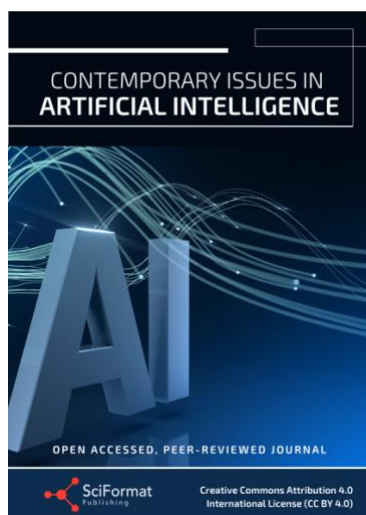




Contemporary Issues in Artificial Intelligence

Vol. 1 (2025)



Publisher:
SciFormat Publishing Inc.

ISNI: 0000 0005 1449 8214
2734 17 Avenue Southwest,
Calgary, Alberta, Canada,
T3E0A7

☎ +15878858911
✉ editorial-office@sciformat.ca

ARTICLE TITLE	CYBERSECURITY CHALLENGES IN THE METAVERSE: A SYSTEMATIC ANALYSIS OF THREATS AND DIRECTIONS FOR LEGAL REGULATION
----------------------	---

ARTICLE INFO	Kateryna Klymenko. (2026) Cybersecurity Challenges in the Metaverse: a Systematic Analysis of Threats and Directions for Legal Regulation. <i>Contemporary Issues in Artificial Intelligence</i> . Vol.1. doi: 10.69635/ciai.2025.55
---------------------	--

DOI	https://doi.org/10.69635/ciai.2025.55
------------	---

RECEIVED	02 June 2025
-----------------	--------------

ACCEPTED	27 December 2025
-----------------	------------------

PUBLISHED	30 December 2025
------------------	------------------

LICENSE	 The article is licensed under a Creative Commons Attribution 4.0 International License .
----------------	--

© The author(s) 2025.

This article is published as open access under the Creative Commons Attribution 4.0 International License (CC BY 4.0), allowing the author to retain copyright. The CC BY 4.0 License permits the content to be copied, adapted, displayed, distributed, republished, or reused for any purpose, including adaptation and commercial use, as long as proper attribution is provided.

CYBERSECURITY CHALLENGES IN THE METAVERSE: A SYSTEMATIC ANALYSIS OF THREATS AND DIRECTIONS FOR LEGAL REGULATION

Kateryna Klymenko

*Institute of Compliance in Financial Markets, Chicago Kent College of Law, 565 West Adams Street,
Chicago, IL 60661, USA*

ORCID ID: 0000-0002-5227-2329

ABSTRACT

The rapid convergence of virtual and augmented reality technologies, distributed ledgers, wearable sensors, and generative artificial intelligence is shaping a new sociotechnical space — the Metaverse, which, according to analyst agencies, is capable of growing from tens of billions of dollars in 2021-2023. to several trillion dollars in the mid-2030s. Simultaneously with the economic potential, this convergence gives rise to qualitatively new cybersecurity challenges that go beyond traditional models of information protection, as they relate not only to data, but also to the bodily experience, identity and psychological integrity of the user. Based on a systematic analysis of specialized scientific literature, industry reports and empirical studies, the article classifies cybersecurity threats in the Metaverse environment in five areas: technical and infrastructure, identification and authentication, data privacy, socio-behavioral and algorithmic-legal. The specifics of threats in the healthcare segment are analyzed, empirical data on the public perception of the responsibility of automated agents for the damage caused are considered, and a comparative legal analysis of the approaches of the European Union and Ukraine to the regulation of high-risk artificial intelligence systems is carried out. Based on the results of the study, a set of areas for improving national legislation is proposed, including the adaptation of a risk-based approach, the development of a three-class model of legal personality of artificial intelligence systems and the introduction of cross-border digital jurisdiction mechanisms.

KEYWORDS

Metaverse; Cybersecurity; Privacy; Artificial Intelligence; Digital Identity; Legal Regulation; Tort Liability; Web 4.0; Virtual Reality; Protection of Personal Data

CITATION

Kateryna Klymenko. (2026) Cybersecurity Challenges in the Metaverse: a Systematic Analysis of Threats and Directions for Legal Regulation. *Contemporary Issues in Artificial Intelligence*. Vol.1. doi: 10.69635/ciai.2025.55

COPYRIGHT

© The author(s) 2025. This article is published as open access under the **Creative Commons Attribution 4.0 International License (CC BY 4.0)**, allowing the author to retain copyright. The CC BY 4.0 License permits the content to be copied, adapted, displayed, distributed, republished, or reused for any purpose, including adaptation and commercial use, as long as proper attribution is provided.

1. Introduction

The concept of "Metaverse", which originally appeared in science fiction literature, over the past five years has become the subject of intensive investments by technological corporations and the object of scientific analysis in the fields of computer science, law, psychology and economics. According to analyst agencies, the global metaverse market, which amounted to approximately \$22.8 billion. in 2021 and about USD 86.3 billion. In 2023, by 2035 it may reach more than \$6.2 trillion. with a compound annual growth rate (CAGR) of 42.8% (ResearchAndMarkets.com, 2025; SkyQuest Technology, 2024). Such rapid economic growth is accompanied by an exponential expansion of the cyberattack surface, as the metaverse integrates personal data, biometric characteristics, financial assets in the form of non-fungible tokens (NFTs), and unprecedentedly detailed user behavioral profiles in a single digital environment.

