BRATISLAVA LAW REVIEW

PUBLISHED BY
THE FACULTY OF LAW,
COMENIUS UNIVERSITY
BRATISLAVA

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

GENESIS OF LEGAL REGULATION WEB AND THE MODEL OF THE ELECTRONIC JURISDICTION OF THE METAVERSE / Oleksii Kostenko, Vladimir Furashev, Dmytro Zhuravlov & Oleksii Dniprov

Oleksii 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

Vladimir Furashev, 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
vfurashev@gmail.com
ORCID: 0000-0001-7205-724X

Dmytro Zhuravlov D.Sc.
Office of the President of Ukraine,
Bankova 11, 01220 Kyiv;
Ukraine
ndz0909@gmail.com
ORCID: 0000-0002-2205-6828

Oleksii Dniprov, D.Sc.
Institute of Public Law
Office of the President of Ukraine
Bankova 11, 01220 Kyiv;
Ukraine
osdniprov@gmail.com
ORCID: 0000-0002-7157-9748

Abstract: *The study examines the transformation of scientific views and approaches to the problem of expediency and necessity of legal regulation of public relations, emerging from the evolution of the world system of public electronic resources in the transmission of information and Internet data from Web 1.0, Web 2.0 to Web 3.0. The stages of formation of the role and place of electronic jurisdiction in public relations are also investigated. Legal regulation of modern relations in virtual and augmented reality environments with the use of Web 3.0 technologies is not available today. At the same time, there are precedents for the application of certain provisions of analogue law to address legal uncertainties in the virtual environment, such as establishing ownership of virtual non-property assets, buying/selling of virtual non-property assets, liability for misappropriation of virtual non-property assets, etc. Obviously, the problem of legal regulation by the rules of analogue law in the virtual environment cannot be fully addressed. The solution to this problem is possible by creating a comprehensive e-jurisdiction and developing the Metaverse Grand Charter of Laws to regulate public relations in the meta-universe and to establish new branch of e-law. Given the urgency of the problem, the model of e-jurisdiction Grand Charter of Laws Metaverse is proposed. The model of complex electronic jurisdiction of Metaverse will allow to create basic conceptual apparatus, doctrinal and normative and legal concepts, to define objects and subjects of legal relations in Metaverse, to establish the basic forms of legal relations and mutual relations in Metaverse. This, in turn, will be the basis for reforming analogue legislation, partial interoperability in the digital environment and the development of new regulations in various areas of law and will stimulate the establishment of new e-jurisdiction. The study proposes the construction and basic elements of electronic jurisdiction, mechanisms for the separation of electronic offences and interaction with analogue jurisdictions. E-jurisdiction of the Metaverse Grand Charter of Laws will provide legal regulation of public relations both directly in Metaverse and in public relations related to the analogue and electronic world.*

Key words: *Metaverse; Cyberspace; Electronic Personalities; Avatars; Digital Humanoids; Electronic Jurisdiction; Web 3.0 Decentraland; Virtual Reality; Augmented Reality; AI; ASI; Cyber Laws; Laws Metaverse*

Suggested citation: Kostenko, O., Furashev, V., Zhuravlov, D. & Dniprov, O. (2022). 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

Submitted: 05 November 2022
Accepted: 08 December 2022
Published: 30 December 2022

1. INTRODUCTION

Historically, our civilization has passed three communication epochs – verbal, when information in the society was transmitted only orally; verbal and sign, where information was transmitted both verbally, and by means of special symbols, meaning letters, words, actions, and events; verbal and written, during which printed literature appeared. Today, humanity has entered the fourth epoch, an era dominated by electronic communication, where integrating information and communication technologies with previous forms of communication.

This epoch has also gone through a path of transformation from archaic computers to meta-universal technology. Metaverse becomes not only an advancing era of communication, but it also becomes a new scientific and technical centre for the development of society, a battery and a designer of modern technologies, a generator of new suppleness, a tool for helping people to survive. It becomes an independent medium, functioning in parallel with the physical world and laws, which requires a certain rethinking in the current society (Shaoying et al., 2022).

The future Metaverse will become a large open scalable system. This system is being created simultaneously covering cyberspace, hardware terminals, different manufacturers and users, providing a wide range of application scenarios in virtual and augmented reality (AR/VR-environments), demonstrating the ultimate form of a super ecosystem. However, without proper legal regulation, the territory of «virtual freedom» can turn into a destructive tool. Only with the support of the law, it is possible to ensure legal regulation of social relations in the metaverse (Pengfei, 2022).

In the present, a handful of different meta-worlds are functioning: Horizon Worlds, Ceek city, Baidu Xi Rang, Metaverse Facebook, Decentraland (Ethereum), Emirates Metaverse, Expanded Virtual World, Qualcomm Nvidia Omniverse iz zasusvannymi technologies AI, AR / VR, holograms, XR-platforms, distribution registers, neural networks, quantum technologies and other technical solutions.

Obviously, the regulation of legal rights in Metaverse is considered a dividing line between electronic gaming software and application products. The legal regulation itself is fragmented and situational, applying existing analogous laws and regulatory acts such as codes, regulations, and standards.

Besides, there is a practice of conducting «experimental legal regimes», known worldwide as «regulatory sandboxes» or «legal incubators», in which the Government determines special legal regulation for a valid period in certain areas for the development of AR/VR environment.

The practice of using metaverses has already had several precedents for the application of certain provisions to resolve legal uncertainties in the virtual environment, such as establishing ownership of virtual intangible assets, buying/selling virtual intangible assets, liability for misappropriation of virtual assets with the signs of various types of discrimination and moral violence, the spread of ideologies of racism and fascism, etc. At the same time, there are more and more types of torts that have a nature exclusively in the Metaverse and should be regulated exclusively within the Metaverse.

