BRATISLAVA LAW REVIEW

PUBLISHED BY
THE FACULTY OF LAW,
COMENIUS UNIVERSITY
BRATISLAVA

ISSN (print): 2585-7088
ISSN (electronic): 2644-6359

# A TYPICAL CROSS-BORDER METAVERSE MODEL AS A COUNTERACTION TO ITS FRAGMENTATION /

Oleksii Kostenko, Dmytro Zhuravlov, Volodymir Nikitin, Volodymyr Manhora, Tamila Manhora

Oleksii V. Kostenko, Ph.D.
State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine",
3-A Askoldiv Alley,
01010 Kyiv; Ukraine.
antizuk@gmail.com
ORCID: 0000-0002-2131-0281

Dmytro V. Zhuravlov, D.Sc.
Office of the President of Ukraine,
Bankova 11, 01220 Kyiv; Ukraine.
ndz0909@gmail.com
ORCID: 0000-0002-2205-682

Volodymir V. Nikitin, D.Sc.
National Aviation University,
1 Huzara Liubomira Ave.,
03058 Kyiv; Ukraine.
vv_nikitin@ukr.net
ORCID: 0000-0001-6915-6319

Volodymyr V. Manhora, Cand.Sc.
Vinnytsia National Agrarian University,
Sonyachna 3,
21000 Vinnytsia; Ukraine.
vmangora@gmail.com
ORCID: 0000-0003-3812-3797

Tamila V. Manhora, Cand.Sc.
Vinnytsia National Agrarian University,
Sonyachna 3,
21000 Vinnytsia; Ukraine.
tmangora@gmail.com
ORCID: 0000-0002-7010-8768

Abstract: *The paper addresses the issue of the Metaverse's territoriality and its connection with national and international law. The study provides a brief overview of hypotheses related to the territoriality of the Metaverse and its connection with national and international law. It explores the concept of electronic jurisdiction for the Metaverse amidst the general absence of a unified transnational legal system for virtual environments. The Internet and the Metaverse are increasingly subject to the reality of fragmenting into separate segments, which can have serious consequences for global security and the economy.*

*The risks associated with the trend of "Metaverse fragmentation" or "Splinternet"—the division of the single global internet space into isolated segments governed by different rules and technical standards—are analysed.*

*Innovatively, a theoretical model of a typical Metaverse is presented, potentially creating a cross-border "sandbox" for modeling technological processes, social relations, business, and legal regulation of virtual technologies to develop proposals for unifying the fundamental components of the Metaverse and simplifying cross-border interactions.*

*The proposed Transborder Standard Model of the Metaverse is an abstract representation of systems used to understand, predict, and explain the behaviour of a complex of systems known under the generalised name Metaverse. This model is characterised by a specific structure composed of modules or ecosystems that functionally differ in purpose and structure and are not connected by similar features. However, their combined application ensures the functionality of virtual environments, and their legal regulation, and can serve as the basis for electronic jurisdiction.*

Key words: *Metaverse; Splinternet; Sandbox; Digital; Electronic Jurisdiction; Metaverse Model*

Suggested citation:
Kostenko, O. V., Zhuravlov, D. V., Nikitin, V. V., Manhora, V. V., Manhora, T. V. (2024). A Typical Cross-Border Metaverse Model as a Counteraction to Its Fragmentation. *Bratislava Law Review*, 8(2), 163-176. https://doi.org/10.46282/blr.2024.8.2.844

Submitted: 20 March 2024
Accepted: 14 October 2024
Published: 31 December 2024

## 1. INTRODUCTION

The Metaverse is a revolutionary concept, a new paradigm for the next-generation internet, a fully immersive shared virtual environment that combines physical reality with digital virtuality. Thanks to the latest developments in new technologies such as augmented reality, artificial intelligence, and blockchain, the Metaverse is transitioning from science fiction to the reality of the near future (Wensheng et al., 2023). The Metaverse is an interconnected network of social, networked immersive environments on permanent multi-user platforms that provide seamless embodied real-time user communication and dynamic interaction with digital artifacts. The Metaverse includes social virtual reality (VR) platforms compatible with massively multiplayer online games, open game worlds, and augmented reality (AR) collaborative workspaces (Aljanabi and Mohammed, 2023). The Metaverse offers new opportunities to provide a safer, more inclusive, and equitable digital space, reducing risks associated with data and its ownership (Mystakidis, 2022). However, this technology also faces its challenges.