The relevance of the study is due to the fact that traditional cybersecurity models developed for the two-dimensional web turn out to be insufficient for an environment characterized by permanence, multi-user, immersiveness, and interoperability of virtual spaces (Di Pietro & Cresci, 2021). In addition to purely technical vulnerabilities, the metaverse actualizes problems that were previously peripheral in nature, such as doxxing, cyberbullying, harassment with avatars, identity forgery through deepfakes, as well as the fundamental question of the possibility of bringing to legal responsibility autonomous AI systems operating in this environment.

The article is aimed at a systematic analysis of cybersecurity problems in the Metaverse environment and the formulation of scientifically based directions for improving legal regulation, in particular in the context of the legislation of Ukraine.

To achieve this goal, the following research tasks have been defined: (1) to clarify the theoretical and methodological foundations of considering the metaverse as an object of cybersecurity; (2) carry out a classification of cybersecurity threats in the Metaverse environment; (3) analyze the specifics of threats to user privacy; (4) investigate the problem of authentication and legal responsibility of automated agents based on empirical data; (5) to consider the features of cybersecurity in the specialized segment of healthcare; (6) carry out a comparative legal analysis of regulatory approaches; (7) formulate proposals for improving national legislation.

The methodological basis of the study is made up of general scientific methods of analysis and synthesis, systemic and structural-functional approaches, as well as special legal methods — comparative law and formal-legal. The empirical base was compiled by specialized scientific publications of 2021–2024. (Di Pietro & Cresci, 2021; Lin, 2021a, 2021b; Lima et al., 2021; Sharma et al., 2024), industry analytical reports (ResearchAndMarkets.com, 2023, 2025; SkyQuest Technology, 2024; Statista, 2022), as well as the author's work on the model of the law on artificial intelligence and the doctrine of digital law of the metaverse (Kostenko, 2024, 2025).

2. Theoretical and methodological foundations of the study of the Metaverse as an object of cybersecurity

2.1 Concept and essential features of the metaverse

In the modern scientific literature, the metaverse is defined as a set of permanent, multi-user, shared three-dimensional virtual spaces that intertwine with the physical world and form a single and continuous virtual universe accessed by users using avatars (Di Pietro & Cresci, 2021). Researchers distinguish three essential features that distinguish the metaverse from previous generations of the Internet: activity diversity — the ability to carry out social, gaming, educational, commercial and labor activities in a single environment; immersiveness, which is achieved thanks to augmented and virtual reality technologies and brain-computer interfaces; as well as interoperability, which involves the seamless transfer of digital assets and user identity between different applications and spaces.

It is the combination of these three features, and not individual technologies themselves, that is the source of qualitatively new cybersecurity risks. If in previous generations of the web, the data of individual platforms remained mostly scattered, then the architecture of the metaverse provides for their systematic aggregation, which radically increases the value of a single point of compromise for an attacker. In the doctrine of digital law, this feature is proposed to be summarized by the formula "Metaverse = Web 4.0 + new social relations + digital legislation + digital jurisdiction", which emphasizes that the security challenges of the metaverse have not only a technical, but also a regulatory and jurisdictional dimension (Kostenko, 2025).

2.2 The concept of the "singularity" of the metaverse and its security implications

Di Pietro and Cresci (2021) propose to consider the metaverse through the prism of the concept of "singularity" — the point at which the gradual accumulation of quantitative technological changes leads to a qualitative transformation of the environment itself. The authors draw an analogy with the second law of dialectics by G. W. F. Hegel, emphasizing that the analysis of the metaverse through the prism of individual components (VR, blockchain, AI) and their isolated interaction is methodologically insufficient, since the cumulative effect of convergence of these technologies in a single domain is a fundamentally new quality, not reducible to a simple sum of parts.

For the purposes of cybersecurity analysis, this theoretical conclusion is of practical importance: security measures developed for individual technologies (for example, standard authentication protocols for web applications) cannot be mechanically transferred to the metaverse environment without taking into account the mutually reinforcement effects of threats that arise at the intersection of privacy, identity, and automated decision-making.

2.3 Methodology and source base of the study

The study is based on a narrative review involving primary scientific sources covering conceptual analysis of metaverse security (Di Pietro & Cresci, 2021), industry specifics of cybersecurity in the medical segment (Lin, 2021a, 2021b), and an empirical study of public perceptions of the responsibility of automated agents (Lima et al., 2021), complemented by an up-to-date critical review (Sharma et al., 2024) and industry statistical reports (ResearchAndMarkets.com, 2023, 2025; SkyQuest Technology, 2024; Statista, 2022). The selection of sources was carried out according to the criterion of thematic relevance and the availability of verified empirical data, which made it possible to avoid purely speculative forecasts. The comparative legal block of the study is based on the text of the proposal of the European Union regulation on artificial intelligence (European Commission, 2021) and the author's developments of the draft Law of Ukraine on Artificial Intelligence (Kostenko, 2024).