Besides, a new perspective acquires the problem of legal regulation of the use of identity (personal) data, which will become the basis for the creation and functioning in the metaverses of virtual avatars or electronic humanoids.

Given the urgency of the problem, there is a need to create a single model of e-jurisdiction, based on which to develop the legislative framework for Metaverse.

Nowadays, this approach is unique, and the proposed Model of Integrated Electronic Jurisdiction Metaverse should become the basis not only for scientific discussions but also for the research in law in order to create initial model legislation that should provide legal regulation of public relations in Metaverse, as well as to launch the digital transformation of analogue legislation.

2. LEGAL REGULATION OF PUBLIC RELATIONS IN THE ELECTRONIC ENVIRONMENT AT THE STAGE OF TECHNOLOGY DEVELOPMENT WEB 1.0

The late 1990s and early 2000s saw the development of information and communication technologies related to the dissemination of information over the Internet. At that time, the environment of electronic resources was a static website designed for reading and viewing – Web 1.0. These information resources did not have interactive elements, multimedia, and did not have the features that allowed users to communicate online, share files, etc. The website creation tool was a number of HTML markup language tags that performed the design function. Besides, the speed of the Internet connection was not enough to transfer images and videos.

At the same time, many scientists saw in this technology the prospects not only for the application in broad fields of science and technology, but also for the formation of new social relations different from the existing ones. The scientists hoped that Web 1.0. and the Internet will allow the society to create new environment free from the state domination or not burdened by excessive legal requirements. This view was formed under the influence of the Declaration of the Independence of Cyberspace, authored by John Barlow and «Code and other laws of cyberspace» by the researcher Lawrence Lessig. In the Declaration, the author presented cyberspace as the space of such power that is necessary for the establishment of freedom. In fact, John Barlow (1996) has declared that cyberspace is a liberal virtual extraterritorial enclave that is not subject to any State jurisdiction and is designed for people free from any privileges and discrimination that completely denies State interference in cyberspace.

At the same time, L. Lessig (1999a) defined that cyberspace is inevitable, but unregulated, and society in the real world is governed by four main regulators: law, social norms, market relations and «architecture/code» (technological capabilities). No nation can live without it, but no nation can control behaviour in cyberspace. Cyberspace is a place where people are free from real control.

In our opinion, according to the technological capabilities of the time and the state of public relations, L. Lessig (1999b) considered the key regulator of cyberspace its architecture, technical components or capabilities, or «code». It is the code that determines the order of cyberspace use, just as public relations in real space are subject to public administration. L. Lessig argues that, in a fundamental sense, the code of cyberspace is its constitution. The code sets out the conditions under which people gain access to cyberspace and sets the rules that control their behaviour. The code forms its own sovereignty, which is an alternative to real physical life.

In his essay, L. Lessig (1998) highlighted for the first time the need for laws that would simultaneously ensure the regulation in cyberspace and minimize restrictions on human rights and freedoms. Analysing this book, Ana Viseu (2001) identifies that L. Lessig offers several ways to deal with the «gloomy» future: open source and development of legislation. According to L. Lessig, open source should act as a kind of constitutional review, ensuring that all citizens can «read» and influence the «created» surrounding environment. Legislative actions lie in the adaptation of the Constitution (US)

DOI: 10.46282/blr.2022.6.2.316

to cyberspace to ensure that the values we experience today will be preserved in cyberspace.

Today, this approach can be called an attempt to «soft» or democratic regulation of cyberspace, which is mainly based on creating a legal basis for the use of certain technologies and provides almost no legal regulation of public relations.

At that time, the development of state legislation regulating cyberspace took place in two main areas: making changes and supplements to criminal codes and drafting legislation by developing a number of separate legislative acts.

The first direction was implemented by Canada, Estonia, Germany, Sweden, Finland, Austria, Italy, Latvia, the Netherlands, Spain, Poland, and Ukraine. For example, Ukraine has introduced a separate section «Criminal offenses in the use of electronic computers, systems and computer networks and telecommunications networks» in articles 361 – 363 and 363¹ of the Criminal Code.

The following countries are worth noting regarding the creation of separate legislation. Thus, in 2000, the Republic of India adopted the Information Technology Act, which provides legal regulation in the area of information and communication technologies and electronic signature technologies. This Law is interesting by the introduction of the special Cyber Appellate Tribunal to deal with offenses committed using modern cyber technologies. Besides, this Law introduces the classification of a number of crimes, including computer distribution of child pornography, electronic fraud and cyberterrorism, which provides for the use of State coercion in the form of fines or restraint of liberty (Articles 66, 66A-66E, 67, 67A-C, 71-79).

The US has passed provisions on controlling the assault of non-solicited pornography and marketing (15 U.S.C. §§ 7701-7713 (2003)), on fraud and related activity in connection with access devices (18 U.S.C. § 1029 (2015)), on fraud and related activity in connection with computers (18 U.S.C. § 1030 (2020)), on fraud and related activity in connection with electronic mail (18 U.S.C. § 1037 (2003)), on wire and electronic communications interception and interception of oral communications (18 U.S.C. §§ 2510-2523 (2022)), and on stored wire and electronic communications and transactional record access (18 U.S.C. §§ 2701-2713 (2018)).

During this period, other countries adopted laws: the Israeli Computer Law (1995), UK Computer Misuse Act (1990) and French Act Relating to Data Processing, Files and Freedoms (1978).

As one can see, society and the State reacted differently to the emergence of information and communication technologies Web 1.0. On the one hand, we have a position of formation of liberal approaches of «soft» regulation of cyberspace; on the other hand, the State, as the regulators of public relations, establish or authorize universally binding rules that, in a sense, restrict civil rights and freedoms, but these rules are ensured by the measures of the State influence, including State coercion.

