Research article
UDC 34:004:343.213.3:343.232:343.235.4
EDN: https://elibrary.ru/rowsaq
DOI: https://doi.org/10.21202/jdtl.2025.23

# Multifactor Model of Jurisdiction: Reviewing Locus Delicti in a Decentralized Metaverse

**Murad M. Madzhumaev**

Peoples' Friendship University of Russia named after Patrice Lumumba, Moscow, Russia

## Keywords

augmented reality,
avatar,
crime,
crime scene,
criminal law,
digital technologies,
jurisdiction,
law,
metaverse,
virtual reality

## Abstract

**Objective**: to critically analyze the possibility of extending the existing spatial criminal law principles to acts committed in the decentralized virtual worlds of the metaverse, and to develop proposals that include updating the approach to establishing jurisdiction over such virtual crimes.

**Methods**: the methodological basis of the research is a set of general scientific methods and approaches of scientific cognition – dialectical, formal logical (analysis and synthesis, induction and deduction), systematic, as well as private scientific methods – formal legal, legal modeling, interpretation. The study relies on an analysis of judicial practice, foreign legislation, technical features of blockchain technologies and decentralized autonomous organizations, which makes it possible to identify gaps in legal regulation and propose conceptually new solutions for determining the crime scene in a virtual environment.

**Results**: the study revealed a limited implementation of the current generally accepted principles of determining jurisdiction in relation to virtual crimes that do not have physical coordinates. The proposed multifactorial jurisdiction model redefines the "crime scene" taking into account factors such as the offender's digital identity, the nature and location of digital assets, platform management protocols, and the actual damage caused. Assumingly, the immutable and verifiable nature of blockchain transactions can serve as a legal equivalent of a physical presence to establish personal jurisdiction, allowing criminal prosecution to be initiated even in cases where the actual location of the offender remains unknown.

**Scientific novelty**: the paper presents an approach that implies the fundamental transformation of reactive, adaptive legal regulation principles into a proactive, comprehensive framework designed specifically for the unique challenges of the metaverse. A paradigm-changing hypothesis was put forward: that a permanent (stable) digital footprint of the offender in virtual spaces can serve to exercise jurisdiction. The model systematically presents the idea of harm as the most important link between virtual offenses and their consequences in the real world.

**Practical significance**: it is currently impossible to apply legal norms and rules to relations in the metaverse, taking into account their specifics. The main provisions and conclusions of the study can be used to improve the mechanisms of legal regulation of the metaverse and to form international protocols on data exchange and mutual legal assistance for searching and collecting evidence based on blockchain technology. They may help to develop legislative initiatives aimed at creating integrated legal mechanisms that are scalable and resistant to rapid technological changes, characteristic for the digital environment.

## For citation

Madzhumaev, M. M. (2025). Multifactor Model of Jurisdiction: Reviewing Locus Delicti in a Decentralized Metaverse. *Journal of Digital Technologies and Law, 3*(4), 570–597. https://doi.org/10.21202/jdtl.2025.23

## Contents

Introduction
1. Criminalization of the metaverse
2. Principles of the operation of criminal law in space
   2.1. Territorial principle
   2.2. Exterritorial operation of criminal law
3. Phenomenon the metaverse: notion and ontological properties
4. Technological basis of the metaverse
5. Digital avatars (digital twins)
6. Operation of criminal law in the metaverse
7. Multifactorial jurisdiction model: rethinking of the crime scene in the metaverse
   7.1. Establishing jurisdiction in relation to the subjects of a virtual deed in the metaverse
   7.2. Digital assets as the basis for establishing jurisdiction in rem

7.3. Platform protocols (code management) as the basis for establishing jurisdiction
7.4. Harm (physical connection or ultimate result) as the basis for establishing jurisdiction
Conclusions
References

## Introduction

The emergence of a metaverse, conceptually represented as a network of regulated, permanent, immersive, interactive, and interconnected virtual worlds combining virtual (VR), augmented (AR), and mixed (MR) realities, as well as blockchain technology, poses a serious challenge to established principles of criminal law, especially the definition of the law in space. Historically, state sovereignty and the inalienable right to make and apply laws have been inextricably linked to territoriality, which underlies the Westphalian system of international law and order (Chimni, 2022). It follows from this fundamental principle that the jurisdiction of a state with respect to acts committed on its "physical" territory (on land, in airspace, in internal waters and territorial sea, on the continental shelf and in the exclusive economic zone) is in principle lawful. At the same time, in case of claims with respect to acts committed outside its territory, they are considered illegal (except for the principles of extraterritoriality).

For all its historical roots, such a traditional model (territoriality and generally accepted principles of extraterritoriality) is becoming more and more "artificial" in the digital age. In particular, according to Actor Network theory, objects (artifacts, technical complexes, non-human "agents", algorithms), the so-called actors or actants, are perceived as acting units of public relations (Wei, 2023). Assumingly, such actors (actants) may include digital counterparts of people in the metaverse who are able to interact and influence the virtual network. The main problem lies in the fundamental incompatibility of such a model of jurisdiction, tied to the physical territory of the state, with the limitless, "non-physical" and decentralized architecture of the metaverse. The metaverse is completely devoid of physical coordinates (Brey, 2025).

In this article, we use the terms "locus delicti", "crime scene", and "scene of the incident". Although they are not identical in content, here they will be understood as having the same meaning, except in cases where the opposite is specifically stipulated. Locus delicti (Latin "crime scene") means an area in which there were signs of the crime's objective element. A crime scene is a narrower and more specific concept. This is the main place where the crime was committed, regardless of where the crime's socially dangerous consequences occurred or where information about the crime was discovered.

On the other hand, the scene of the incident is a broader category. It designates a place or territory where there is information related to the event that is being investigated in a criminal procedural manner[1]. This includes not only a specific crime scene, but also any other place where objective consequences of the crime or other traces of criminalistic significance are found.

Determining the location of a crime (locus delicti) is one of the fundamental tasks of criminal law science, since the solution of several fundamental issues depends on it. First, it defines the law applicable to a particular crime, as well as the proper investigative and judicial jurisdiction of the case. The limitation periods of criminal liability are directly related to this, since their establishment depends on the jurisdiction in which the crime was committed. Second, the crime scene serves as a starting point for establishing the constituent elements of the deed and its correct qualification. This, in turn, affects the implementation of "non bis in idem" ("not twice for the same thing") principle and extradition issues.

In the criminal-procedural law, a crime scene is an indispensable landmark for almost all investigative actions. It serves as the main source of evidence, ensuring a proper chain of proving on which their subsequent verification and evaluation depend. In addition, the crime scene is the starting point for finding witnesses, checking alibis, and motivating procedural documents such as the investigator's orders to conduct a search and seizure (or a court decision if a search is conducted in residential premises). All these actions together contribute to building a case that will allow for a reasonable accusation, taking into account the presumption of innocence.

In criminology, a crime scene is a central element that defines the entire investigation process. This is extremely important for inspecting the crime scene, building forensic versions of events and planning further investigative actions. All types of evidence are collected at the crime scene, and their forensic photo and video recording is carried out. In addition, the interaction between investigators (inquirers), employees of operational search units, and, if necessary, authorized representatives of law enforcement agencies of other states is organized. Also, competent persons with special knowledge (specialists and subsequently experts) actively work at the crime scene, which contributes to the effective detection and investigation of crimes.