3. Systematization of cybersecurity threats in the Metaverse environment

The analysis of scientific sources provides grounds to identify five interrelated groups of cybersecurity threats in the Metaverse environment, which are summarized in Table 1.

Table 1. Classification of Cybersecurity Threats in the Metaverse Environment
(systematized by the author based on: Di Pietro & Cresci, 2021; Sharma et al., 2024)

Threat category	Examples of manifestations	Main sources of risk
Technical and infrastructural	Denial-of-service (DDoS) attacks, compromise of render servers, vulnerabilities in augmented/virtual reality device communication protocols, attacks on sensor data transmission channels	Distributed platform architecture; heterogeneity of peripheral devices; lack of uniform standards of interaction
Identification and authentication	Avatar identity theft, impersonation through deepfakes and behavioral pattern reproduction, compromise of VR/AR headset credentials, bots impersonating humans	Biometric profiling of body movements; the complexity of verifying the "humanity" of the interlocutor; lack of cross-platform authentication
Data privacy	Profiling based on physiological and behavioral data, doxxing, leakage of sensitive information about user habits, secondary use of biometrics without consent	Continuous collection of multi-sensor data; Aggregate data from multiple apps into a single profile
Socio-behavioral	Cyberbullying, Coordinated Harassment, Sexual Harassment Using Avatars, Abuse of Underage Users, Social Engineering in an Immersive Environment	No physical barriers to contact; the effect of disinhibiting behavior in the anonymous avatar space
Algorithmic and legal	Bias of automated moderators, opacity of recommendation algorithms, gap of responsibility for harm caused by autonomous agents, manipulative content generated by AI	Delegating decisions to algorithms without proper supervision; lack of an established doctrine of AI legal personality

The technical and infrastructure group of threats is due to the fact that the metaverse operates on the basis of a distributed infrastructure of edge computing, rendering servers for three-dimensional environments, and low-latency network protocols. Sharma et al. (2024) emphasize that current cybersecurity solutions are only partially able to counteract attacks on this infrastructure, since most security standards were developed for the client-server architecture of the classic web, and not for environments with a high degree of touch integration.

The identification-authentication group is, in our opinion, the most specific for the metaverse, since it is here that technological convergence gives rise to fundamentally new attack vectors. Wearable devices capture unique biometric patterns of body movement that can be used by an attacker to create a digital twin of the victim and carry out social engineering on behalf of the victim against the circle of trusted persons (Di Pietro & Cresci, 2021). The problem is compounded by the fact that metaverse users are increasingly interacting with chatbots and game agents, which makes the distinction between humans and machines a non-trivial task and creates favorable conditions for masking harmful automated activity.

The group of data privacy threats is discussed in detail in Section 4 of this article. The socio-behavioral group covers phenomena that in the traditional web were peripheral in nature (cyberbullying, coordinated bullying), but in an immersed three-dimensional environment, in the absence of physical barriers of deterrence, they become systemic. Finally, the algorithmic legal group reflects the fundamental problem of delegating socially significant decisions to automated systems in conditions where the scale of the metaverse makes it impossible to fully human supervision of each decision; This problem is analyzed in detail in Chapter 5 based on empirical evidence.

Thematic Structure of Metaverse Cybersecurity Publications

(Based on Literature Analysis Results)

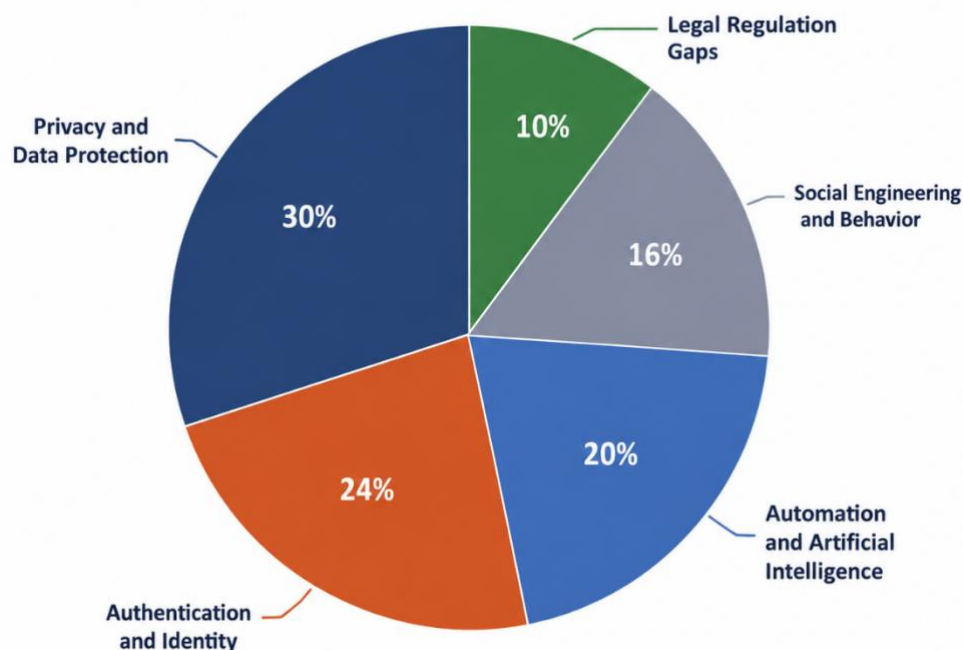


Fig. 1. Thematic structure of Metaverse cybersecurity challenges based on the results of literature analysis (illustrative breakdown, compiled by the author)