However, despite the significant potential of the Metaverse in shaping the future of the internet, there are obstacles that need to be overcome, as well as challenges and problems that require further discussion and development, first and foremost, the need for legal regulation of the Metaverse (Ramírez-Herrero, Ortiz-de-Urbina-Criado and Medina-Merodio, 2023).

The current legal regulation of the Metaverse faces three important challenges. The first involves the development of legal mechanisms for holding individuals accountable for cybercrimes committed using digital technologies, both at the national and international levels (Stănilă, 2023).

The second challenge is related to the lack of a unified transnational legal system for the Metaverse that regulates social relations on a global scale, given that jurisdiction should not be limited to specific territories or borders (Qin, Wang and Hui, 2022).

The third problem is that there is no basic or typical Metaverse model because of which any virtual spaces should be formed in the future. This model should become the foundation for technological, technical-legal, legal and social regulation of social relations, the creation of electronic jurisdiction in new digital worlds and emerging societies. The development of a projection of the basic or typical Metaverse model, based on well-known taxonomies (Park and Kim, 2022), is the purpose of this study.

## 2. THE COLLAPSE OF THE DIGITAL SPACE AND ITS GLOBAL CHALLENGES

The disintegration of the Internet and the Metaverse into separate fragments, a process often described as «Splinternet» could have far-reaching consequences for global security, the economy, and society (Luts, Nastasiak, Karmazina and Kovbasiuk, 2021) as a whole (Crespo-Pereira, Sánchez-Amboage and Membiela-Pollán, 2023). Assessing this phenomenon requires consideration of several key aspects:

Economic Impact: Restrictions on Innovation: Fragmentation can make it difficult to collaborate and share knowledge, which is critical for the development of new technologies. This can slow down innovation and reduce global competitiveness (Ghirmai et al., 2023).

Trade Barriers: A fragmented digital world could lead to the creation of new trade barriers, affecting global trade and economic growth (Rawat and El alam, 2023).

Security and Privacy: Fragmentation can complicate international cooperation on cybersecurity, increasing the risks of cyberattacks and malicious activity (Sebastian, 2023).

Data Protection: Different data protection regulations may complicate international information sharing and affect user privacy.

Socio-cultural impact: Fragmentation can lead to greater control over information by governments or large corporations, limiting freedom of speech and access to information (Wang, Su and Yan, 2023; Garrido, Nair and Song, 2023).

Societal Divide: Different information spaces can contribute to the creation of information bubbles, which exacerbates social and political divides.

Legal and Regulatory Challenges: International Law and Standards: The development of separate rules and standards in different jurisdictions can complicate international cooperation and legal interaction (Bagheri and Jahromi, 2016).

Conflict of Jurisdictions: Conflicts between different national and international laws can create legal uncertainty, especially for international companies (Kalyvaki, 2023).

Technology Challenges: Interoperability and Integration: Fragmentation can complicate the interoperability of technologies and platforms, creating technical barriers for users and developers (González H., Kauffer, Koff and Maganda, 2023).

In conclusion, the fragmentation of the Internet and Metaverse could have serious implications for the global economy, security, human rights, and socio-cultural dynamics. It requires close monitoring, international dialogue, and cooperation to ensure a balanced approach between national interests and global integration.

## 3. METAVERSE DEVELOPMENT STATUS

During the evolution of post-industrial society and its transformative trends, experts predict a three-phase developmental trajectory for the Metaverse. The first phase is characterised by the technocratic nature of the Metaverse, where entities, objects, content, and code depend on its developers and the owners of internet components. In the second phase, while the technical core of the Metaverse remains under the control of the owners and developers, there emerges a trend toward partial transfer of ownership and control over the content to users (content creators) and stakeholders. The third phase represents a profound transformation: content in the Metaverse will no longer be tied to specific developers. Instead, control over entities, subjects, and objects in this digital world will be exercised directly by the owners through code, endowing subjects and objects with functions and rights similar to those of their owners. This stage also includes the reclassification of entities within the Metaverse (Kostenko et al., 2023a).

Currently, the Metaverse is in its nascent stage, comprising disconnected technological and informational domains or digital corporations. These meta-corporations are in competition for users, finances, products, and technologies. Researchers have noted the structuring of the Metaverse, which is now unfolding in the first phase of its development. It's crucial to recognise that today's Metaverse is being shaped under the control of private, business, and state meta-corporations. Despite this, the Metaverse is already giving rise to elements such as Personal Metaverse (PM), Collective Metaverse (CM), Corporate Metaverse (CorpM), Confederative Metaverse (CfM), State Metaverse (SM), and Darkmetaverse (DarkMet), the latter serving as a counter element to positive technologies. (Kostenko et al., 2023a).