3. DEVELOPMENT OF «ELECTRONIC» LEGISLATION OF THE PERIOD OF WEB 2.0 TECHNOLOGIES

Since 2004, the term «Web 2.0» has become widespread as one that characterizes the next stage in the development of information and communication technologies. In the future, it will often be used along with the term «scientific and technological revolution 4.0», as they describe the significant changes in society that occur as a result of its digitalization.

The term Web 2.0 means a comprehensive combination of technologies such as high-speed Internet protocols, fifth-generation mobile (5G), and the many standards of

wireless networks, interactive Web sites, resources, and platforms. The main difference between Web 2.0 and Web 1.0 is that content is created and produced by the users who are both consumers of content and are not owners of technical resources. At the same time, the emergence of Web 2.0 as an environment free from State domination and unencumbered by excessive law has been characterized by the emergence of the darknet network, cybercrime, malware, anonymous hackers, cryptocurrency, pirated content, destructive information, etc.

At the same time, «electronic» legislation was actively and proactively developed – national and international legislation in the sphere of information, criminal, civil, administrative law, intellectual property law and technical regulation of information and communication technologies through regulations, rules, certification, etc. For example, the regulation of the use of the IoT devices is carried out simultaneously with the introduction of technical and legal regulation (Kostenko, 2021b) and the governance of the use of AI is formed by many countries in accordance with the adopted AI Development Strategies (Zhang et al., 2021, 2022).

A significant number of international documents on the information society have been developed and adopted at the initiative and participation of non-governmental organizations. In solving infrastructure issues of Internet organization, the position of sovereign is has not always been and is the main priority. Effective regulators of the global information society have been the tools of soft international law, which, although not binding, are extremely responsive to new challenges and reflect the interests of all relevant actors. However, non-binding rules have a significant normative and convincing value. That is, technological innovations should be taken into account when developing the relevant regulations (Kyryliuk, 2015). For example, Ukraine for some time did not rush to develop modern legislation in the sphere of information technology and was rather slow in digitizing both public authorities and recodification of current legislation. However, the Parliament has recently developed and adopted a number of modern legal acts such as the Act on Protection of Information in Information and Communication Systems (1994), the Act on Electronic Trust Services (2017), the Act on The Main Principles of Ensuring Cyber Security of Ukraine (2017), the Act on Critical Infrastructure (2022), the Act on Virtual Assets (2022) and the Order of The Cabinet of Ministers on The Approval of The Concept of The Development of Artificial Intelligence in Ukraine (2020). In 2019, the Ministry of Digital Transformation of Ukraine was established, which is tasked with digitizing public authorities and mechanisms of public administration. The judicial system of Ukraine introduces such digital mechanisms as electronic judiciary and electronic registers.

Modern global legal regulation of cyberspace has significant achievements, but they are offset by two problems:

1. focus of the law to the formation of legal responsibility for cybercrime, as special types of crime committed with the use of digital tools in the national and cross-border information and communication environment (Riek and Böhme, 2018);
2. the absence of a single transnational law that would ensure public relations not only at the national but also at the transnational level (Razmetaeva, Ponomarova and Bylya-Sabadash, 2021), in which the postulate that jurisdiction should not be attached to a certain territory or borders is gradually gaining public importance, and technical possibilities for regulating cyberspace are limited both objectively and subjectively (Vartanian, 2000).

DOI: 10.46282/blr.2022.6.2.316

Nowadays, academic debates revolve around the issue of the territoriality of cyberspace as a whole and its individual elements. As cyberspace now functions, its relation to the borders, national and international law is still sufficiently clear and proportionately dependent. There is a real possibility of separating cyber incidents in the jurisdictions of national and international law. That is, physical boundaries are still identical to regulatory boundaries, and law performs the vast majority of its functions within these borders, namely: economic, political, ideological, cultural and educational, regulatory, educational, protective and preventive ones, taking into account national characteristics.

N. Tsaugourias (2018) states in his study that the state extends its sovereignty to the physical level, i.e., to the infrastructure located on its territory. The state exercises sovereign authority in its territory. The state can also defend its control over cyberspace and cybercrime that takes place on its territory. Besides, the state is obliged to defend its sovereignty, including information one. That is, it not only entitled, but also obliged to control the security of information that passes through its infrastructure, which takes place or terminates s on its territory, or is transmitted through national technical hubs. This shows that under existing international law, the rules of territorial limitation may extend to cyberspace in its present form. The difference between the physical world and cyberspace is that the authority in the physical world is organized and operates in certain territories, while in cyberspace the authority is direct, not fragmented, or identical to the boundaries of cyberspace. People can transfer certain activities and actions to cyberspace, they can nominally/virtually populate cyberspace, but they can never remove themselves from the real world in real life. This means that cyberspace and its organization cannot be independent of the States and therefore cyberspace cannot be sovereign, because power in cyberspace is mediated by the States.

That is why many researchers such as P. Dombrowski, Ch. Demchak, L. Lessig, I. Shumsky and others are inclined to the projection of the Westphalian system on the «state structure» of cyberspace, because thanks to it the concept of sovereign State and its basic features, principles of equality in relations in the system of international law were formed; the institution of international guarantees, equality of States, the concept of sovereignty, the solution of international problems by peaceful means were introduced (Demchak and Dombrowski, 2014; Shumskiy, 2020). At the same time, A. Segura-Serrano (2006), analysing the current legislation, proposes the concept of the Common Heritage of Mankind (CHM), according to which the regulation of cyberspace should be carried out by international law. The concept of the CHM provides for the need to establish international Internet governance agencies, consensus-building on intellectual property and rights protection, privacy issues, the use of force and self-defence in cyberspace.

