“COPPA”). Federal Trade Commission; Federal Trade Commission. <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>
- Fiaz, F., Sajjad, S. M., Iqbal, Z., Yousaf, M., & Muhammad, Z. (2024). MetaSSI: A Framework for Personal Data Protection, Enhanced Cyber security and Privacy in Metaverse Virtual Reality Platforms. *Future Internet*, 16(5), 176. <https://doi.org/10.3390/fi16050176>
- Fruhlinger, J. (2021, February 8). COPPA explained: How this law protects children's privacy. CSO Online. <https://www.csoononline.com/article/570311/coppa-explained-how-this-law-protects-childrens-privacy.html>
- Garg, K. (2024). Digital identities in Metaverse: Privacy, security, and user authentication in virtual financial systems. *International Journal of Financial Engineering*. <https://doi.org/10.1142/s242478632442009x>
- Gavriliuță, C. (2021). DIGITAL IDENTITY. *Analele Științifice Ale Universității»Alexandru Ioan Cuza«Din Iași. Sociologie Și Asistență Socială*, 14(2), 45–54. <https://www.cceol.com/search/article-detail?id=1226433>
- Ghaffar, S. A. (2024). Metaverse Dynamics: Predictive Modeling of Roblox Stock Prices using Time Series Analysis and Machine Learning. *International Journal Research on Metaverse*, 1(1), 77–93. <https://doi.org/10.47738/ijrm.v1i1.6>
- Greggworth. (2022, July 15). Lack of federal data privacy legislation leaves US agencies to provide guidance. Thomson Reuters Institute. <https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/data-privacy-federal-guidance/> <https://doi.org/10.1109/bigdata55660.2022.10021112>
- Inekwe, J. N., Jin, Y., & Valenzuela, M. R. (2018). The effects of financial distress: Evidence from US GDP growth. *Economic Modelling*, 72, 8–21.
- Jaloliddin Abdusatarov, & Muhammad Ali Turdialiev. (2024). the Issues of Intellectual Property in the Realm of Metaverse. *Social Science Research Network*. <https://doi.org/10.2139/ssrn.4694628>
- Jesse, V. (2024). Intellectual Property Disputes and International Jurisdiction in Metaverse Environment
- KALYVAKI, M. (2023). Navigating Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction. *Journal of Metaverse*, 3(1), 87–92. <https://doi.org/10.57019/jmv.1238344>
- Kamal, A. L. M., & AboElsoud, M. E. (2023). Modeling economic growth factors in Egypt: A quantile regression approach. *Heliyon*, 9(2).

- Kasiyanto, S., & Kilinc, M. R. (2022). The Legal Conundrums of Metaverse. *Journal of Central Banking Law and Institutions*, 1(2), 299–322. <https://doi.org/10.21098/jcli.v1i2.25>
- Krishnaa, R. (2023, May 9). Challenges in Metaverse Jurisdiction and International Treaty Law. *IRPJ = Intergovernmental Research and Policy Journal*. <https://irpj.euclid.int/articles/challenges-in-the-Metaverse-jurisdiction-and-international-treaty-law/>
- Latifzadeh, M., & Mahdi, M. (2023). Introducing Digital Identity in Metaverse, Identifying Related Legal Challenges and Solutions. *Law Quarterly*, 53(2), 349–372. <https://doi.org/10.22059/jlq.2023.353867.1007743>
- LI, C., & white, K. (2023). In collaboration with Accenture Metaverse Privacy and Safety. https://www3.weforum.org/docs/WEF_Metaverse_Privacy_and_Safety_2023.pdf
- Lucatch, D. (2021, December 28). Digital Identity in Metaverse. *Forbes*. <https://www.forbes.com/councils/forbesbusinesscouncil/2021/12/28/digital-identity-in-the-Metaverse/>
- Lutkevich, B. (2020). What is HIPAA (Health Insurance Portability and Accountability Act)? Search Health IT. <https://www.techtarget.com/searchhealthit/definition/HIPAA>
- Mahmoud Ghorab (2022), the impact of foreign investment on GDP in Egypt, *Scientific Journal of Economics and Management*, 52 (4), 105-140
- Matytsin, D. E., Tymchuk, Y. A., Kazachenok, O. P., & Baltutite, I. V. (2024). Theoretical and Legal Comprehension of the Essence of Meta- Universe as a Promising Investment Platform for the Conclusion of Remote Investment Transactions in the Virtual Real Estate Market. *Intelligent Systems Reference Library*, 237–243. https://doi.org/10.1007/978-3-031-51536-1_22
- McKinsey & Company. (2022, August 17). What is Metaverse and where will it lead next? [Www.mckinsey.com; McKinsey & Company. https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-the-Metaverse](https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-the-Metaverse)
- Mehdi Letafati, & Safa Otoum. (2023). on the privacy and security for e-health services in Metaverse: An overview. *Ad Hoc Networks*, 150, 103262–103262. <https://doi.org/10.1016/j.adhoc.2023.103262>