Determining the location of a crime (locus delicti) is especially important when investigating crimes, the constituent elements of which are fully or partially concentrated in a decentralized virtual space – the metaverse. The total turnover of the global metaverse market is showing rapid growth, estimated as US$ 110.4 billion in 2024 and projected to exceed US$ 4.47 trillion by 2034; it reflects a high cumulative annual growth rate (CAGR)

[1] Bertovskiy, L. V. (ed.). (2021). Criminology: tutorial for Bachelor students (2nd ed., amended and complemented). Moscow: RG-Press.

of 44.8 %[2]. In 2024, the largest contribution was into the hardware segment, which includes advanced headsets and tactile sensors, accounting for 52.8 % of the total market share[3]. The underlying virtual reality (VR) and augmented reality (AR) technologies combined accounted for 34.2 % of the market, forming the basis of immersive digital environments[4].

The user base of the metaverse consists mainly of young people (four out of five users are under the age of 16) and comprises about 700 million active users monthly worldwide[5]. Growth forecasts are quite impressive, with some reports suggesting that by 2030 the number of users will reach 5 billion, taking into account mobile phone users, while more accurate estimations, based on data on VR/AR users, predict a figure closer to 1 billion[6]. This determines the relevance of studying the problem under consideration regarding the definition of locus delicti in deeds committed in the metaverse.

This article examines the fundamental problem of the operation of criminal law in the decentralized virtual environment of the metaverse. First of all, we will analyze the problem of the metaverse criminalization, to use it as the basis for discussing the applicability of traditional legal approaches to it. Further, we will discuss in detail the well-established principles of criminal jurisdiction in space, in particular territorial and extraterritorial approaches and their limitations when applied to a virtual environment. Then we will study the metaverse phenomenon, describing its ontological properties such as immersiveness, synchronicity, stability, compatibility and decentralization, as well as its technological foundations and the role of digital avatars. Following this, we provide a critical assessment of the operation of criminal law in the metaverse, which leads to the main thesis of this work: the need to develop a new multifactorial model of jurisdiction. This model, intended to rethink the concept of locus delicti in the metaverse, systematically defines jurisdiction based on a multi-pronged analysis of the offender's digital identity, the location of digital assets, platform management protocols, and the actual damage or physical connection caused by the virtual action.

## 1. Criminalization of the metaverse

Although some of the examples below are of a civil law nature, they can be used to outline landmarks useful for rethinking the concept of an incident in criminal law.

One of the most notable conflicts of legal interests arises in connection with the illegal use of intellectual property in the metaverse. A clear example of this is

2 Metaverse Market. Report ID: 101905. (2025). Market.us Scoop. https://clck.ru/3QGxSF

3 Ibid.

4 Ibid.

5 Duarte, F. (2025, June 5). Number of Metaverse Users in 2025. Exploding Topics. https://clck.ru/3QGxcm

6 Ibid.

the civil dispute between Roblox Corporation (further – Roblox), which develops and operates a virtual online entertainment platform, and WowWee Group Limited (further – WowWee), a leading developer, manufacturer, seller and distributor of innovative high-tech consumer robots, entertainment products and other gaming devices. Roblox, registered in California (USA), claimed that WowWee, registered in Hong Kong, illegally reproduced (copied) the design of Roblox virtual avatars to create and sell a line of physical minifigures (dolls) under the name My Avastars[7]. Based on the evidence presented, it was determined that WowWee intentionally sought to position these dolls as "real" versions of Roblox avatars, i.e. to establish a link between their physical product and the Roblox ecosystem, thereby using virtual intellectual property for material benefits[8].

As for criminal prosecution for infringement of copyright and related rights, the case presents a multifaceted jurisdictional dilemma, since it is necessary to determine the location of the crime (locus delicti). This may be Hong Kong, where WowWee is physically located; California (USA), where Roblox is located; the location of the servers (cloud, disk), where the data of the Roblox online platform are stored; or a decentralized virtual space (metaverse), where the original copyrighted avatar is located.

A similar dispute is between Impulse Communications, Inc. (a corporation from Delaware with headquarters in Rhode Island, USA) and Uplift Games LLC, Treetop Games LLC, Lionfield Investments LTD – companies that manage games with virtual pets called Adopt Me[9].

Another similar case occurred in a dispute between Hermès International (Paris, France) and Hermès of Paris, Inc. (New York, USA) and Mason Rothschild (Los Angeles, California, USA). Mr. Rothschild, operating from California, created and commercialized a collection of digital assets called MetaBirkins in the form of non-exchangeable tokens (NFTs), which were digital copies of the famous Hermès Birkin bag and were promoted as luxury items in the metaverse[10].

In the case of criminal prosecution for trademark infringement, the same serious problem of establishing a specific crime scene will arise. When determining jurisdiction, the crime scene may be the location of Hermès International (Paris, France); Hermès of Paris, Inc. (New York, USA); Mason Rothschild (California, USA); or the location of a decentralized blockchain network where infringing NFTs were created and sold.

---

7 Roblox Corporation et al v. WowWee Group Limited et al, No. 3:2022cv04476-SI – Document 69 (N.D. Cal. 2024). https://clck.ru/3QGxeC

8 Ibid.

9 Impulse Communications, Inc. v. Uplift Games, LLC et al, No. 24-cv-166-JJM-LDA – Document 29 (D.R.I. 2024). https://clck.ru/3QGxjZ

10 Hermes International et al v. Rothschild, No. 1:2022cv00384 – Document 140 (S.D.N.Y. 2023). https://clck.ru/3QGxnH

According to the indictment, in another case, the accomplices entered into a criminal conspiracy which acted from 2018 to 2022 to defraud investors of a group of companies owned by one of the attackers[11]. They raised funds promising to develop virtual technologies, including their own cryptocurrency, which was to be used in the metaverse they were creating[12]. They also promised knowingly unattainable high incomes and spread false claims that well-known entrepreneurs and wealthy buyers were involved in the acquisition[13]. Instead, they misappropriated funds for personal gain, including using the money to purchase personal real estate[14]. This case shows that if the entire scheme had been implemented in a fully decentralized metaverse without using traditional infrastructure, there would have been problems defining jurisdiction.

Finally, the most striking manifestation of the problem under consideration is probably the UK police investigation of crimes against sexual integrity committed in immersive virtual reality. As a result of the indecent acts, the victim allegedly suffered psychological and emotional trauma, which, despite the lack of physical contact, is an obvious sign of the objective element of crime[15]. An urgent question arises: where is the crime scene located if it was committed exclusively using avatars in virtual space? The crime scene can be determined by the physical coordinates of the victim or the perpetrator, or by the virtual environment (meta-territory) in which the crime was committed.

All these examples require a new legal approach to determining the crime scene, recognizing the metaverse as a full-fledged new space for crimes. This in turn, requires new principles for determining the operation of criminal law in space.

## 2. Principles of the operation of criminal law in space

### 2.1. Territorial principle

The main principle determining the operation of criminal law in space is the principle of territoriality. According to it, the state has exclusive jurisdiction to prosecute and punish crimes committed on its territory (Payer, 2023). A crime is considered committed on the territory of the Russian Federation if any of its constituent features, including the beginning, continuation or completion, took place within its state border (the doctrine

11 United States District Court District of Nebraska. (2025, June 4). 22-3077 – USA v. Chandran et al. [Government]. Administrative Office of the United States Courts. https://clck.ru/3QGxrp

12 Ibid.

13 Ibid.

14 Ibid.

15 Camber, R. (2024, January 1). British police probe VIRTUAL rape in metaverse: young girl's digital persona 'is sexually attacked by gang of adult men in immersive video game' – sparking first investigation of its kind and questions about extent current laws apply in online world. Daily Mail Online. https://clck.ru/3QGxwo

of subjective territoriality, the doctrine of objective territoriality, and the doctrine of effect (consequences) (Ryngaert, 2023).