The future of e-justice in cyberspace is a separate issue. So far, there are many examples of successful solutions concerning local electronic court systems, such as in the Federal Republic of Brazil, the People's Republic of China, and others.

E. Keddell (2019), Y. Razmetaeva and S. Razmetaev (2021) correctly stress on certain risks of e-justice, which lies in the difficulties of synchronous integration of basic electronic tools into national justice systems, as well as possible bias of electronic justice algorithms. Moreover, this may be an intentional bias that was incorporated by the developers, or an unintentional bias that duplicates the prejudices developed in analogue justice.

An example of risky justice is the study of N. J. Gervassis (2004). He shares the L. Lessig's theory of cyberspace law based solely on cyberspace code and proposes the use of the CyberLaw protocol. CyberLaw is a re-designed network protocol in accordance with the rules of existing legal systems, which is transformed into an alternative form of

indirect «invisible» legislation. That is, part of the legal risks in cyberspace is blocked and corrected by the CyberLaw protocol at the stage of their establishment. It should be noted that the author himself acknowledges that this approach has great potential for abuse in the case of misapplication.

4. METAVERSE STRUCTURE BASED ON WEB 3.0 TECHNOLOGIES

Today we are observers, participants and users of the latest information technologies, which are already generically called Web 3.0. Web 3.0 technologies are information and communication decentralized electronic virtual eco-networks that operate on the basis of blockchain, electronic neural networks, machine learning, AI, IoT, semantic web, cryptocurrency, virtual and augmented reality, continuous availability. According to the research by E. Özkahveci, F. Cívek and G. Ulusoy (2022), the term «metauniverse» is now the most popular term, has many interpretations and is used to describe digitization processes in almost all spheres of human life.

Web 3.0 is the launching pad for the beginning of the scientific and technological revolution 5.0 and the next stage of human development – electronic humanoids and the metaverse. An unambiguous definition of the metaverse is not accepted.

The Metaverse or Decentraland characterizes an infinite number of virtual worlds, in which and between which physical and digital subjects and objects interact socially; the latter are endowed with certain properties: rights, duties and responsibilities. The key element of the Decentraland is the identification of physical and digital subjects and objects. Identification data is a pass to the Metaverse.

Taking into account the main features of post-industrial society and the trends of the transition period to it from industrial society, we can predict that the Metaworld will undergo the following three phases of development:

- the first phase – the shell of the Metaverse (basic level software and engineering), the actors and objects completely dependent on the developers and owners of the shell;
- the second phase – the shell of the Metaverse, the actors and objects belong to the developers and partly belong to the owners / users;
- the third phase – the Metaverse does not belong to specific developers, the management of actors and objects is carried out either by the owner (hardware bio identification) or autonomously (actors and objects are endowed with functionality and rights inherent in the owner).

Only individuals will be considered the actors of the Metaverse, and the category of objects will include legal entities, avatars, electronic personalities, AAI and ASI virtual digital works, digital humanoids, intangible electronic assets of all forms and types, etc. It is likely that in the third phase of the Metaverse the development of a number of objects such as avatars, electronic personalities, virtual digital works of the ASI class and digital humanoids will be transferred to the category of the actors, as at the legislative level they will be endowed with certain rights and responsibilities inherent only in the actors.

Currently, the Metaverse is undergoing the initial stage of its establishment and development (Özgökçeler, 2021). Its structure can be classified as interconnected technology information domains or electronic information corporations. Metacorporations compete in the fight for the user, finance, products and technology. The users of corporate meta-universes still can be anonymous or use aliases to register accounts and create impersonal avatars or e-personalities (Kostenko, 2022), and this reduces trust in the Metaverse as a whole and leaves grounds for abuse and wrongdoing.

DOI: 10.46282/blr.2022.6.2.316

In our opinion, in the near future, the Metaverse will be more structured and will consist of the following elements: Personal Metaverse (PM), Collective Metaverse (CM), Corporate Metaverse (CorpM), Confederate Metaverse (CfM), State Metaworld (SM) and Megametaverse (MMV / WM).

Personal Metaverse (PM) means that each individual (actor of the Metaverse) can create his/her own electronic Metaverse (avatar, electronic humanoid, electronic personality) according to the personal imagination and be in it consciously and exclusively personally, for example, by analogy with the novel «Robinson Crusoe» by English writer Daniel Defoe.

Collective Metaverse (CM) is a voluntary electronic association of the actors and objects of the Metaverse, which operates by mutual agreement, but with mandatory compliance with generally accepted basic requirements or rules of MMV law.

Corporate Metaverse (CorpM) is a voluntary, industrial, scientific, commercial, religious or other electronic association of entities and objects of the Metaverse, which operates under corporate rules as long as they do not contradict generally accepted basic requirements or rules of MMV.

Confederate Metaverse (CfM) is a political union of the actors and objects of the Metaverse, each of which retains its independence, and all together respect the mutually agreed rules of law.

State Metaworld (SM) is an electronic State having the external and internal electronic characteristics of the State, as well as electronic substantive-spatial, informative-public, regulatory and institutional features.

Megametaverse or Whitemetaverse (MMV or WM) is a common decentralized electronic space, in which there are many personal, collective, corporate, confederate and State Metaverses that interact with each other under WM law.

It is advisable in the Metaverse to also enable Darkmetaverse (DarkMet) as required antagonistic element in the meta-universe, in which actors, objects and meta-universes with a self-governing system different from the one adopted in WM can be concentrated.