## 4. SPLINTERNET METAVERSE OR DIGITAL BALKANISATION

The initial phase of the Metaverse's evolution highlights the emerging concept of "Metaverse Fragmentation through the implementation of a 'Local Cyber Sovereignty' mechanism" (Moldovan, 2021; Vidyarthi and Hulvey, 2021). Considering this, we propose

DOI: 10.46282/blr.2024.8.2.844

an original definition for Metaverse fragmentation: "Metaverse Fragmentation refers to the division of the global Metaverse network (WEB 3.0) into distinct segments ('Splinternet'), each governed by different jurisdictions and regulated by varying laws, standards, and technical solutions". This is exemplified by specific cases such as the "The Golden Shield Project" or the "Great Firewall of China," the use of Deep Packet Inspection (DPI) technology, and the "Oculus" system in the creation of Russia's "sovereign Internet", as well as networks like North Korea's "Kwangmyong", Iran's National Information Network "NIN", and internet content filtering systems in Iraq, Myanmar, Pakistan, and Turkmenistan (Tai and Zhu, 2022; Gosztonyi 2023).

The trend towards creating a "Splinternet" is increasingly evident in countries where governments significantly restrict fundamental human and democratic values. These regimes, under the guise of "preserving cultural identity" through control over content and information flows, believe that internet surveillance will help protect the nation from external cyber threats. They also think that isolating cyberspace and the Metaverse will allow for more effective control over the information space by limiting access to alternative information sources. In the "Splinternet," artificial intelligence and machine learning technologies are also actively employed for pervasive information control, potentially leading to issues in international relations due to information isolation.

## 5. DESTRUCTIVE TRANSFORMATION IN THE METAVERSE

The year 2022 marked significant changes in the approaches to the development of the Metaverse. Numerous conflicts and military actions triggered processes of geopolitical instability, encompassing uncertainties in international relations, global disputes, economic fluctuations, terrorist threats, and other complexities.

The emergence of the so-called "Splinternet" in certain regions indicates a potential intensification of isolation for specific segments of cyberspace and the birth of unique WEB 3.0 content, encompassing corporate (CorpM), state Metaverse (SM), and Darkmetaverse (DarkMet). A key feature of the "Splinternet" is the use of artificial intelligence to enhance cyberattack algorithms and to create autonomous systems capable of identifying vulnerabilities and conducting cyberattacks without direct human intervention, along with the uncontrolled development of "intelligent" digital weapons (Kostenko et al., 2022b).

There is an increasing risk of anonymous large-scale cyberattacks targeting the critical infrastructure of nations and regions. The role of Darkmetaverse (DarkMet) in the use of anonymous "no name" cyber mercenaries, private companies for conducting destructive cyber operations, and the involvement of criminal groups with cyber capabilities are intensifying. This complicates international politics and the procedures for investigating cybercrimes.

## 6. CYBER DIPLOMACY

International politics since February 2022 has been influenced by the fragmentation of the Metaverse, leading to what has been termed as "digital political balkanisation" (Spence, 2018), aligning with geopolitical fault lines. This has given rise to distinct digital political regional segments managed by individual states or groups of states, each with its unique regulations, standards, and policies. For instance, the European Union effectively implements geoblocking mechanisms and imposes mandatory conditions for global compliance with its data protection regulations (GDPR), significantly impacting international trade and relations. The United States is proactively

safeguarding its digital borders against potential cyber threats and espionage, particularly from China and Russia.

"Cyber Diplomacy" has emerged as a novel phenomenon in international politics, introducing a new dimension to international relations. Private organisations and states are negotiating digital standards and Metaverse regulations, potentially forming new types of cross-border trade barriers or gateways, influencing the global economy and security. This includes collaboration between nations to prevent and respond to cyber threats, the formulation of international norms and treaties, the establishment of global standards for personal data protection, internet freedom of expression, and economic cooperation through digital trade rules, e-commerce, and intellectual property protection. The fragmentation of the Metaverse is creating geopolitical tension, instability, and turbulence, exacerbating international and national risks, and restricting access to global markets and services.