4. User Privacy in the Metaverse: Profiling, Doxxing, and Behavioral Surveillance

In the logic of the modern digital economy, if the user does not pay for the service, his data becomes the product. Di Pietro and Cresci (2021) make a compelling case that this pattern in the metaverse environment is taking on extreme expression: the platform is capable of capturing body movements, physiological responses, and probably even patterns of user brain activity, making modern social media data collection mechanisms comparatively primitive. This creates unprecedented opportunities for micro-targeted influencers that go far beyond traditional contextual advertising.

The authors identify three areas in which privacy risks increase most significantly: personal information (risk of doxxing — disclosure of private information for the purpose of extortion or public humiliation), behavior (risk of surveillance, harassment and social engineering carried out in an immersive environment without physical restrictions inherent in the real world) and communication (risk of unauthorized distribution of intimate content, similar to "revenge", but in the format of three-dimensional interaction avatars). Empirical surveys confirm the high level of user concern about these risks: according to a survey of metaverse users in the United States, 43% of respondents are "very concerned" about the possible theft of real identities, 41% are "very concerned" about selling their data to third parties, and 35% are about hacking the metaverse identity or avatar itself (Statista, 2022).

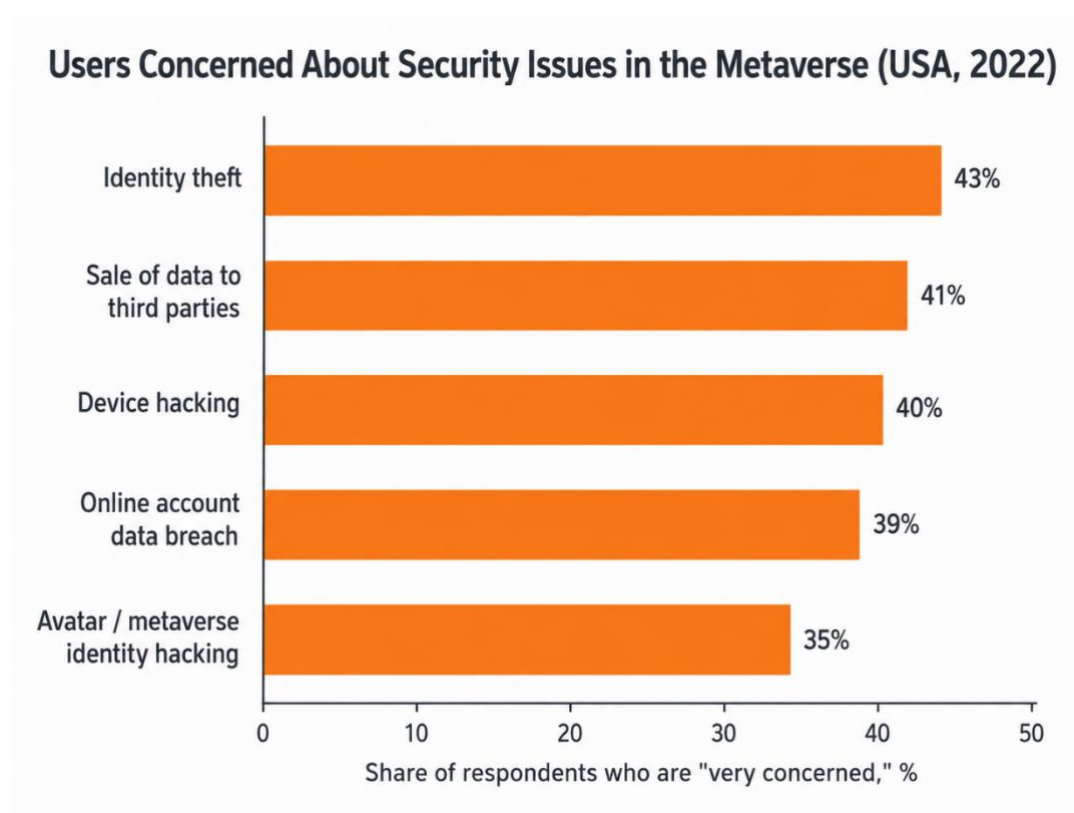


Fig. 2. The level of concern of metaverse users about security and privacy issues (compiled by: Statista, 2022)

In response to these risks, the scientific literature has proposed a combination of three basic strategies for protecting avatar privacy, summarized in Table 2.