Since the Metaverse is considered to be an information and communication social ecosystem that creates, maintains, develops and ensures the functioning of public relations in electronic virtual form, it is appropriate to note that the electronic jurisdiction» of the Metaverse is a complex branch of law that regulates social relations that make up its subject matter – social relations in the metauniverse, as well as between the metauniverse and the physical world (Wyss, 2022). Each actor will have personal three-dimensional unique avatar, and the actors / objects will have unique property passports. Actors and objects can perform various activities – financial, scientific, creative, social, public ones, etc.

For example, the Republic of Barbados announced in 2021 that it will open its next embassy in the Metaverse, whose diplomatic complex is being built in Decentraland. The Barbados ambassador to the United Arab Emirates argued that «governments can act together when land is no longer physical land and restrictions are no longer part of the equation». He also noted that small countries do not have physical and financial capacity to support 197 diplomatic missions around the world, but the Metaverse ensures parity with such large countries as America or Germany. Other countries also have experience of virtual embassies – Sweden and Estonia have opened embassies in the Metaverse Second Life.

The United Arab Emirates has already become a leader in the Metaverse, building a modern digital economy, implementing policies and developing a regulatory framework in such areas as virtual assets, artificial intelligence and data protection.

Thus, the UAE State Regulatory Authority of the Virtual Asset Management Authority of Dubai (VARA) has opened a representation in the virtual world of The Sandbox, which will work with the private sector and relevant government agencies to establish legislative and oversight framework for digital assets. Besides, anti-money-laundering regulations and tracing of cross-border transactions will be formulated to ensure transparency and security for businesses and investors. Digital assets such as cryptocurrency, non-interchangeable tokens (NFT), etc. will be supported by a single legislative and regulatory framework.

In mid-April 2022, Emirates announced the creation of a brand in the sphere of metaverses (Emirates Metaverse), as well as collectible and useful indispensable tokens for its customers and employees.

In 2022, the world's first customer service centre developed by the UAE Ministry of Health and Prevention appeared in the Metaverse.

As the reality shows – social relations in the Metaverse are created, established and developed against the scepticism of individual scientists, experts and politicians.

5. PROBLEMS OF LEGAL REGULATION OF PUBLIC RELATIONS IN METAVERSE

The difference between the current cyberspace WEB 2.0 and the Metaverse of WEB 3.0 is that the vast majority of processes and procedures in modern cyberspace are governed by laws and regulations, including a certain range of public relations. However, in view of the above, it is the processes of modelling / predicting the transformation of existing and the establishment of new social relations in the Metaverse that need special attention, namely, to determine their direction and characteristics. This forms the basis for the establishment of mechanisms and means of their legal regulation. Besides, one has to decide on the following:

- what exactly will be considered «social relations in the Metaverse» and «relations in the Metaverse»;
- when, how and to what extent, electronic actors and objects are granted rights specific to an individual;
- what form of justice will be applied in the Metaverse.

Already, electronic personalities, avatars and electronic humanoids can qualitatively duplicate the appearance and behaviour of both the imaginary person and the real owner of the avatar or its user. Identical reproduction of a person, a real person is no longer considered the prerogative of medicine and requires reliable control over the use of human identification data of the «red» group (according to the author's classification) (Kostenko, 2021a) or hypersensitive personal data (according to the GDPR classification).[1] Virtual assets, smart contracts, NFT, virtual lands (Decentraland and The Sandbox meta-universes) are real electronic intangible assets of the Metaverse, with which very real, legally significant actions are being taken. The rules and norms of behaviour in the Metaverse are still being created by projection of the physical world and are of corporate nature. However, the trend of migration and transfer of the norms of public morality in the Metaverse by simulating cosmopolitan e-social relationships in the absence of clear attributes of the electronic state and the state structure of the Metaverse.

[1] EU Regulation on The Protection of Natural Persons with Regard to The Processing of Personal Data and on The Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (2016).

DOI: 10.46282/blr.2022.6.2.316

From virtual to real: it is no longer about imitating the real world, but about self-development based on the virtual world, which can not only shape a system of values independent of the real world, but also affect the real world (Pu et al., 2022).

The main problem of legal regulation of public relations in Metaverse is the lack of a single legal mechanism for regulating public relations arising in the Metaverse.

Establishing the mechanisms for the legal regulation of public relations in the Metaverse should solve many legislative problems related to differences in regulations of various jurisdictions. Most legal systems have existing archaic regulations, which are formulated without taking into account the possible emergence of social relations with the use of electronic technologies of the Metaverse. In some cases, these laws may regulate certain issues of information technology use, but their scope is often either narrow or ambiguous, creating a situation of legal uncertainty.

Modernizing national legislation to ensure legal compatibility across multiple jurisdictions is often replaced by temporary rules or regulations. At present, the legal institutions of national legal doctrines still have the levers to regulate general processes of digitalization of society. Individual cases of «electronic offenses» are considered by the judicial system through the projection of existing law, thus forming the basis for future e-justice in the Metaverse. Different cultural features and state priorities lead to significant differences in motivation and verdicts, and modern legislation, although progressive in nature, does not have full practical application or become fictious laws that are declarative in nature.

However, certain Metaverse technologies already exist and need to be regulated as they form new social relations, in which there are actors and objects, including those with the properties of actors.

So far, these properties are artificially created by the developers and are formed by them according to their imagination or the imagination of scientists or project customers.

E-justice, as well as generally accepted legislation, is absent in the Metaverse in general, or its role exploits certain provisions of local, national regulations and traditional "analogue" justice, very slowly transforming in accordance with the development of electronic public relations in the Metaverse.