## 7. JURISDICTION AND TERRITORIALITY OF METAVERSE

Currently, no nation has fully resolved the issue of territorial sovereignty in the Metaverse. As the Metaverse is a rapidly evolving digital environment, states are just beginning to grasp its potential opportunities and challenges. The complexities of defining territoriality in the Metaverse are discussed in scholarly research on jurisdiction, information law, and the regulation of social relations associated with the use of electronic avatars, artificial intelligence, and electronic personality in the Metaverse (Kostenko et al., 2022a).

Academic debates are presently focused on the practical resolution of Metaverse territoriality. While the Metaverse still closely aligns with national legislation and international law, there is potential for establishing a separate jurisdiction for cyber incidents regulated by national and international law, for instance, through the creation of a distinct electronic jurisdiction and a Metaverse Codes and Laws model.

One direction for jurisdiction development suggests that states exercise sovereign authority over their physical territories and infrastructure and are obligated to oversee the security of information passing through their technical hubs. Thus, international law could impose territorial restrictions on the Metaverse (Tsaugourias, 2018). Another direction supports the idea of projecting the Westphalian system onto the "state structure" of the Metaverse, as it fosters the formation of concepts of sovereignty (Lessig, 2006; Demchak and Dombrowski, 2014), and the equality of states in international law (Lessig, 1998). The concept of the Common Heritage of Mankind (CHM) is also considered, according to which the regulation of cyberspace should be conducted by international law through the creation of international Internet governance bodies and finding a consensus on the application of force and self-defense in the Metaverse (Segura-Serrano, 2006). The most viable hypothesis is considered to be the creation of a single universal electronic jurisdiction of the Metaverse, which could become a single universal transnational electronic body responsible for dispute resolution and the investigation of offenses in the Metaverse (Kostenko et al., 2022a).

A primary challenge in establishing territorial jurisdiction within the Metaverse lies in the lack of technical and legal mechanisms to set physical boundaries, which hampers a state's ability to enforce its laws and complicates the resolution of legal disputes. The absence of specific Internet legislation also contributes to the violation of existing national laws. The anonymity and pseudonymity of internet users fail to provide reliable identification, consequently favouring offenders over state and law enforcement

DOI: 10.46282/blr.2024.8.2.844

agencies. Disputes over territorial jurisdiction positioning in cyberspace are already adversely affecting the validity of court decisions, leading to their annulment.

The uncertainty of national courts' competence creates a legal vacuum, complicating legal relations in the Metaverse and limiting the enforcement of valid court decisions. Legal scholars criticise existing legal systems for their inefficiency in resolving cyber conflicts and suggest specialised rules for addressing them (Adams and Albakajai, 2016; Appazov, 2014).

Meanwhile, individual national legal systems are taking measures to extend their jurisdiction over certain types of offenses in the Metaverse. For instance, the United Kingdom extends extraterritorial jurisdiction over crimes such as child cruelty, sexual offenses, fraud, and terrorism. The Republic of Egypt modernised its national legislation by adopting "The Anti-Cyber and Information Technology Crimes Law," passed in 2018,[1] aiming to expand the fight against crimes in the field of information technology (Abdelkarim, 2023).

Today, some researchers propose to divide the jurisdiction of the Metaverse into the following subgroups (figure 1):

Analogue Law Jurisdiction (JAI) and Electronic Law Jurisdiction or Electronic Jurisdiction (JEL).

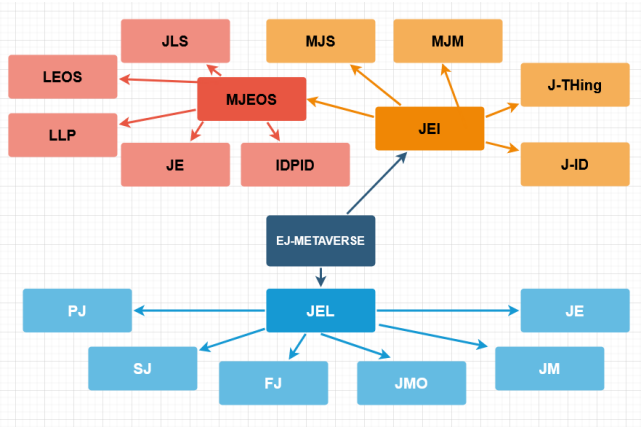


Figure 1. Metaverse jurisdiction

Today's jurisdiction in analog law can be categorised into:

Personal Jurisdiction (PJ) – This type of jurisdiction allows a court to make decisions regarding specific parties or individuals.

Subject Matter Jurisdiction (SJ) – This jurisdiction type empowers a court to hear and resolve cases involving certain subjects.