Table 2. User Privacy Strategies in Three-Dimensional Social Metaverses
(compiled from: Di Pietro & Cresci, 2021)

Privacy Policy	Description of the mechanism	Application Limitations
Cloning avatar activity	Creating a "dummy" or several clones of your own avatar to divert attention from the real activity of the user	Does not eliminate the initial collection of biometric data by the platform; requires additional computing resources
Private instances of space	Temporarily create a private copy of a public virtual space or block other users' access to it	Limits social interaction; possible only for spaces that technically support instantiation
Teleportation, invisibility, disguise	Providing the user with the ability to instantly change location, become invisible to other avatars, or apply appearance masking	Requires additional identity verification to prevent abuse (e.g., moderation evasion)

It is important to emphasize that none of the strategies given were designed for complex, massively interconnected multiverses; existing solutions are focused on simplified metaverse models and need significant refinement before being implemented in scalable commercial platforms (Di Pietro & Cresci, 2021). In addition, the effectiveness of technical privacy strategies is limited without appropriate regulatory backing — in particular, without the legal obligation of platforms to provide users with an accessible menu of privacy settings and without establishing legal liability for the forced aggregation of biometric profiles.

5. Authentication, Artificial Intelligence, and the Problem of Legal Liability of Automated Agents

The problem of authentication in the metaverse is inextricably linked to the question of content integrity and the ability to distinguish between a human and an automated agent. As AI-powered chatbots and in-game agents become increasingly compelling, there is an increasing risk of automated accounts being used to manipulate users on a scale beyond the capabilities of current detection systems (Di Pietro & Cresci, 2021). This problem has a direct legal continuation: if an automated agent is capable of causing harm comparable to the harm from human actions, the question arises of an adequate model of legal responsibility for such damage.

An empirical study by Lima et al. (2021), which covered 3559 respondents in two surveys, makes it possible to check how much public intuition about punishing automated agents is consistent with the capabilities of current legal doctrines. The researchers found a statistically significant conflict: respondents showed a clear desire to punish AI and robots for the harm caused (the average rating of the desire to punish for autonomous agents is 1.42 on a scale of 0-3), but at the same time they did not believe that such punishment could provide deterrence or retaliation, and categorically did not want to endow automated systems with assets or physical independence — that is, exactly those legal prerequisites, which are necessary for civil and criminal liability, respectively.

Table 3. Average Attribution of Responsibility, Punishment, and Awareness for Autonomous Agents
(compiled from data: Lima et al., 2021, Figure 1A)

Agent Type	Responsibility (M, scale 0–3)	Punishment (M, scale 0–3)	Awareness (M, scale 0–3)
Human (autonomous agent)	2,51	2,55	2,04
Artificial intelligence (autonomous)	1,73	1,57	0,78
Robot (autonomous)	1,55	1,53	0,57

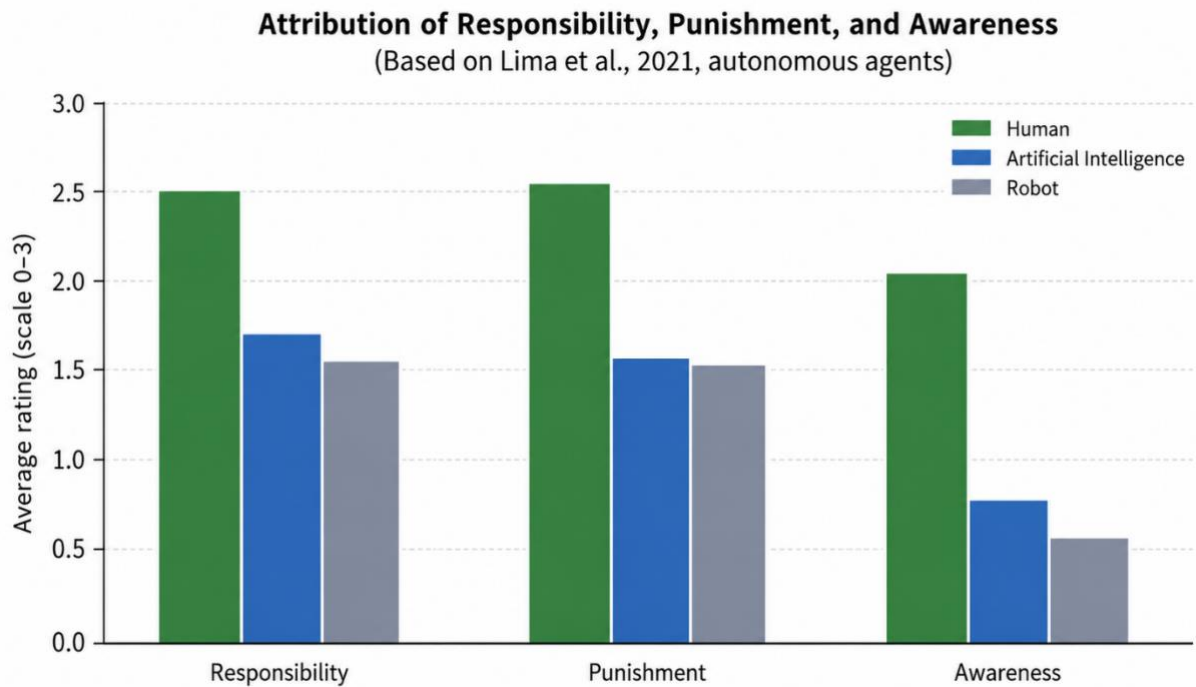


Fig. 3. Comparative attribution of responsibility, punishment and awareness to humans, artificial intelligence and work (by: Lima et al., 2021)

As can be seen from Table 3 and Figure 3, a human agent is attributed significantly higher responsibility than AI or robot (2.51 versus 1.73 and 1.55, respectively), and the level of awareness of one's own actions, which respondents attribute to automated agents, is extremely low (0.78 and 0.57 versus 2.04 for humans). The authors of the study interpret this as confirmation of the "retribution gap" formulated by Danager: people seek to punish an automated offender guided by punitive intuition, despite the realization that such a sanction will not achieve any of the classic functions of legal punishment (Lima et al., 2021).