The territory of the Russian state, defined by the Russian Constitution, includes land territory, water territory, subsoil and airspace (Part 1 of Article 67 of the Russian Constitution). The land territory covers the mainland and islands within the state border. The water territory comprises internal waters such as rivers and lakes, and a territorial sea – a strip of marine water area 12 nautical miles wide adjacent to land or inland waters (Part 1 of art. 2 of the Federal Law "On internal sea waters, territorial sea and contiguous zone of the Russian Federation")[16]. The subsoil is a part of the Earth crust below the Earth surface (the soil layer, and in its absence – below the Earth surface and the bottom of reservoirs and watercourses, extending to depths accessible for geological study and development) (preamble of the Federal Law "On subsoil")[17]. The airspace is an area above land and water with an assumed upper limit 100–110 km (conditional boundary between the Earth atmosphere and space (Karman line) (Pogorzelska, 2024).

The state border defining the sovereign territory of the Russian Federation is a vertical plane running along these physical borders. Outside of these defined zones, the territorial principle applies to certain crimes committed on the Russian continental shelf and in its exclusive economic zone. Both of these zones are marine areas outside the territorial sea, where the Russian Federation exercises special sovereign rights, in particular with regard to natural resources.

According to the territorial principle, Russian criminal law applies to crimes committed on civil ships and aircraft registered in the Russian Federation when they are in international waters or airspace, as well as on Russian military ships and aircraft, regardless of their location (Part 3 of Article 11 of the Russian Criminal Code)[18].

## 2.2. Exterritorial operation of criminal law

It is customary to distinguish cases in which a state's jurisdiction is assumed to be exercised beyond its national borders, known as extraterritorial jurisdiction. In this regard, the following principles are distinguished: active citizenship, passive citizenship, protective and universal jurisdiction.

The principle of active citizenship (personal, national) reflects the right of the state to exercise criminal jurisdiction over the deeds of its citizens who have committed

[16] On internal sea waters, territorial sea and contiguous zone of the Russian Federation. No. 155-FZ of July 31, 1998 (with amendments and additions, Federal Law of July 31, 2025 No. 304-FZ). Garant. https://clck.ru/3QGyAr

[17] On subsoil. No. 2395-I of February 21, 1992 (with amendments and additions, Federal Law of July 31, 2025 No. 353-FZ). KonsultantPlyus. https://clck.ru/3QGyCQ

[18] Criminal Code of the Russian Federation of June 13, 1996. No. 63-FZ. KonsultantPlyus. https://clck.ru/3QGyDx

criminally punishable deeds outside its territory, regardless of their geographical location (Esakov, 2015).

On the other hand, although it is the subject of scientific debate, the principle of passive citizenship (passive personal citizenship) implies exercising extraterritorial criminal jurisdiction by the state in relation to crimes where the victim is its citizen (Esakov, 2015). In this case, the crime is committed by foreign nationals (or stateless persons) outside the state border.

If a crime committed outside the state territory by a foreign citizen (or a stateless person) encroaches on the interests of that state, then the law of that state applies in accordance with the principle of protection (Esakov, 2015).

The principle of universality allows for the application of state law in the criminal prosecution of foreign citizens and stateless persons who have committed crimes against the peace and security of humankind. The application of this principle is justified due to considerations of international public policy (Esakov, 2015).

## 3. Phenomenon the metaverse: notion and ontological properties

The concept of the metaverse, which was once limited to the realm of science fiction, is now turning into a new reality, which in the future will give a new expression to human interaction in the digital dimension. In 1992, Neal Stephenson described the metaverse in his novel “Snow Crash” as a virtual reality that would replace the Internet (Ioannıdıs & Kontıs, 2023). Since then, the idea of the metaverse has improved significantly with the development of virtual reality (VR), augmented reality (AR), haptics, and artificial intelligence technologies.

The metaverse is a set of interconnected digital spaces and phenomena that combine a virtually enhanced physical reality and a physically stable virtual reality. Thus, there is a qualitative transition from the current stage of the Internet development to an immersive three-dimensional online environment. The network space proposed within the metaverse concept allows users to interact with each other and with the computer environment in real time, usually using digital avatars (Han et al., 2023). Its transformative potential extends to virtually all areas of human activity, including healthcare, education, work, social interaction, commerce, and entertainment.

*Immersiveness*

A characteristic feature of the metaverse is its ability to immerse users in three-dimensional space. This immersion is achieved through advanced augmented reality (XR) devices, which include virtual reality (VR) headsets, augmented reality (AR) devices, and mixed reality (MR) technology. These tools use stereoscopic images and spatial sound to create the illusion of depth and space, allowing users to feel “real” (telepresence) in a place other than their physical location (Bhowmik, 2024). The degree of sensory

immersion plays a crucial role in arousing emotions and influencing user behavior. Such a deep level of engagement means that virtual experiences can have a significant psychological impact, further blurring the line between the virtual and real worlds.

*Synchronicity of interaction*

The metaverse provides real-time interaction between users and the virtual environment (Hosseini et al., 2024). This kind of instantaneity is crucial for creating a dynamic and operational experience, allowing for synchronous social interaction, joint work, and flexible gameplay. The sense of "presence" is greatly enhanced by the instant adaptation of the user's vision and sensory feedback in response to their movements and actions (Hosseini et al., 2024). This reality means that actions and their consequences in the metaverse can be instantaneous.

*Stability (constancy)*

The next feature of the metaverse is its constancy, which ensures the continuous existence of the virtual world and all the changes taking place in it, even when users are not connected to the system (Richter & Richter, 2023). This means that users' avatars, digital twins (virtual representations of objects), and the state of the metaverse spaces remain unchanged over time, ensuring stability and integrity. Unlike traditional online games, where sessions end and progress can be reset or limited to specific episodes, a truly permanent metaverse implies a stable digital environment that evolves based on user actions and remains unchanged until users change it. Although modern platforms demonstrate a certain degree of local persistence, the general criterion of stable, universal persistence, as it is represented for the metaverse, remains an important area for technological progress and research.

*Interoperability*

Another feature of the metaverse is functional compatibility (interoperability), which is the ability to seamlessly move virtual digital objects, avatars, and data between different virtual worlds and platforms throughout the metaverse (Richter & Richter, 2023). It is this property that ensures the unity and interconnectedness of the digital universe. It significantly differs from the current mode, when virtual worlds are largely incompatible with each other and often remain "closed". It is generally recognized that to ensure genuine interoperability we need compatible technologies, equipment, protocols and standards that ensure the smooth exchange of information and simultaneous response of different systems.

*Decentralization*

The main feature of the metaverse is its decentralization, which implies the distribution of control and rights among network participants (McStay, 2023), rather than their concentration in the hands of a single central authority (provider). In fact, this is an integral principle of managing the metaverse, influencing decision-making, setting rules, and maintaining the overall structure of the virtual environment. The main instrument of decentralization is blockchain technology, which provides transparency and autonomy

by recording transactions and alterations in a publicly accessible and immutable registry (Panda, 2023). Such distributed control is aimed at empowering users by giving them more rights to their digital assets (such as virtual real estate, gaming items, and virtual currency) and direct participation in managerial decision-making, which reduces vulnerability to arbitrary actions by a central authority. Decentralization also helps to overcome censorship, since no organization is able to prescribe content or restrict access, and this promotes freedom of expression and creativity.