Financial Jurisdiction (FJ) – Primarily concerns monetary financial matters.

Mandatory Jurisdiction (JMO) – This jurisdiction enables a country to enact laws, particularly concerning the activities, status, circumstances, or choices of an individual (except for laws that conflict with the interests of other countries).

[1] Anti-Cyber and Information Technology Crimes Law «EGYPT» Law (2018).

Judgment Jurisdiction (JM) – Under this jurisdiction, a state has the authority to adjudicate a case concerning a relevant individual in civil or criminal matters, irrespective of whether the state is a party or not - a simple connection between the two is sufficient.

Enforcement Jurisdiction (JE) – This jurisdiction depends on the existence of prescriptive jurisdiction. That is, without mandatory jurisdiction, it cannot be enforced to penalise an individual who violates its laws and regulations (Sharma, 2021).

The jurisdiction of electronic law, or electronic jurisdiction, is currently in the stage of a model or concept of an electronic legal domain, defined by the scope of the application of laws and regulatory acts that govern digital spaces. It encompasses the regulation of social and legal relations arising in digital environments. Electronic jurisdiction covers relationships that do not exist in the analog world, and their regulation is the task of contemporary legal professionals and legislators.

If we consider electronic jurisdiction as a branch of electronic law, it would be prudent to envisage the following types:

Jurisdiction of Identification Data (JID) – This legal domain defines the competence of authorities and entities in managing identification data, including their collection, storage, usage, and protection. A subtype of identification data jurisdiction is actively evolving in the European Union as General Data Protection Regulation GDPR and the United Nations Commission On International Trade Law has created the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (2022).

Jurisdiction of Digital Content and Products (J-thing) – This legal field governs the rights and obligations associated with the creation, distribution, usage, storage, destruction, protection, and obsolescence of digital content and products (things) exclusively in the Metaverse and its variants.

Metaverse Jurisdiction for Interaction with Other Metaverses (MJM) – This area of legal regulation is responsible for the legal structuring of interactions and relationships between different virtual platforms or Metaverses. It encompasses legal aspects related to the creation, management, usage, and interaction of digital spaces that have defined their legal status or legal construction as Metaverse. The legal regulation will address issues of transfer and usage of digital assets (virtual property, avatars, digital tokens) between Metaverses of different legal constructions, rights of electronic users, protection of identification and personal data, electronic intellectual property, and inter-platform interaction variations. This jurisdiction will also be endowed with the power to resolve cross-border conflicts and disputes arising between different Metaverses and electronic platforms, as well as among users of these platforms.

The Metaverse Jurisdiction for Transnational Interaction with Physical States (MJS) is an intricate legal field that integrates both analog and electronic international law to regulate relationships between the virtual worlds of the Metaverse and real-world nations, especially in the context of crossing national borders and jurisdictions. Legal regulation will address issues like intellectual property rights protection, tax and customs obligations, virtual commerce regulation, transfer of identification and personal data, commercial information between virtual and physical realms, and resolving conflicts between Metaverse jurisdictions and national jurisdictions.

The Jurisdiction of Electronic Entities and Objects (MJEOS) is a complex legal field that combines various sectoral and interdisciplinary legal institutions (objects, entities, AGI-endowed entities, avatars, electronic personalities/electronic humanoids, AI, and AGI).

DOI: 10.46282/blr.2024.8.2.844

## 8. A TYPICAL CROSS-BORDER METAVERSE MODEL

The international scientific and public communities face a critical task of developing safe methods for the creation and management of the Metaverse within a transnational space. There is an urgent need to initiate the development of standardised technical and software solutions in areas such as identification, blockchain, cybersecurity, digital content, and assets. However, a key aspect is the formulation of effective national and international regulatory mechanisms, as well as the adaptation of existing legislative norms to regulate the social and legal relationships emerging within the Metaverse. These processes can be successfully implemented through the establishment of an "International Scientific Sandbox for the Metaverse."

Within the framework of this initiative, a priority task will be the development of a "Transborder Model of the Metaverse," which will unify the key components of the ecosystem. This model aims to create a universal platform for formulating norms and laws that will ensure the reliable functioning of the Metaverse. In doing so, it will guarantee its interoperability, integration with the physical world, and alignment with traditional legislation.