For the doctrine of artificial intelligence law, this empirical result is of significant practical importance: attempts to introduce the "electronic legal personality" of autonomous systems solely for the purpose of imposing tort or criminal liability on them are met not only with theoretical objections by scholars (Bryson et al., cited by: Lima et al., 2021), but also with contradictory public intuition, which simultaneously demands punishment and refuses to ensure its legal enforceability. In the context of the development of Ukrainian legislation on artificial intelligence, this argues in favor of a three-class model of legal personality of AI systems, which distinguishes between (1) instrumental systems without independent legal personality, the responsibility for which rests with the developer, owner or operator; (2) systems with limited functional legal personality in clearly defined areas (e.g. representation of interests in digital transactions); and (3) a hypothetical class of systems with extended autonomy, for which a special-purpose regime of joint (several) responsibility of all actors involved — developer, owner, and operator — can be considered, instead of shifting the burden exclusively to the system itself (Kostenko, 2024).

6. Cybersecurity in Specialized Metaverse Segments: A Healthcare Case Study

Of particular note is the medical metaverse segment (Healthcare Metaverse), which integrates mobile medical applications (mHealth), wearable sensors, electronic medical records, and clinical decision support systems into a single immersive environment (Lin, 2021b). The specificity of this segment lies in the critical sensitivity of the processed data: even a minor modification or leakage of a patient's medical data can have irreversible consequences for his life and health, which fundamentally distinguishes the medical metaverse from entertainment or commercial segments.

Lin (2021b) identifies a specific threat set for this segment, which includes distributed denial-of-service (DDoS) attacks, internal staff attacks, malware, including ransomware, phishing, as well as risks related to proprietary device policies (BYOD), network penetration, and third-party attacks. The author emphasizes that

the existing arsenal of countermeasures — multi-factor authentication, intrusion detection and prevention systems, firewalls, digital forensics, antivirus software, access control and encryption — remains insufficient despite its necessity due to the scale and heterogeneity of modern medical information systems.

The practical conclusion for the regulation is that a unified cybersecurity standard for the metaverse as a whole is unlikely to be adequate for the medical segment: the latter requires an industry profile of requirements comparable in severity to current medical data protection standards (e.g., HIPAA in a US jurisdiction), but adapted to the specifics of continuous multi-sensor data collection inherent in immersive technologies.

7. Economic Dimension and Market Trends of Cyber Threats in the Metaverse

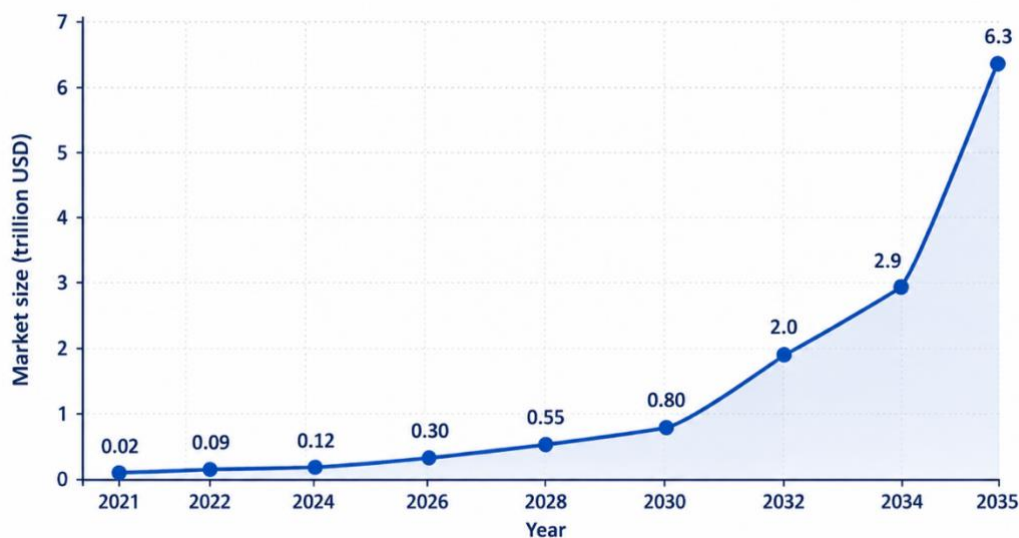
The scale of the potential consequences of cyber threats in the Metaverse environment should be considered in the context of the predicted dynamics of the market itself. Despite the differences in the methodology of individual analytical agencies, all available forecasts unanimously record ultra-high growth rates — from 39.7% to 42.8% per year (Table 4), which is significantly ahead of the dynamics of the adjacent cybersecurity market, which, according to ResearchAndMarkets.com (2023), is growing much more slowly — from USD 197.4 billion. in 2021 to the projected USD 657.02 billion. In 2030, that is, with an average annual growth rate of only 12.8%.