## 4. Technological basis of the metaverse

The metaverse functioning is based on the synergetic integration of various advanced technologies, forming a multi-level ecosystem that supports its immersive, constant and interactive characteristics.

Extended reality (XR) is an umbrella term that encompasses virtual reality (VR), augmented reality (AR), and mixed reality (MR). It is a range of immersive technologies used to access and interact with (in) the metaverse (Özkan & Özkan, 2024).

Virtual reality (VR) immerses users in a fully computer-generated, artificial three-dimensional environment. This is usually achieved using virtual reality headsets equipped with stereoscopic screens and spatial sound, creating a strong sense of presence (Bhowmik, 2024). Motion sensors track the user's movements, correcting the virtual view in real time, while tactile feedback devices can create a sense of touch, allowing users to manipulate virtual objects (Bhowmik, 2024).

Augmented reality (AR) superimposes digital data (elements, objects) on the physical world, improving the user's perception of reality (Bhowmik, 2024). Unlike VR, AR combines physical and digital elements, creating a holistic interface that integrates virtual content into the user's real-world environment, often using devices such as smartphones or transparent VR headset modules. With AR applications, users can interact with the displayed data as if they were real, access maps, or create shared AR experiences (Syed et al., 2022).

Mixed reality (MR) combines elements of VR and AR, allowing digital and real objects to coexist and interact in real time (Rokhsaritalemi et al., 2020). This technology is a more advanced form of mixing physical and virtual reality.

## 5. Digital avatars (digital twins)

In the metaverse, users employ virtual avatars as their digital representations through which they express themselves, communicate, and otherwise interact with others in virtual space (Kim et al., 2025). These avatars can be highly customizable, allowing users to express themselves in unique ways or even recreate characters from popular culture. The ability to create and embody digital identities goes beyond simple profile photos, representing personality, style, and even social status in the metaverse.

At the same time, the very concept of a digital personality in the metaverse remains complex and multifaceted, fundamentally different from a personality in the real world. In the digital space, one person can have several different and even pseudonymous identities, which complicates traditional concepts of identity and responsibility. The increasing convergence of real and virtual personalities means that harm caused to a user's avatar can have serious moral and legal consequences in the real world. Undoubtedly, with this understanding of digital identity, new legal issues arise regarding personal rights, fraud, and deception in a virtual environment.

## 6. Operation of criminal law in the metaverse

Traditional legal regulations basically focus on social relations in the physical world that develop between people located in a certain territory. By its nature, the metaverse transcends such physical boundaries, creating a global, interconnected digital space in which users from different countries can easily interact with each other. This fundamentally new circumstance means that actions performed in the virtual world can have consequences in the real world in several jurisdictions, as shown by the examples above. Consequently, it becomes much more difficult to determine which country's legislation is to be applied, as well as to establish the investigative and judicial jurisdiction of a criminal case.

Web 3, the next stage in the Internet development, is widely considered to pose new challenges in terms of accounting for geopolitical boundaries, but many online activities are still indirectly linked to the user's location through parameters such as language, time zone, domain names, IP addresses, and other metadata. Perhaps the most important and at the same time fraught with certain risks is the fact that immersion in a virtual world, especially one designed to mimic or (conditionally) replace the real world, does not imply a presumption of mandatory compliance with the laws of any particular country, with the possible exception of the rules of this platform (metaverse).

The limitations of the existing principles of determining jurisdiction and legal structures in terms of an appropriate response to the peculiar challenges of the metaverse indicate the need to develop new comprehensive legal approaches. A reactive approach, reduced to attempts to simply adapt existing legal norms to new digital realities, may not be sufficient and may lead to the constant appearance of gaps in legal regulation, especially in criminal law.

## 7. Multifactorial jurisdiction model: rethinking of the crime scene in the metaverse

Based on the above, we propose to revise the content of the "crime scene" concept in a decentralized metaverse and consider it not as a specific spatial point, but as a distributed system of individual components. In this system, each component (signs of a criminal deed both inside and outside the metaverse) is an independent link that defines jurisdiction.

It seems appropriate to determine jurisdiction based on a comprehensive analysis of all these components, not limited to a single, often arbitrary, location in physical space.

The main idea of the multifactorial jurisdiction model is to consider a crime as an event with several legally significant points of contact in digital and physical space, rather than as a deed committed in one specific geographical location. The model elements rely on the theoretical comprehension of the established legal principles of determining the criminal law operation in space and are designed to provide a structured and reliable basis for criminal prosecution.

The proposed model includes four key factors, each providing the court with a separate basis for determining criminal jurisdiction:

a) the subject (of a virtual deed);

b) digital assets;

c) platform protocols (code management);

d) harm (physical connection or final result).

### 7.1. Establishing jurisdiction in relation to the subjects of a virtual deed in the metaverse

Identification of a person who has committed crimes in the metaverse should be carried out based on information contained in a distributed registry (in other words, in blocks interconnected in a chain in a decentralized database (blockchain) (Komalavalli et al., 2020), or through a pseudonym associated with the offender's digital identity. In this case, an unchangeable and irreversible digital footprint of criminal activity is recorded.

The main distinguishing feature of a virtual action is its immutability. After being fixed, it is permanently recorded in a distributed ledger (blockchain), which makes it immutable and irreversible (Aakula et al., 2023). Each block contains cryptographic references to the previous block, a timestamp, and transaction data, which technically eliminates the possibility of changing information in a separate block without changing the entire chain (Aakula et al., 2023). This mechanism provides an exceptionally reliable and verifiable digital footprint of activity that can serve as reliable evidence.

The distributed nature of the action recording means that information is distributed across a network of interconnected nodes rather than being stored in a single centralized repository (Aakula et al., 2023). In this way, increased transparency, resistance to forgery, and global availability of records are achieved. Examples of virtual deeds are the transfer of digital assets, the use of malicious smart contracts (for example, when committing theft), or even virtual harassment. These actions, although they occur exclusively in a virtual environment, have tangible legal and economic consequences in the real world.

The main hypothesis is that the offender's address in the blockchain, by virtue of its verifiable, unchangeable and traceable activity, acquires a kind of legal equivalent of physical presence for the purposes of establishing personal jurisdiction.

This is a fundamental paradigm shift, establishing a new form of jurisdiction based on stable digital data and not limited to a temporary physical location. Such a conceptual shift facilitates the initiation of criminal prosecution based on the offender's verifiable and irreversible actions on the blockchain, even if their physical location remains unknown. This is consistent with the principles of due process by establishing a clear, digitally derived link between the suspect's unique digital identifier and the alleged offense.

The solved "blockchain paradox" is manifested by an internal contradiction: although transactions on the blockchain may seem anonymous due to the use of pseudonymous digital wallets, the main activity is traceable in principle. The offender's actual identity may remain unknown, but their digital activity in the distributed registry is constantly recorded and can be tracked using signature schemes and cryptographic hashes that reveal behavioral patterns (Trozze et al., 2022). The main task is to bridge the gap between monitored digital activity and a real person.