6. METAVERSE E-JURISDICTION MODEL BASED ON WEB 3.0 METAVERSE TECHNOLOGIES

The establishment of law in the Metaverse objectively begins with the stage of projection of the laws of physical society on electronic social relations. But, given that the Metaverse is comprehensive, the projection of the laws of different countries will not have the desired effect. It is the advanced development of the relevant basic provisions of the global electronic legislation of the Metaverse that will provide an impetus for the modernization and improvement of national legislation in the area of optimizing and improving the efficiency of its use.

Legal regulation of public relations in the Metaverse requires the development of a comprehensive electronic jurisdiction grounded on the latest basic legislation – the Grand Charter of Laws Metaverse (GLM). In our opinion, GLM should include the following key parts:

- Constitution. The Great Charter
- General norms, composition of the laws of the Grand Charter
- WM Common law
- WM Judicial system WM

- WM e-Office Act
- Mode of cross-border interaction in WM
- Code of fundamental technical regulations
- Certificate of identity management
- Code of Non-property Electronic Assets
- Criminal Electronic Code
- Code of Cyber Defence
- Military regulation
- WM Grand Electronic Judicial Code
- Other regulations.

E-jurisdiction, e-justice is one of the key elements of e-public relations in the Metaverse. E-justice, at the initial stage, can be based on traditional "analogue" justice, which is transformed in accordance with the development of electronic social relations in the Metaverse.

The creation of mechanisms for the legal regulation of public relations in the Metaverse should solve many legislative problems related to differences in regulations of various jurisdictions governing the use of information and communication technologies, identification procedures, copyright, ownership of non-property assets, liability for damages, the list of crimes and coercive State measures for their commission.

Current «analogue era legislation» should be taken as a basis and begin to form the Grand Charter of Laws Metaverse.

The Constitution, the Charter, the common law, the judiciary should have the structures that maximize democratic and legitimate functioning of the WM.

The set of fundamental technical regulations are technical and legal documents that should fix the reference program codes, which will be used to determine the legal status and ownership of non-property electronic assets, such as NFT or content, at the legislative level.

The Code of Non-property Electronic Assets is intended to regulate relations with non-property assets and to establish electronic property rights and electronic intellectual property rights.

DOI: 10.46282/blr.2022.6.2.316

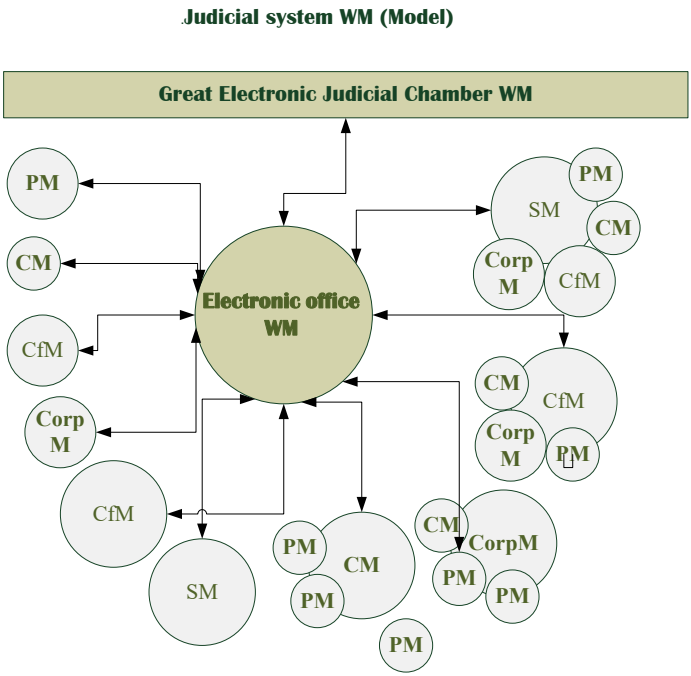

Fig.1 Judicial system WM (Model).

The Criminal Electronic Code is designed to identify the types of offenses with the development and use of information and communication technologies and technologies of the Metaverse, as well as establishment of State and other coercive measures in the case of offenses. The Cyber Security Code is a technical and legal document that should establish reference programs, administrative, managerial, and technical measures to ensure cybersecurity at the legislative level, which will be mandatory for all the actors and objects of WM.

Military regulation is the set of statutes, instructions, and rules in the case of hostilities in the WM. The WM Grand Electronic Judicial Code will contain the rules and algorithms of e-jurisdiction, define its actors, objects, territoriality, specialization, etc. The Electronic Office WM will play an important role in GLM. In fact, this is the core of WM e-jurisdiction (Fig. 1). The Office will operate with the use of AAI and ASI and will perform the tasks of the Central Analytical Centre and the Separator of Electronic Reports of Electronic Incidents (Electronic Offenses). The WM e-Office will accept requests for e-incidents from all WMs and facilities, analyse the composition of offenses under WM legislation and the Grand Charter of Laws Metaverse itself, form a chain of «territorial accountability» and to draw up a list of participants in the proceedings. For example, if the electronic offence concerns the national «analogue» legislation, such an offense will be considered within national jurisdiction. In the case of an electronic offense CfM or SM between the jurisdictions of different metaverses, such an offense will be considered by

the WM Grand Electronic Court Chamber. At this stage in the formation of the WM and its Grand Charter of Laws Metaverse national legislation needs to be reconfigured or modernized to ensure legal compatibility and functioning of meta-universes emerging to make social relations and information technology activities more structured.

The rules and norms of behaviour in WM are still created according to the projection of the physical world and are corporate in nature. However, there is a trend of migration and transfer of norms of public morality in the Metaverse by simulating cosmopolitan e-social relations in the absence of clear attributes of the electronic State and the State structure of the Metaverse. The development of global electronic legislation of the Metaverse will give impetus to the modernization of national legislation.

The model of e-jurisdiction will outline the most important and problematic issues that arise in the evolution of mankind and the development of virtual reality technologies, as well as form the basis for e-law to regulate public relations in the Metaverse.