Table 4. Comparison of Global Metaverse Market Size Forecasts as Estimated by Various Analytics Agencies

Forecast source	Base year and market volume	Forecast Year and Market Volume	Annual Growth Rate (CAGR)
ResearchAndMarkets.com (2025)	2025 — USD 124.87 billion. USA	2035 — 6.27 trillion dollars. USA	42,78%
ResearchAndMarkets.com (2025)	2023 — USD 86.31 billion. USA	2031 — USD 803.29 billion. USA	39,68%
ResearchAndMarkets.com (2022, 3BiT CAGR)	2021 — USD 22.79 billion. USA	2030 - Forecast based on CAGR	39,80%

Global Metaverse Market Size and Forecast, 2021–2035

Market size in trillion USD



Note: Data for 2021–2023 are actual estimates; 2024–2035 are forecasts.

Source: Statista, 2023; Analysis

Fig. 4. Dynamics and forecast of the global Metaverse market volume, 2021–2035 (built on: ResearchAndMarkets.com, 2022, 2025; SkyQuest Technology, 2024)

The gap between the growth rate of the metaverse market (about 40% per year) and the growth rate of the cybersecurity solutions market (about 13% per year) creates a structural imbalance that researchers label as the "Wild, Wild West" of the metaverse: phishing attacks, NFT asset fraud, and malware are already being recorded in the early stages of platform development, while investments in security infrastructure are systematically lagging behind the pace of commercialization of the environment itself. This confirms the thesis of the need for proactive, rather than reactive, regulation of metaverse cybersecurity — that is, the establishment of mandatory security requirements at the stage of platform design (security by design), and not just responding to incidents that have already occurred.

8. Comparative Legal Analysis of Approaches to Regulating Cybersecurity and Artificial Intelligence in the Metaverse

The European Union's Artificial Intelligence Regulation (European Commission, 2021) is the first attempt to systematically regulate high-risk AI applications, including biometric identification and law enforcement. At the same time, as Di Pietro and Cresci (2021) point out, the metaverse as a "singleton" platform — that is, a platform that seeks centralized aggregation of virtually all types of online activity — poses a regulatory challenge that is not fully covered by the current European approach: the question of which jurisdiction applies to the cross-border interaction of millions of users in a single virtual space remains open.

Table 5. Comparative Analysis of EU and Ukrainian Regulatory Approaches to Artificial Intelligence in the Projection on the Metaverse Environment
(compiled by the author on the basis of: European Commission, 2021; Kostenko, 2024)

Comparison criterion	EU Artificial Intelligence Regulation (AI Act)	Draft Law of Ukraine on Artificial Intelligence	Significance for the Metaverse
Regulatory approach	Risk-oriented, with a gradation of AI systems according to the level of risk	Risk-based approach adapted to the national context	Allows you to differentiate requirements for entertainment and critical segments (medicine, finance)
Biometric identification	Prohibition of certain practices of mass biometric identification in public space	Elaboration of provisions on profiling, social scoring and recognition of emotions (Article 5 of the draft)	Directly refers to biometric profiling of avatars and wearable sensors
Synthetic/Generated Content	Labeling requirements for deepfakes and AI-generated content	Elaboration of definitions of deepfakes and synthetic media	Critical to counteract avatar impersonation in immersive environments
Модель відповідальності	Division of responsibilities between the supplier and the user of the AI system	Discussion on the three-class model of AI legal personality (instrumental / limited legal personality / autonomous systems)	Avoids the "retribution gap" recorded empirically (Lima et al., 2021)
Jurisdictional dimension	Extraterritorial action on systems affecting individuals in the EU	Needs to develop the concept of digital jurisdiction for cross-border platforms	The metaverse as a "singleton" platform requires a consistent cross-border jurisdiction (Di Pietro & Cresci, 2021)

The comparative analysis allows us to conclude that the current regulatory models, including the draft Ukrainian law on artificial intelligence, are mostly focused on classifying AI systems by risk level and establishing prohibitions on certain practices (profiling, social scoring, emotion recognition), but do not contain specialized provisions that would take into account the specifics of the immersive, multi-sensory environment of the metaverse. This confirms the need to develop an industry addendum to the general legislation on artificial intelligence, dedicated specifically to the security aspects of virtual and mixed realities.

9. Directions for improving the legislation of Ukraine on Metaverse cybersecurity

Based on the analysis, a set of areas for improving national legislation in the field of cybersecurity of the metaverse is proposed.

Firstly, it is expedient to legislate the principle of "security by design" as a mandatory requirement for developers of metaverse platforms operating in Ukraine or providing services to Ukrainian users, with a special emphasis on the protection of biometric data obtained by wearable sensors and augmented and virtual reality headsets.

Secondly, taking into account the empirically recorded conflict between the public desire to punish automated agents and the inability to ensure the legal feasibility of such punishment (Lima et al., 2021), it is proposed to develop a three-class model of legal personality of artificial intelligence systems, which distinguishes between instrumental, limited legal personality and potentially autonomous systems, with the imposition of primary responsibility on the developer, owner and operator of the system on the principle of solidarity (joint) responsibility, and not on the automated system itself (Kostenko, 2024).