If a virtual action is an immutable and verifiable record, then the action per se becomes a "tangible", verifiable object in the digital space. This transforms a virtual action from a simple proof of human behavior into a digital object that can be the subject of research during a trial. We are talking not only about who committed the act, but also about what this act is and where it is recorded (in our case, in the blockchain). This extends the concept of substantive jurisdiction (jurisdiction in rem) beyond digital assets, extending it to digital actions per se. This means that the court can extend its jurisdiction over virtual actions as a separate legal fiction (digital "thing" or "events"), which will allow for investigations, injunctions (for example, blocking smart contract functions), or even "removing" a digital footprint, even before the offender is identified or physically detected. This is a significant extension of the in rem principles to the field of digital behavior, providing a powerful new tool for law enforcement in decentralized environments.

To implement the above, it may be necessary to develop and implement special regulations requiring centralized exchanges and other services to store information about their customers and provide it upon appropriate official request.

This includes collecting and verifying personal information, like full name, date of birth, residential address, and a standard ID. The introduction of such a standard at the international level would allow obliging exchanges around the world to store such data and provide it upon legitimate request, thereby establishing an important link between a blockchain address and a real person. This would significantly expand the capabilities of law enforcement agencies in overcoming the blockchain paradox by providing legitimate access to identification data.

However, it should be noted that the existence of decentralized exchanges (DEXs), which often do not collect this information, is a problem that requires a separate scientific study.

### 7.2. Digital assets as the basis for establishing jurisdiction in rem

Digital assets, including cryptocurrencies, non-fungible tokens (NFTs), and in-game (computer) items, are generally recognized as a separate type of property (or, more precisely, rights) that can be used in criminal activity as an object or means of crime. Their official classification as a new form of property allows them to be directly subject to the established principle of substantive jurisdiction. This principle makes it possible to exercise jurisdiction over disputed property located within the territorial jurisdiction, regardless of the physical location of its owner (Niesel, 2023). Such a legal classification is crucial because it allows the seizure of property and, if necessary, its confiscation, which are the object (means) of criminal activity, thereby guaranteeing the possibility of recourse to legal protection and the return of property in the digital sphere.

Although the blockchain per se serves as the main location of digital assets (and in fact the storage server), their practical digital location can be deduced from a number of circumstances. Jurisdiction can actually be established where a digital asset interacts with the physical world. A striking example is the situation when digital assets were acquired or disposed of using fiat currency through a local banking institution; this creates a clear and indisputable link to a specific physical territory.

Centralized platforms, such as exchanges, perform an essential function in this case, acting as entry (and exit) points between the metaverse and the real world. The jurisdiction of the court at their location extends to the activities of these exchanges, which allows seizing or freezing assets stored on the accounts of these platforms.

An alternative option for establishing jurisdiction is the location of the hosting provider, on whose server a certain segment of the decentralized network is located. This approach is based on the identification and use of the Internet physical infrastructure (cables, servers, data centers), which underlies even the most decentralized digital operations. In the legal analysis of intangible assets, a legal fiction is often created to link these assets to a specific location, taking into account factors such as the effectiveness of law enforcement and access to legal remedies (Wendehorst, 2023). In some cases, this may imply the physical location of a digital wallet if it can be reliably linked to a specific person.

The above approaches to asset location demonstrate the crucial, often overlooked relationship between centralized gateways and decentralized networks for enforcement purposes. Centralized exchanges by their nature provide a regulated “point of control” where a real personality and physical location can be linked to digital assets in accordance with the requirements of anti-money laundering and terrorist financing legislation (Schuler et al., 2024). However, purely decentralized assets or transactions, although more difficult to seize directly, still depend on the underlying physical infrastructure (nodes, servers, hosting providers) for their operation (Schuler et al., 2024; Bains et al., 2022).

All this indicates the need for dual regulation: for digital assets interacting with the traditional financial system or centralized service providers, the use of these centralized structures is of paramount importance for effective legally meaningful measures. For truly decentralized assets bypassing such gateways, the focus shifts to identifying and asserting jurisdiction over the physical infrastructure supporting the network. This highlights the fundamental contradiction between the decentralized ideal of the metaverse and the practical reality of law enforcement, implying that even the most "limitless" digital assets are ultimately tied to physical reality to one degree or another, whether through human interaction with centralized services or through the underlying computing infrastructure.

### 7.3. Platform protocols (code management) as the basis for establishing jurisdiction

In terms of establishing jurisdiction, the protocol refers to the underlying blockchain network or a set of rules (code) governing the virtual space in which the offense was committed. It provides a technical framework and automated rules embedded in the system. A decentralized autonomous organization (further – DAO), on the contrary, is a form of managing this virtual space, often built on the basis of a specific protocol or interacting with it (Qin et al., 2022). It functions as an organizational structure, usually managed by decentralized software, with voting and finances processed through the blockchain (Qin et al., 2022). An offense can be committed both by using a protocol (for example, the deployment of a malicious smart contract), and within the DAO (for example, by falsifying voting in its management system).

The principle of "code management" as the basis of jurisdiction is based on the following legal theory. A DAO, by its very nature, as a self-governed and self-regulated structure, can be involved in criminal activities such as laundering (legalization) of criminal proceeds (Benson et al., 2024) or fraud (Scharfman, 2024) (through its representatives or collective actions of token holders or third parties). This is analogous to traditional legal entities, such as commercial organizations or government agencies. Just as a commercial organization is a legal entity capable of bearing legal (administrative, civil) responsibility for its actions, a DAO, through code-based management and collective decision-making, can be recognized as a legal entity in certain jurisdictions. The "code rule" (Judge et al., 2025), which regulates operations and transactions on the blockchain, provides a form of responsibility on the chain.

Jurisdiction may be extended to individuals who have created, deployed, or actively control the protocol, provided that they are physically located within the jurisdiction of the relevant state. Thus, traditional personal jurisdiction is applied when there is a link to a person, which provides direct contact for law enforcement.

Formal legal structures transform a decentralized protocol or DAO from a "shadow" or ambiguous network into a legally recognized organization with a specific location and legal personality (Pesqueira, 2025). This is crucial in order to avoid ambiguous qualifications of the deed, which can lead to unlimited personal liability of individual token holders, thus deterring participation in the activities of the organization. Turning to foreign experience, one can note that some US states (for example, Wyoming[19], Vermont[20], Tennessee[21] and the Republic of the Marshall Islands[22]) have adopted laws recognizing DAOs as legal entities, usually in the form of a decentralized autonomous organization with limited liability (DAO LLC). Such legal recognition ensures predictability, limited liability of participants (similar to traditional LLCs) and the ability of DAOs to enter into civil law relations, i.e. conclude contracts, own property, and interact with traditional legal systems.

At the same time, the inherent global and decentralized nature of the DAOs means that they can affect social relations that arise in the territories of different jurisdictions.

Therefore, there is a contradiction between the ideal of decentralization and the need to ensure legal responsibility. Decentralization implies the distribution of control and stability to a central authority, while the proposed solution for jurisdiction over protocols and DAO is largely based on the creation of formal legal structures and legal status for DAO (as was done in a number of US states mentioned above). This is a direct conceptual contradiction. The essence of decentralization is to eliminate single points of control and authority, which naturally makes it difficult for traditional legal systems to identify a responsible party. The imposition of a legal "shell" or the requirement to register as an LLC, in fact, reintroduces a certain degree of centralization or identifiable legal personality. Being necessary to establish legal responsibility, this may be perceived as compromising the basic principles of decentralization, in addition restraining innovation in this field.