The main values and objects of the Metaverse to be protected in electronic jurisdiction should be:

1. Trust and reputation to be built by each subject and object of the Metaverse from the moment of its registration in the Metaverse using blockchain technology.
2. Integrity, reliability and validity of identification data, by means of which individuals and legal entities, other actors and objects are identified in the Metaverse:
   - biometric identification of individuals as particularly valuable and unique attribute or code of access to the Metaverse;
   - IoT identification data (Universal Identification Systems Object IDentifier (OID), Electronic Product Code (EPC), Universally Unique IDentifier (UUID) and International Mobile Identity Identifier (IMEI));
   - AI, AAI and ASI identification data (electronic certificates of quantum cryptographic systems that will protect the AI core from external attacks);
   - identification data of other types of objects.
3. Intellectual property rights and ownership of non-property electronic assets in the metauniverse.
4. Information security and cybersecurity.

The creation of the Grand Charter of Laws Metaverse requires the involvement of a large number of specialists in law and modern electronic technologies, as well as specialists who will conduct interdisciplinary research in many areas.

The Grand Charter of Laws Metaverse project is the project to be developed with the initiative and participation of non-governmental organizations, Metaverse corporations and research institutions, as well as leading Metaverse researchers.

7. CONCLUSION

The era of industrialization and industrial society is coming to an end. Mankind has clearly taken a course to build a new social system, which, at present, is most defined as a post-industrial society. It is already obvious that the «return» point has been passed. Humanity is currently in transition from an industrial to a post-industrial society. This path will be difficult, the resolution and settlement of very complex issues and contradictions, including the issues of national and international jurisdiction. One of the features of post-industrial society is maximizing cyberspace and using it effectively in conjunction with

DOI: 10.46282/blr.2022.6.2.316

natural space in almost all areas of human life. That is, in fact, forming a post-industrial society, mankind forms cyber civilization (Metaverse).

Thus, humanity, rebuilding post-industrial society, forced to simultaneously address the issues of formation of the Metaverse and ensure the effectiveness of its use. Clearly, the development of the Metaverse will be gradual, consistent.

The early stage of development of Metaverse is a promising start for the study of social relations created in the virtual environment, the ability to focus on laws and rules, which will be relevant in the phased creation of a society of digital humanoids in the Metaverse. This is especially important given that these technologies, like many others, are multi-purpose in nature.

The main problem of legal regulation of social relations in the Metaverse is the lack of a unified legal mechanism for regulating even fundamental social relations that arise in the Metaverse.

The solution to this problem is possible by creating a comprehensive electronic jurisdiction and the Metaverse Grand Charter of Laws to regulate public relations in the Metaworld and the formation of a new branch of law.

Creating a comprehensive Metaverse e-jurisdiction requires:

- research in the field of information law on the direction of development of the basic conceptual apparatus, doctrinal and normative and legal concepts; recognition of structures of combined concepts and conceptual schemes, definition of objects and actors of legal relations in the Metaverse;
- study and recoding of current and projected norms of modern information, administrative, civil, criminal, labour law, property law, intellectual property, personal data protection and other branches and institutions of law, as well as the institutions of State security, information and cybersecurity.

The Metaverse Grand Charter of Laws project is the project to be developed with the initiative and participation of non-governmental organizations, meta-universe corporations and research institutions, as well as leading Metaverse researchers.

BIBLIOGRAPHY:

Barlow, J. P. (1996). *Declaration of the Independence of Cyberspace*. Available at: https://www.eff.org/cyberspace-independence (accessed on 15.12.2022).

Demchak, C. and Dombrowski, P. (2014). Cyber Westphalia: Asserting State Prerogatives in Cyberspace. *Georgetown Journal of International Affairs, International Engagement on Cyber III: State Building on a New Frontier 2013-14,* 29-38.

Gervassis, N. (2004). From Laws for Cyberspace to Cyber Laws (Literally): Integration of Legal Norms into Internet Protocols and Law for Closed Digital Management Communities. *SCRIPT-Ed*, 1(2), 259-271. DOI: https://doi.org/10.2966/scrip.010204.259

Keddell, E. (2019). Algorithmic Justice in Child Protection: Statistical Fairness, Social Justice and the Implications for Practice. *Social Sciences*, 8(10), 281-303. DOI: https://doi.org/10.3390/socsci8100281

Kostenko, O. (2021a). Identification Data Management: Legal Regulation and Classification. *Scientific Journal of Polonia Universit*, 43(6), 198–203. DOI: https://doi.org/10.23856/4325

Kostenko, O. (2021b). Identyfikatsiia IoT. *Juris Europensis Scientia*, 1, 77-83. DOI: https://doi.org/10.32837/chern.v0i1.177

Kostenko O. (2022). Electronic Jurisdiction, Metaverse, Artificial Intelligence, Digital Personality, Digital Avatar, Neural Networks: Theory, Practice, Perspective. *World Science,* 73(1), 1-13. DOI: https://doi.org/10.31435/rsglobal_ws/30012022/7751

Kyryliuk, O. (2015). Miake Pravo Yak Normatyvna Osnova Hlobalnoho Informatsiinoho Suspilstva. *Actual problems of international relations*, Release 125 (part I), pp. 106-17. Available at: http://apir.iir.edu.ua/index.php/apmv/article/view/2664/2368 (accessed on 15.12.2022).

Lessig, L. (1998). The Laws of Cyberspace. *Taiwan Net '98 Conference*. Available at: https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf (accessed on 15.12.2022).

Lessig, L. (1999a). *Code and other laws of cyberspace*. New York: Basic Books.

Lessig, L. (1999b). *Code. Version 2.0.* New York: Basic Books.