Third, given the cross-border nature of metaverse platforms and their tendency towards centralized aggregation of user activity (Di Pietro & Cresci, 2021), it is relevant to develop a doctrine of digital jurisdiction capable of determining the applicable law and competent authority in situations where harm is caused to a user of one state by an avatar or an automated agent registered in another jurisdiction. The author proposes to consider this problem within the framework of the doctrinal formula "Metaverse = Web 4.0 + new social relations + digital legislation + digital jurisdiction" (Kostenko, 2025), which provides for the parallel development of the substantive and jurisdictional components of regulation.

Fourth, for segments with high data sensitivity, in particular the medical metaverse, it is proposed to introduce an industry profile of cybersecurity requirements, which would establish mandatory standards for multi-factor authentication, encryption and backup of medical data received through immersive interfaces (Lin, 2021b), by analogy with the approaches used in personal data protection legislation in the field of healthcare.

Fifthly, taking into account the problem of doxxing, harassment and social engineering in an immersed environment recorded in the literature (Di Pietro & Cresci, 2021), it is advisable to supplement the legislation on cyberbullying and harassment with special corpus delicti that take into account the specifics of interaction through avatars, including the definition of the legal status of a person's "digital twin" as an object of legal protection.

10. Conclusions

The study confirms that the Metaverse environment gives rise to qualitatively new cybersecurity challenges that are not reduced to a simple extrapolation of threats to the traditional web. The convergence of immersion, interoperability, and automation technologies creates a "singularity" effect, in which the aggregate risk exceeds the sum of the risks of the individual components of the technologies (Di Pietro & Cresci, 2021).

The systematization of threats in five areas — technical and infrastructure, identification and authentication, data privacy, socio-behavioral, and algorithmic legal — shows that the most specific for the metaverse are identification and algorithmic-legal threats, since they are associated with multi-sensor biometrics unique for this environment and increasingly deep automation of decision-making.

Empirical evidence from Lima et al. (2021) demonstrates a contradiction in public intuition about the responsibility of automated agents, which both demands punishment and refuses to ensure its legal enforceability, arguing in favor of models of joint responsibility of all actors involved instead of placing responsibility on the AI system itself.

The comparative legal analysis showed that the current regulatory framework, including the legislation of Ukraine on artificial intelligence, needs a sectoral supplement that would take into account the specifics of the immersive environment, and the economic analysis of market trends — a significant gap between the growth rate of the metaverse market (about 40% per year) and the pace of development of the protective cybersecurity infrastructure (about 13% per year) — confirms the need for a proactive regulatory response.

Prospects for further research are related to the empirical verification of the proposed three-class model of the legal personality of artificial intelligence based on the material of Ukrainian law enforcement, as well as the development of industry standards for cybersecurity for certain segments of the metaverse, primarily medical and financial.

REFERENCES

1. Di Pietro, R., & Cresci, S. (2021). *Metaverse: Security and privacy issues*. ResearchGate. <https://www.researchgate.net/publication/357116743>
2. European Commission. (2021). *Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*. European Commission.
3. Kostenko, O. (2024). *AI law model for ethical legislation* [Monograph]. SciFormat Publishing.
4. Kostenko, O. (2025). *Metaverse and digital law* [Monograph]. Zenodo. <https://doi.org/10.5281/zenodo.21619125>
5. Lima, G., Cha, M., Jeon, C., & Park, K. S. (2021). The conflict between people's urge to punish AI and legal systems. *Frontiers in Robotics and AI*, 8, Article 756242. <https://doi.org/10.3389/frobt.2021.756242>
6. Lin, W. W. K. (2021a). *Cybersecurity in metaverse*. ResearchGate. <https://www.researchgate.net/publication/355444858>
7. Lin, W. W. K. (2021b). *Cybersecurity intelligence in the healthcare metaverse*. ResearchGate. <https://www.researchgate.net/publication/357070600>
8. ResearchAndMarkets.com. (2023, January 17). Cyber security market report 2022: Introduction of blockchain cybersecurity presents opportunities. *Business Wire*. <https://www.businesswire.com/news/home/20230118005655/en>
9. ResearchAndMarkets.com. (2025, November 19). Metaverse industry research and global forecasts report 2025–2035: \$6.25+ trillion market expands as Meta, Microsoft, and Google invest in virtual advertising, immersive events, next-gen entertainment. *Business Wire*. <https://www.businesswire.com/news/home/20251119891533/en>
10. Sharma, S., Singh, J., Gupta, A., Ali, F., Khan, F., & Kwak, D. (2024). User safety and security in the metaverse: A critical review. *IEEE Open Journal of the Communications Society*, 5, 5467–5487. <https://doi.org/10.1109/OJCOMS.2024.3397044>
11. SkyQuest Technology. (2024, July 1). Metaverse market size: Set to reach USD 803.29 billion by 2031. *GlobeNewswire*. <https://www.globenewswire.com/news-release/2024/07/01/2906714/0/en/Metaverse-Market-Size-Set-to-Reach-USD-803-29-Billion-by-2031-SkyQuest-Technology.html>
12. Statista. (2022, October 19). *Potential security concerns according to metaverse enthusiasts in the United States as of August 2022* [Graph]. <https://www.statista.com/statistics/1346474/us-metaverse-security-concerns-2022/>