The main challenge is to achieve a pragmatic balance in which legal responsibility can be implemented without compromising the fundamental advantages of decentralization, such as freedom from censorship and promotion of innovative initiatives. This

---

19 WY Stat § 17-31-101 (2024). 2024 Wyoming Statutes, Title 17 – Corporations, Partnerships and Associations, Chapter 31 - Decentralized Autonomous Organization Supplement, Article 1 – Provisions, Section 17-31-101 – Short Title. https://clck.ru/3QGyrv

20 11 VT Stats § 4171. 2024 Vermont Statutes, Title 11 – Corporations, Partnerships and Associations, Chapter 25 – Limited Liability Companies, § 4171. Definitions. https://clck.ru/3QUdkt

21 TN Code § 48-250-101 (2024). 2024 Tennessee Code, Title 48 – Corporations and Associations (§ 48-1-101 – 48-250-115) Limited Liability Companies (§ 48-201-101 – 48-250-115), Chapter 250 – Blockchains (§§ 48-250-101 – 48-250-115), Section 48-250-101 – Chapter definitions. https://clck.ru/3QwuTB

22 52 MIRC Ch. 7 § 701. Republic of the Marshall Islands Code, Title 52 – Associations Law, Chapter 7 – Decentralized Autonomous Organization Act 2022. https://clck.ru/3QwuHz

presupposes a future legal environment in which hybrid legal structures will increasingly prevail, combining aspects of decentralized governance with traditional legal personality.

### 7.4. Harm (physical connection or ultimate result) as the basis for establishing jurisdiction

Harm (physical connection or ultimate result) is the only physically determined element in the multifactorial jurisdiction model. It acts as the most important link to the real world, which connects a virtual offense with its material, legally significant consequences for an individual or organization. This factor directly fits into and expands the existing legal doctrine of consequences, according to which jurisdiction can be established based on the negative consequences of a deed that occurred in a certain territory. Its main purpose is to ensure that the victim has access to justice in court at his place of residence, providing a clear and accessible way to recover damages, regardless of the virtual nature of the original deed.

The harm factor serves as an important starting point for establishing jurisdiction in cases where other factors (such as the perpetrator identity, the specific location of digital assets) may be ambiguous or inaccessible. It transforms the abstract nature of crimes in the metaverse into specific legal constructions that correspond to existing, established legal norms. In addition, this factor suggests that victims are not left without legal protection just because the crime was committed in a new digital environment, which means that the fundamental principle of access to justice will be respected. Apparently, this also means that in court proceedings involving crimes in the metaverse, it will be of paramount importance to prove a clear and direct causal relationship between virtual action and real damage.

In this study, we highlight only psychological harm, reputational damage, and material damage as examples of harm from metacrimes.

Psychological harm is an obvious and widespread type of harm that can be inflicted in a virtual environment. The experience of virtual realities, especially immersive ones created with the help of virtual and augmented reality (VR/AR) technologies, can cause genuine psychological and emotional reactions, making the harm experienced in virtual space as real and significant as the harm caused in the physical environment. A prime example is the UK police investigation into lewd acts committed in immersive virtual reality, during which, according to reports, the victim suffered “psychological and emotional trauma” despite the absence of physical contact[23].

[23] Camber, R. (2024). British police probe VIRTUAL rape in metaverse: young girl’s digital persona ’is sexually attacked by gang of adult men in immersive video game’– sparking first investigation of its kind and questions about extent current laws apply in online world. Daily Mail Online. https://clck.ru/3QGzVQ

Reputational damage caused in the metaverse (for example, dissemination of false brand information, unauthorized use of trademarks on virtual goods, or sale of counterfeit virtual items) can lead to significant and measurable damage to the reputation and financial standing of a company or individual in the real world. A clear illustration is the case Hermès v. Rothschild, when the creation and commercialization of MetaBirkins NFT was recognized as a violation and dilution of trademark rights, which caused reputational and financial damage to Hermès[24].

Material damage, in addition to direct financial damage, covers damage caused to the "digital twin" of a real object, which, in turn, leads to damage to the physical object per se. Digital twins are virtual representations of physical objects, processes, or systems that dynamically simulate and predict the behavior of their (real) physical prototypes (Segovia & Garcia-Alfaro, 2022). They are integrated with real-time data (Segovia & Garcia-Alfaro, 2022), which means that malicious actions or vulnerabilities exploited in the digital twin can directly manifest as damage or failure in the physical twin. In this context, the use of cyber-physical systems is a recognized risk.

The nature of these forms of harm – intangible, digitally mediated, or associated with complex interactions of digital twins – creates significant and unavoidable difficulties with proving. Documenting psychological harm from a virtual deed requires overcoming traditional skepticism about the virtual nature of harm, which is considered less real, which necessitates reliable psychological and medical methods of proving. Reputational damage, although it has tangible consequences, is often diffuse, difficult to quantify accurately, and can spread rapidly in the digital space. Material damage caused to digital twins requires highly specialized forensic computer analysis to establish an accurate cause-and-effect relationship between the digital attack and the physical consequences. In these cases, the case is not limited to "classical" physical evidence.

All this indicates a significant and growing demand for specialized forensic expertise (for example, digital psychologists, brand evaluators, forensic analysts of cyber-physical systems) and for the development of new legal standards for digital evidence. The rules of proving should be adapted to account for and evaluate new forms of evidence related to intangible and digital-mediated damage.

## Conclusion

The development of virtual worlds, a metaverse with their inherent properties of decentralization, stability and immersiveness, makes it difficult to apply the traditional principles of determining the operation of criminal law in space. Well-established legal

[24] Hermes International et al v. Rothschild, No. 1:2022cv00384 – Document 140 (S.D.N.Y. 2023). https://clck.ru/3QGzYA

approaches, conditioned by the physical borders (territory) of the state and the interaction of persons in objective reality, turn out to be untenable in relation to crimes committed in virtual spaces that do not have defined boundaries. The cases cited in this paper, ranging from violations of intellectual property rights to property crimes and crimes against sexual integrity, confirm the existence of a serious gap in modern criminal law regarding the definition of the crime scene in the metaverse.

In order to overcome this deepening jurisdictional gap, this article proposes a multifactorial model of jurisdiction in which the crime scene is considered not as a specific point in space, but as a distributed system consisting of individual components. This paradigm shift, based on an analysis of the offender's digital identity, the nature and location of digital assets, management protocols embedded in the platform code, and the material damage caused, allows for a comprehensive framework for determining criminal jurisdiction.

In particular, the model substantiates that the immutable and verifiable nature of blockchain transactions can serve as the legal equivalent of a physical presence to establish personal jurisdiction. In addition, the classification of digital assets as an independent form of property allows direct application of in rem jurisdiction, while the principle of "code management" helps to establish jurisdiction over organizations or individuals responsible for the protocol development and control. At the same time, the harm factor ensures victims' access to justice, linking virtual offenses with their material consequences in the physical world.

For all its theoretical persuasiveness and expediency, the proposed model is not devoid of internal limitations that force one to assess it critically. The establishment of jurisdiction based on the offender's digital identity, although theoretically justified, largely depends on overcoming the "blockchain paradox" – the internal contradiction between the anonymity of pseudonymous digital wallets and the traceability of basic activity. The effectiveness of this approach depends on the development and implementation (at the global level) of strict rules for centralized exchanges and the future creation of mechanisms to identify the persons behind decentralized identification data. The problem posed by completely decentralized exchanges (DEXs), which often circumvent such data collection measures, remains a major obstacle requiring further scientific research and legal regulation.