The structure of the "Transborder Standard Model of the Metaverse" could consist of the following levels, encompassing these modules (figure ecosystems):

1. Technological Level: This level establishes standard methods and data transmission systems, protocols, interfaces, and foundational modules for creating typical blockchains, mathematical and quantum cryptography, modules for relativistic databases, algorithms for big data, and more.
2. Cybersecurity and Infrastructure Protection Level: This involves a technological module (network perimeter protection, endpoint protection, data protection, monitoring, and incident response), and an organisational module (policies and procedures, staff and AI awareness training, physical security, vulnerability and patch management, regular system checks, and audits), among others.


Figure 2. Transborder Standard Model of the Metaverse

3. Identification and Identity Data Management Level: This level addresses technical identification protocols via external devices, network identification protocols, standards, and unified requirements for identification procedures, as well as dedicated standards for handling personal data. It also includes modules for the security of identification data, control and verification of authenticity, authorised access, preservation, destruction, and data oblivion.
4. Virtual Reality Technologies Level: This involves standards and requirements for software and hardware support of AR/VR/XR/MR technologies, Cloud Computing, avatar creation, digital personalities, virtual objects and entities, digital assets, and other technological solutions.
5. Industrial Metaverse Technologies Level: This level encompasses software and hardware modules for "digital twin" technologies and Industrial IoT (IIoT), as well as technologies ensuring the interoperability of Metaverse/Metaverse and Metaverse/Physical World (PhW).
6. ANI AI, ASI, Machine Learning Technologies Level: This includes technologies and methodologies of Artificial Narrow Intelligence (ANI), Artificial Super Intelligence (ASI), Machine Learning (Supervised Learning, Unsupervised Learning, Semi-Supervised Learning, Reinforcement Learning, Deep Learning, Ensemble Methods), Natural Language Processing, and Big Data.
7. Military Protocols and Regulations in the Metaverse: This covers military regulations and protocols for Metaverse/Metaverse and Metaverse/PhW interactions, as well as the use of VR in military applications and ethically contentious purposes.
8. Legal Regulation Level of Virtual Reality Technologies: This involves the virtual electronic jurisdiction, virtual electronic court, virtual e-criminal code, copyright code for e-intellectual property, and e-property for virtual assets and entities.
9. Sociological and Ethical Issues Level: This addresses privacy and data protection, disorientation and dependency, perception manipulation, content responsibility, social isolation, ethics of virtual world creation, impact on children and youth, mental health risks, identity management challenges, accessibility, and the digital divide.

The proposed model is an abstract representation of systems that is used to understand, predict, and explain the behaviour of a complex of systems under the generalised name Metaverse. This model has a specific structure based on modules or ecosystems that are differently functional in purpose and structure, not related to each other by similar features, but their joint application creates the latest, modern, and unique functionality of virtual environments that requires legal regulation and can become the basis of electronic jurisdiction.

## 9. CONCLUSION AND DISCUSSION

The fragmentation of the Metaverse serves as a catalyst for delineating the boundaries between national sovereignty and the need for global standards. It lays the groundwork for the immediate initiation of cross-border processes to accommodate varying levels of technological advancement and internet access across different countries, as well as for harmonising international standards with a country's domestic legislation.

DOI: 10.46282/blr.2024.8.2.844

The emergence of the "Splinternet" has become a pivotal component of global cyber policy, with profound implications for national security, political control, and the future of the global internet, international relations, and the world economy. The turbulent processes of cyber policy are generating geopolitical contradictions and conflicts among states in cyberspace, where countries strive to isolate their networks from external influences. This development has intensified the struggle for information influence, as states seek to control the flow of information within their borders to maintain political and ideological "stability" and safeguard their national economies from external digital threats.

Consequently, there is an urgent need for the creation of a modern standard cross-border Metaverse model and a unified international legal base to ensure the operation of cross-border virtual reality ecosystems and an electronic jurisdiction system. This need extends to updating and developing national legal bases in response to the ongoing changes in the social, technological, and geopolitical conditions of society.

The necessity for rapidly enhancing the role of international forums and organisations in developing unified rules and norms is pressing. Collaboration between governments, the private sector, academic circles, and civil society in shaping the future of global technological and legal regulation of the Metaverse is of utmost importance.

BIBLIOGRAPHY:

Abdelkarim, Y. A. (2023). Untangling the Jurisdictional Web in Cyberspace. *Journal of Research, Innovation and Technologies*, vol. II, 2(4), 238–246, https://doi.org/10.57017/jorit.v2.2(4).08

Adams, J. and Albakajai, M. (2016). Cyberspace: A New Threat to the Sovereignty of the State, *Management Studies*, 4(6), 256–265. Available at: https://www.davidpublisher.com/index.php/Home/Article/index?id=26237.html (accessed on 03.11.2024).