Özgökçeler, D. (2021). The methods and ways of implementation of the metaverse concept that can be transferred to the general audience of its cultural and commercial potential in-converted. *Academia.edu.* Available at: https://www.academia.edu/70076301/he_Methods_And_Ways_Of_Implementation_Of_The_Metaverse_Concept_That_Can_Be_Transferred_To_The_General_Audience_Of_Its_Cultural_And_Commercial_Potential_In_converted (accessed on 15.12.2022).

Özkahveci, E., Cívek, F. and Ulusoy, G. (2022). Endüstri 5.0 Döneminde Metaverse (Kurgusal Evren)'Ün Yeri. *Journal of social, humanities and administrative sciences*, 50(8), 398-409. DOI: https://doi.org/10.31589/joshas.929

Pengfei, Z. (2022). *If the metaverse is the future then what is the future of the metaverse?* Xinhuanet. Available at: http://www.xinhuanet.com/techpro/20220120/264c62d021974eee81d70c35083ef91a/c.html (accessed on 15.12.2022).

Pu, Q. L., Pang, Y., Peng, B., Hu, C. J., and Zhang, A. Y. (2022). *Metaverse report— Future is here. Global XR indurstry insight*. Available at: https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/technology-media-telecommunications/deloitte-cn-tmt-metaverse-report-en-220321.pdf (accessed on 15.12.2022).

Razmetaeva, Y., Ponomarova, H., and Bylya-Sabadash, I. (2021). Jurisdictional Issues in the Digital Age. *Ius Humani. Law Journal*, 10(1), 167-183. DOI: https://doi.org/https://doi.org/10.31207/ih.v10i1.240

Razmetaeva, Y. and Razmetaev, S. (2021). Justice in the Digital Age: Technological Solutions, Hidden Threats and Enticing Opportunities. *Access to Justice in Eastern Europe*, 2(10) 104–117. DOI: https://doi.org/10.33327/AJEE-18-4.2-a000061

Riek, M. and Böhme, R. (2018). The costs of consumer-facing cybercrime: an empirical exploration of measurement issues and estimates. *Journal of Cybersecurity*, 4(1), 2057-2085. DOI: https://doi.org/10.1093/cybsec/tyy004

Segura-Serrano, A. (2006). Internet Regulation and the Role of International Law. In A. von Bogdandy and R. Wolfrum, (eds.), *Max Planck Yearbook of United Nations Law, Volume 10* (pp. 191-272). Leiden: Brill.

Shaoying, P., Pengzhi, C., Xinru, F., Lifu, Q., Junhui, H., and Liwen, J. (2022). *Ten conjectures: Interpretation of the development trend of the most comprehensive metaverse*. IT Times. Available at: https://m.jiemian.com/article/7078158.html (accessed on 15.12.2022).

Shumskiy, I. (2020). The Westphalian System as the Origin of the New Modern System of International Relations. *International Law Almanac,* 23(10), 81-86. DOI: https://doi.org/10.32841/ila.2020.23.10

Tsaugourias, N. (2018). Law, Borders and the Territorialisation of Cyberspace. *Indonesian Journal of International Law*, 15(4). DOI: https://doi.org/10.17304/ijil.vol15.4.738

Vartanian, T. (2000). Whose Laws Rule the Internet? A U.S. Perspective on the Law of Jurisdiction in Cyberspace. International Law FORUM du droit international, 2(3), 96–201. DOI: https://doi.org/10.1163/157180400322765009

Viseu, A. (2001). Code and Other Laws of Cyberspace. By Lawrence Lessig. *Canadian Journal of Communication*, 26(1), 179-180.

Wyss, J. (2021). *Barbados Is Opening a Diplomatic Embassy in the Metaverse*. Bloomberg. Available at: https://www.bloomberg.com/news/articles/2021-12-14/barbados-tries-digital-diplomacy-with-planned-metaverse-embassy?leadSource=uverify%20wall (accessed on 15.12.2022).

Zhang, D., Mishra, S., Brynjolfsson, E., Etchemendy, J., Ganguli, D., Grosz, B., Lyons, T., Manyika, J., Niebles, J. C., Sellitto, M., Shoham, Y., Clark, J., and Perrault, R. (2021). *Artificial Intelligence Index Report 2021*.

Zhang, D., Maslej, N., Brynjolfsson, E., Etchemendy, J., Lyons, T., Manyika, J., Ngo, H., Niebles, J. C., Sellitto, M., Sakhaee, E., Shoham, Y., Clark, J., and Perrault, R. (2022). *Artificial Intelligence Index Report 2022*.

EU, Regulation on The Protection of Natural Persons with Regard to The Processing of Personal Data and on The Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (2016).

France, Act Relating to Data Processing, Files and Freedoms (1978).

India, Information Technology Act (2000).

Israel, The Computer Law (1995).

Ukraine, Act on Protection of Information in Information and Communication Systems (1994).

Ukraine, Act on Electronic Trust Services (2017).

Ukraine, Act on The Main Principles of Ensuring Cyber Security of Ukraine (2017).

Ukraine, Act on Critical Infrastructure (2022).

Ukraine, Act on Virtual Assets (2022).

Ukraine, Order of The Cabinet of Ministers on The Approval of The Concept of The Development of Artificial Intelligence in Ukraine (2020).

United Kingdom, Computer Misuse Act (1990).

USA, 15 U.S.C. §§ 7701-7713 (2003).

USA, 18 U.S.C. § 1029 (2015).

USA, 18 U.S.C. § 1030 (2020).

USA, 18 U.S.C. § 1037 (2003).

USA, 18 U.S.C. §§ 2510-2523 (2022).

USA, 18 U.S.C. §§ 2701-2713 (2018).