Similarly, although the classification of digital assets as property simplifies the application of in rem jurisdiction, practical enforcement mechanisms for assets located exclusively in decentralized networks, without interaction with centralized gateways, remain insufficiently developed. Dependence on the identification of the Internet physical infrastructure (for example, hosting providers) to establish jurisdiction over purely decentralized assets, although necessary, is a conceptual contradiction with the very essence of decentralization.

The principle of "code management" as a jurisdictional link also presents a semantic dilemma. The proposal to provide formal legal structures and status to decentralized autonomous organizations, while extremely important for ensuring the unavoidable responsibility, inherently reintroduces a certain degree of centralization, which contradicts the fundamental principles of decentralization. A pragmatic balance between ensuring legal responsibility and preserving the main advantages of decentralization, such as the absence of censorship and the innovation promotion, requires constant discussion and the potential development of hybrid legal structures.

Finally, although the harm factor provides an important physical connection, the intangible and digitally mediated nature of harm such as mental suffering, reputational damage, and damage caused to digital twins is fraught with certain difficulties in proving. To overcome traditional skepticism about the virtual nature of harm, we need to develop new research methodologies, as well as to adapt the rules of evidence to account for and evaluate these new forms of digital evidence.

Therefore, future research should focus on a number of important areas. First, it is advisable to conduct comparative legal studies to clarify how different jurisdictions are currently dealing with these issues and to identify best practices for cross-border cooperation in investigations of crimes related to the metaverse. Second, it is extremely important to develop standardized international protocols on data exchange and mutual legal assistance in the search and collection of evidence based on blockchain technology. Third, interdisciplinary research involving legal scholars and computer scientists is crucial for clarifying the technical and conceptual understanding of digital identity, ownership of digital assets, and the nature of damage in virtual environments. Finally, we believe that legislative initiatives should go beyond reactive adaptation but proactively create a comprehensive legal framework that should be inherently scalable and sustainable under the rapid technological changes characteristic of the metaverse. Only through such concerted and collaborative efforts can the international community hope to create a reliable and fair system of justice in the emerging digital environment of the metaverse.

## References

Aakula, A., Sandhu, K., Srinivasan Venkataramanan, V., Alluri, R. R., & Saini, V. (2023). Forging Unbreakable Identities: The Biometric-Blockchain Nexus. *Nanotechnology Perceptions*, *19*, 644–652. https://doi.org/10.62441/nano-ntp.v19i3.5078

Bains, P., Ismail, A., Melo, F., & Sugimoto, N. (2022). Regulating the crypto ecosystem: The case of unbacked crypto assets. *International Monetary Fund*.

Benson, V., Turksen, U., & Adamyk, B. (2024). Dark side of decentralised finance: a call for enhanced AML regulation based on use cases of illicit activities. *Journal of Financial Regulation and Compliance*, *32*(1), 80–97. https://doi.org/10.1108/JFRC-04-2023-0065

Bhowmik, A. K. (2024). Virtual and augmented reality: Human sensory-perceptual requirements and trends for immersive spatial computing experiences. *Journal of the Society for Information Display*, *32*(8), 605–646. https://doi.org/10.1002/jsid.2001

Brey, P. (2025). Will There Be a Metaverse? In The Metaverse: A Critical Assessment. *SpringerBriefs in Ethics* (pp. 33–57). Springer, Cham. https://doi.org/10.1007/978-3-031-93471-1_3

Chimni, B. S. (2022). The international law of jurisdiction: A TWAIL perspective. *Leiden Journal of International Law*, *35*(1), 29–54. https://doi.org/10.1017/S0922156521000534

Esakov, G. A. (2015). Extraterritorial criminal jurisdiction: contemporary global trends. *Statute*, *8*, 82–89. (In Russ.).

Han, E., Miller, M. R., DeVeaux, C., Jun, H., Nowak, K. L., Hancock, J. T., Ram, N., & Bailenson, J. N. (2023). People, places, and time: a large-scale, longitudinal study of transformed avatars and environmental context in group interaction in the metaverse. *Journal of Computer-Mediated Communication*, *28*(2), zmac031. https://doi.org/10.1093/jcmc/zmac031

Hosseini, S., Abbasi, A., Magalhaes, L. G., Fonseca, J. C., da Costa, N. M., Moreira, A. H., & Borges, J. (2024). Immersive interaction in digital factory: Metaverse in manufacturing. *Procedia Computer Science*, *232*, 2310–2320. https://doi.org/10.1016/j.procs.2024.02.050

Ioannıdıs, S., & Kontıs, A. P. (2023). The 4 Epochs of the Metaverse. *Journal of Metaverse*, *3*(2), 152–165. https://doi.org/10.57019/jmv.1294970

Judge, B., Nitzberg, M., & Russell, S. (2025). When code isn't law: rethinking regulation for artificial intelligence. *Policy and Society*, *44*(1), 85–97. https://doi.org/10.1093/polsoc/puae020

Kim, H. S., Kim, S., & Lee, E. J. (2025). The mirror of the metaverse: an exploration of reciprocal effects between self-views and avatar-based self-presentation. *Human Communication Research*, *51*(3), 142–152. https://doi.org/10.1093/hcr/hqaf005

Komalavalli, C., Saxena, D., & Laroiya, C. (2020). Overview of blockchain technology concepts. In *Handbook of research on blockchain technology* (pp. 349–371). Academic Press.

McStay, A. (2023). The metaverse: Surveillant physics, virtual realist governance, and the missing commons. *Philosophy & Technology*, *36*(1), 13. https://doi.org/10.1007/s13347-023-00613-y

Niesel, Z. (2023). Crypto Contacts: Jurisdiction and the Blockchain. *Tulane Law Review*, *98*, 917.

Özkan, A., & Özkan, H. (2024). Meta: XR-AR-MR and mirror world technologies business impact of metaverse. *Journal of Metaverse*, *4*(1), 21–32. https://doi.org/10.57019/jmv.1344489

Panda, S. K. (2023). Revolution of the metaverse and blockchain technology. In *Metaverse and immersive technologies: An introduction to industrial, business and social applications* (pp. 97–125). https://doi.org/10.1002/9781394177165.ch4

Payer, A. (2023). The Territorial Principle as a Basis for State Criminal Jurisdiction: Particularly with Regard to Cross-Border Offences and Attempts, and to Multiple Parties to an Offence Acting in Different Countries. *International Criminal Law Review*, *23*(2), 175–238. https://doi.org/10.1163/15718123-bja10151

Pesqueira, A. (2025). The Impact and Potential. In A. Pesqueira, & A. de Bem Machado (Eds.), *Navigating Privacy, Innovation, and Patient Empowerment Through Ethical Healthcare Technology* (pp. 217–254). IGI Global. https://doi.org/10.4018/979-8-3693-7630-0

Pogorzelska, K. (2024). Does Using Satellite Data for Sustainable Development Justify Unsustainable Use of Outer Space? In *Regulation of Outer Space* (pp. 7–25). Routledge. https://doi.org/10.4324/9781003512677

Qin, R., Ding, W., Li, J., Guan, S., Wang, G., Ren, Y., & Qu, Z. (2022). Web3-based decentralized autonomous organizations and operations: Architectures, models, and mechanisms. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *53*(4), 2073–2082. https://doi.org/10.1109/TSMC.2022.3228530