Aljanabi, M. and Mohammed, S. Y. (2023). Metaverse: open possibilities. *Iraqi Journal For Computer Science and Mathematics*, 4(3), 79–86, https://doi.org/10.52866/ijcsm.2023.02.03.007

Appazov, A. (2014). Legal Aspects of Cybersecurity, University of Copenhagen. Available at:https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf (accessed on 03.11.2024).

Bagheri, M. and Jahromi, M. (2016). Globalization and extraterritorial application of economic regulation: crisis in international law and balancing interests. *European Journal of Law and Economics*, 41, 393–429, https://doi.org/10.1007/S10657-012-9351-2

Crespo-Pereira, V., Sánchez-Amboage, E. and Membiela-Pollán, M. (2023). Facing the challenges of metaverse: a systematic literature review from social sciences and marketing and communication. *Profesional De La información Information Professional*, 32(1). DOI: https://doi.org/10.3145/epi.2023.ene.02

Demchak, C. and Dombrowski, P. (2014). Cyber Westphalia: Asserting State Prerogatives in Cyberspace. *Georgetown Journal of International Affairs, International Engagement on Cyber III*, 29–38. Available at: https://www.researchgate.net/publication/291335219 (accessed on 03.11.2024).

Garrido, G., Nair, V. and Song, D. (2023). SoK: Data Privacy in Virtual Reality. DOI: https://doi.org/10.48550/arXiv.2301.05940

Ghirmai, S., Mebrahtom, D., Aloqaily, M., Guizani, M. and Debbah, M. (2023). Self-Sovereign Identity for Trust and Interoperability in the Metaverse. DOI: https://doi.org/10.48550/arXiv.2303.00422

González, H. C. A., Kauffer, E., Koff, H. and Maganda, C. (2023). Enhancing challenged integration. *Regions and Cohesion*, 13(1), v–vi, https://doi.org/10.3167/reco.2023.130101

Gosztonyi, G. (2023). The Rise of Digital Authoritarianism Across the Globe. *Censorship from Plato to Social Media. Law, Governance and Technology Series*, vol. 61, 157–168, https://doi.org/10.1007/978-3-031-46529-1_11

Kalyvaki, M. (2023). Navigating the Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction. *Journal of Metaverse,* 3(1), 87–92, https://doi.org/10.57019/jmv.1238344

Kostenko, O., Furashev, V., Zhuravlov, D. and Dniprov, O. (2022a). Genesis of Legal Regulation Web and the Model of the Electronic Jurisdiction of the Metaverse. *Bratislava Law Review*, 6(2), 21–36, https://doi.org/10.46282/blr.2022.6.2.316

Kostenko, O., Jaynes, T., Zhuravlov, D., Dniprov, O. and Usenko, Y. (2022b). Problems of using autonomous military AI against the background of Russia's military aggression against Ukraine. *Baltic Journal of Legal and Social Science,* (4), 131–145, https://doi.org/10.30525/2592-8813-2022-4-16

Kostenko, O., Zhuravlov, D., Dniprov, O. and Korotiuk, O. (2023a). Metaverse: Model Criminal Code. *Baltic Journal of Economic Studies*. 9(4), 134–147, https://doi.org/10.30525/2256-0742/2023-9-4-134-147

Kostenko O. V. and Golovko, O. M. (2023b). Electronic Jurisdiction of the Metaverse: Challenges and Risks of Legal Regulation of Virtual Reality. *Information and law*. 1(44), 102–105. Available at: http://ippi.org.ua/kostenko-ov-golovko-om-elektronna-yurisdiktsiya-metaverse-vikliki-ta-riziki-pravovogo-regulyuvannya (accessed on 03.11.2024).

LawBhoomi. Prachi Sharma (2021). Concepts and Issues of Jurisdiction in Cyber Space. Available at: https://lawbhoomi.com/jurisdictional-aspects-in-cyber-law-and-information-technology-act/ (accessed on 03.11.2024).

Lessig, L. (1998). The Laws of Cyberspace. Taiwan Net '98 Conference. Available at: https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf (accessed on 03.11.2024).

Lessig, L. (2006). Code: version 2.0. Basic Books: New York, 2006. Available at: https://archive.org/download/Code2.0/Code_text.pdf (accessed on 03.11.2024).