- Mezei, P., & Chawla Aror, G. (2019). *Elgaronline* from Edward Elgar Publishing. [Elgaronline.com. https://www.elgaronline.com/](https://www.elgaronline.com/)
- NATLEX - Egypt - Law 151/2020 on the Protection of Personal Data. (2020). [ilo.org. https://natlex.ilo.org/dyn/natlex2/r/natlex/fe/details?p3_isn=111246&cs=1cC2P3AfHgLTzjaCaGdWFAqxMoyyVTno2m6emtknnETzOR4L35fstMjNV2Ld5berdxzVg1ra8tYsrtqkzSg7-g](https://natlex.ilo.org/dyn/natlex2/r/natlex/fe/details?p3_isn=111246&cs=1cC2P3AfHgLTzjaCaGdWFAqxMoyyVTno2m6emtknnETzOR4L35fstMjNV2Ld5berdxzVg1ra8tYsrtqkzSg7-g)
- Pedraça, S. A. (2024, February 20). Reframing the Game: How the interaction between technology, culture, and marketing plays along in the platform society. *Spectrum.library.concordia.ca*. <https://spectrum.library.concordia.ca/id/eprint/993823/>
- Petar Radanliev. (2024). The rise and fall of cryptocurrencies: defining the economic and social values of block chain technologies, assessing the opportunities, and defining the financial and cyber security risks of Metaverse. *Financial Innovation*, 10(1). <https://doi.org/10.1186/s40854-023-00537-8>
- Raji, M. A., Olodo, H. B., Oke, T. T., Addy, W. A., Ofodile, O. C., & Oyewole, A. T. (2024). BUSINESS STRATEGIES IN VIRTUAL REALITY: a REVIEW OF MARKET OPPORTUNITIES AND CONSUMER EXPERIENCE. *International Journal of Management & Entrepreneurship Research*, 6(3), 722–736. <https://doi.org/10.51594/ijmer.v6i3.883>
- Ruiiu, P., Nitti, M., Piloni, V., Cadoni, M., Grosso, E., & Fadda, M. (2024). Metaverse& Human Digital Twin: Digital Identity, Biometrics, and Privacy in the Future Virtual Worlds. *Multimodal Technologies and Interaction*, 8(6), 48. <https://doi.org/10.3390/mti8060048>
- Saridakis, G., Khan, Z., Knight, G., Idris, B., Mitra, J., & Khan, H. (2024). A Look into the Future: The Impact of Metaverse on Traditional Theories and Thinking in International Business. *Mir. Management International Review/Management International Review*. <https://doi.org/10.1007/s11575-024-00550-8>

- State of California Department of Justice. (2024, March 13). California Consumer Privacy Act (CCPA). State of California - Department of Justice - Office of the Attorney General. <https://oag.ca.gov/privacy/ccpa>
- Tekla Berozashvili. (2024, April 25). Securing Digital Identities in the Era of Remote Identity Verification. <https://doi.org/10.13140/RG.2.2.11839.11688>
- The World Bank. (2024). Data Bank | the World Bank. Worldbank.org. <https://databank.worldbank.org/>
- UC Berkeley. (2019). HIPAA PHI: Definition of PHI and list of 18 identifiers. Berkeley.edu. <https://cphs.berkeley.edu/hipaa/hipaa18.html>
- Ugur Korkut Pata, Mustafa Tevfik Kartal, & Serpil Kılıç Depren. (2024). the Role of Information and Communication Technologies and Energy-Related Research and Development Investments in Energy Transition: Evidence from the United States of America by Machine Learning Algorithm. Energy Technology. <https://doi.org/10.1002/ente.202301199>
- UN.ESCAP. (2021). Foreign direct investment trends and outlook in Asia and the Pacific 2021/2022. Repository.unescap.org. <https://repository.unescap.org/handle/20.500.12870/4146>
- Wang, S., & Wang, W. (2023). A review of the application of digital identity in Metaverse. Security and Safety, 2(Security and Safety Volume 2, 2023), 2023009. <https://doi.org/10.1051/sands/2023009>
- Xu, X., Aschakulporn, P., & Zhang, J. A. (2024). Is the unreal world real? Corporate fraud and investment credibility. Googleusercontent.com. https://scholar.googleusercontent.com/scholar?q=cache:pmktz71QYWsJ:scholar.google.com/+foreign+investors%E2%80%99+confidence+in+the+Metaverse&hl=en&as_sdt=0
- Yadav, A. B. (2024). Protecting privacy in the digital marketplace: A comparative study of legal mechanisms for consumer rights in Metaverse. Journal of Data Protection & Privacy. <https://hstalks.com/article/8655/protecting-privacy-in-the-digital-marketplace-a-co/?business>
- Zhang, W., & Wu, H. (2023). Digital Identity, Privacy Security and their Legal Safeguards in Metaverse. Security and Safety in the “Metaverse,” Volume 2, 2023(Security and Safety). <https://doi.org/10.1051/sands/2023011>
- Zhao, R., Zhang, Y., Zhu, Y., Lan, R., & Hua, Z. (2023). Metaverse: Security and Privacy Concerns. ArXiv (Cornell University), 3(2), 93–99. <https://doi.org/10.57019/jmv.1286526>
- Zou, J., & Hu, X. (2024). Risks of Social Interaction Order in Metaverse and Legal Responses. Proquest.com. <https://www.proquest.com/openview/72f2a0c4d9ccd84492ca54c67353ad2f/1?pq-origsite=gscholar&cbl=1006393>