Luts, L., Nastasiak, I., Karmazina, C. and Kovbasiuk, S. (2021). Prospects for the development of modern interstate legal systems in the context of globalization challenges. *Journal Amazonia Investiga*, 10(40), 233–243, https://doi.org/10.34069/AI/2021.40.04.23

Moldovan, C. (2021). Suveranitatea digitală – viitorul spaţiului virtual? Is Cybersovereignty the Future of Cyberspace? *Analele Ştiinţifice ale Universităţii «Alexandru Ioan Cuza» din Iaşi.* Tomul LXVII, supliment 2, Stiinţe juridice, 2021. 271–284. DOI: 10.47743/jss-2021-67-4-19. Available at: http://pub.law.uaic.ro/files/articole/2021/vol.2_2/19.moldovan.pdf (accessed on 03.11.2024).

Mystakidis, S. (2022). Metaverse. *Encyclopedia*. 2(1), 486–497, https://doi.org/10.3390/encyclopedia2010031. Available at: https://www.mdpi.com/2673-8392/2/1/31 (accessed on 03.11.2024).

Park, S. and Kim, Y. (2022). A Metaverse: Taxonomy, Components, Applications, and Open Challenges. *IEEE Access*, 10, 4209–4251, https://doi.org/10.1109/ACCESS.2021.3140175

Qin, H., Wang, Y. and Hui, P. (2022). Identity, Crimes, and Law Enforcement in the Metaverse. ArXiv, abs/2210.06134, https://doi.org/10.48550/arXiv.2210.06134

Ramírez-Herrero, V., Ortiz-de-Urbina-Criado, M. and Medina-Merodio, J.-A. (2023). La revolución del metaverso: análisis crítico de sus luces y sombras. *ESIC Market*, 54(3), e334, https://doi.org/10.7200/esicm.54.334

Rawat, D. B. and Hassan El alam (2023). Metaverse: Requirements, Architecture, Standards, Status, Challenges, and Perspectives. DOI: https://doi.org/10.48550/arXiv.2302.01125

Sebastian, G. (2023). A Descriptive Study on Metaverse: Cybersecurity Risks, Controls, and Regulatory Framework. *International Journal of Security and Privacy in Pervasive Computing (IJSPPC),* 15(1), 1–14, https://doi.org/10.4018/IJSPPC.315591

Segura-Serrano, A. (2006). Internet Regulation and the Role of International Law. *Max Planck Yearbook of United Nations Law*, 10, 191–272. Available at: https://www.mpil.de/files/pdf3/06_antoniov1.pdf (accessed on 03.11.2024).

Stănilă, L. (2023). On the curiosities of the future: meta criminal law. *SHS Web of Conferences*, https://doi.org/10.1051/shsconf/202317703001

Tai, K. and Zhu, Y. Y. (2022). A historical explanation of Chinese cybersovereignty. *International Relations of the Asia-Pacific*, 22(3), 469–499, https://doi.org/10.1093/irap/lcab009

Tsaugourias, N. (2018). Law, Borders and the Territorialization of Cyberspace. *Indonesian Journal of International Law*, 15(4), article 5, 523–551, http://dx.doi.org/10.17304/ijil.vol15.4.738

Vidyarthi A. and Hulvey, R. (2021). Building Digital Walls and Making Speech and Internet Freedom (or Chinese Technology) Pay for It. *Indian Journal of Law and Technology,* 17, 1–42. Available at: https://www.ijlt.in/_files/ugd/066049_a45f48ddbdd54fad8b13a25ec3aadeeb.pdf (accessed on 03.11.2024).

Wang, Y., Su, Z. and Yan, M. (2023). Social Metaverse: Challenges and Solutions. DOI: https://doi.org/10.48550/arXiv.2301.10221

Wensheng G., Zhenqiang Y., Shicheng W. and Yu, P. S. (2023). Web 3.0: The Future of Internet. *Companion Proceedings of the ACM Web Conference 2023 (WWW '23 Companion)*. New York: Association for Computing Machinery, 1266–1275, https://doi.org/10.1145/3543873.3587583

Anti-Cyber and Information Technology Crimes Law «EGYPT» Law (2018).

Council on foreign relations. Blog Post by A. Michael Spence (2018). Preventing the Balkanization of the Internet. Available at: https://www.cfr.org/blog/preventing-balkanization-internet (accessed on 03.11.2024).

Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the proc easing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016).

UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (2022).

DOI: 10.46282/blr.2024.8.2.844