Richter, S., & Richter, A. (2023). What is novel about the Metaverse? *International Journal of Information Management*, *73*, 102684. https://doi.org/10.1016/j.ijinfomgt.2023.102684

Rokhsaritalemi, S., Sadeghi-Niaraki, A., & Choi, S. M. (2020). A review on mixed reality: Current trends, challenges and prospects. *Applied Sciences*, *10*(2), 636. https://doi.org/10.3390/app10020636

Ryngaert, C. (2023). Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. *German Law Journal*, *24*(3), 537–550. https://doi.org/10.1017/glj.2023.24

Scharfman, J. (2024). Decentralized autonomous organization (dao) fraud, hacks, and controversies. In *The Cryptocurrency and Digital Asset Fraud Casebook, Volume II: DeFi, NFTs, DAOs, Meme Coins, and Other Digital Asset Hacks* (pp. 65–106). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-60836-0_3

Schuler, K., Cloots, A. S., & Schär, F. (2024). On DeFi and on-chain CeFi: how (not) to regulate decentralized finance. *Journal of Financial Regulation*, *10*(2), 213–242. https://doi.org/10.1093/jfr/fjad014

Segovia, M., & Garcia-Alfaro, J. (2022). Design, modeling and implementation of digital twins. *Sensors*, *22*(14), 5396. https://doi.org/10.3390/s22145396

Syed, T. A., Siddiqui, M. S., Abdullah, H. B., Jan, S., Namoun, A., Alzahrani, A., Nadeem, A., & Alkhodre, A. B. (2022). In-depth review of augmented reality: Tracking technologies, development tools, AR displays, collaborative AR, and security concerns. *Sensors*, *23*(1), 146. https://doi.org/10.3390/s23010146

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, *11*(1), 1. https://doi.org/10.1186/s40163-021-00163-8

Wei, W. (2023). Using actor–network theory to revisit the digitalized tool in social design. *The Design Journal*, *27*(1), 49–67. https://doi.org/10.1080/14606925.2023.2279836

Wendehorst, C. (2023). Proprietary rights in digital assets and the conflict of laws. In *Blockchain and Private International Law* (pp. 101–127). Brill Nijhoff. https://doi.org/10.1163/9789004514850_007

## Author information

**Murad M. Madzhumaev** – Cand. Sci. (Law), Leading researcher, Senior Lecturer, Department of Criminal Law, Criminal Procedure and Criminology, Institute of Law, Peoples' Friendship University of Russia named after Patrice Lumumba
**Address**: 6 Miklukho-Maklaya Str., 117198 Moscow, Russia
**E-mail**: murad.mad@outlook.com
**ORCID ID**: https://orcid.org/0000-0003-3332-2850
**Scopus Author ID**: https://www.scopus.com/authid/detail.uri?authorId=58624042900
**WoS Researcher ID**: https://www.webofscience.com/wos/author/record/ABB-9737-2021
**Google Scholar ID:** https://scholar.google.com/citations?user=qpGC84MAAAAJ
**RSCI Author ID**: https://www.elibrary.ru/author_items.asp?authorid=1212027

## Conflict of interest

The author declares no conflict of interest.

## Financial disclosure

The research was made under the grant of the Russian Scientific Fund No. 25-28-01478. https://rscf.ru/project/25-28-01478/

## Thematic rubrics

**OECD**: 5.05 / Law
**PASJC**: 3308 / Law
**WoS**: OM / Law

## Article history

**Date of receipt** – August 21, 2025
**Date of approval** – September 4, 2025
**Date of acceptance** – December 20, 2025
**Date of online placement** – December 25, 2025

**Научная статья**
**УДК 34:004:343.213.3:343.232:343.235.4**
**EDN:** https://elibrary.ru/rowsaq
**DOI:** https://doi.org/10.21202/jdtl.2025.23

# Многофакторная модель юрисдикции: переосмысление места преступления в децентрализованной метавселенной

**Мурад Мамедович Маджумаев**

Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия

## Ключевые слова

аватар,
виртуальная реальность,
дополненная реальность,
место преступления,
метавселенная,
право,
преступление,
уголовное право,
цифровые технологии,
юрисдикция

## Аннотация

**Цель**: провести критический анализ возможности распространения существующих принципов действия уголовного закона в пространстве на деяния, совершенные в децентрализованных виртуальных мирах метавселенной, и разработать предложения, включающие обновление подхода к установлению юрисдикции в отношении таких виртуальных преступлений.

**Методы**: методологическую основу исследования составляет совокупность общенаучных методов и подходов научного познания – диалектический, формально-логический (анализ и синтез, индукция и дедукция), системный, а также частно-научные методы – формально-правовой, правовое моделирование, толкование. Исследование опирается на анализ судебной практики, зарубежного законодательства, технических особенностей блокчейн-технологий и децентрализованных автономных организаций, что позволяет выявить пробелы в правовом регулировании и предложить концептуально новые решения для определения места совершения преступления в виртуальной среде.

**Результаты**: выявлена ограниченность реализации существующих общепринятых принципов определения юрисдикции в отношении виртуальных преступлений, которые не имеют физических координат. Предлагаемая многофакторная модель юрисдикции переопределяет «место преступления» с учетом таких факторов, как цифровая идентичность правонарушителя, характер и местонахождение цифровых активов, протоколы управления платформой и причиненный реальный ущерб. Предполагается, что неизменяемый и верифицируемый характер операций в блокчейне может служить своеобразным юридическим эквивалентом физического присутствия для установления персональной юрисдикции, позволяя инициировать уголовное преследование даже в тех случаях, когда фактическое местонахождение правонарушителя остается неизвестным.

**Научная новизна**: в работе изложен подход, предполагающий фундаментальное преобразование реактивных, адаптивных принципов правового регулирования в проактивную, комплексную основу, предназначенную специально для уникальных вызовов метавселенной. Выдвинута меняющая парадигму гипотеза, которая заключается в том, что постоянный (устойчивый) цифровой след правонарушителя в виртуальных пространствах может служить основой для осуществления юрисдикции. В модели системно увязано представление о вреде как важнейшем звене между виртуальными правонарушениями и их последствиями в реальном мире.

**Практическая значимость**: обусловлена отсутствием в настоящее время возможности применения к отношениям в метавселенной правовых норм и правил, учитывающих их специфику. Основные положения и выводы исследования могут быть использованы для совершенствования механизмов правового регулирования метавселенной, формирования международных протоколов об обмене данными и взаимной правовой помощи в вопросах поиска и сбора доказательств, основанных на технологии блокчейн, а также для разработки законодательных инициатив, направленных на создание комплексных правовых механизмов, масштабируемых и устойчивых к быстрым технологическим изменениям, характерным для цифровой среды.

## Для цитирования

Маджумаев, М. М. (2025). Многофакторная модель юрисдикции: переосмысление места преступления в децентрализованной метавселенной. *Journal of Digital Technologies and Law*, *3*(4), 570–597. https://doi.org/10.21202/jdtl.2025.23

## Список литературы

Есаков, Г. А. (2015). Экстратерриториальное действие уголовного закона: современные мировые тенденции. *Закон*, *8*, 82–89. https://elibrary.ru/uhlbaf

Aakula, A., Sandhu, K., Srinivasan Venkataramanan, V., Alluri, R. R., & Saini, V. (2023). Forging Unbreakable Identities: The Biometric-Blockchain Nexus. *Nanotechnology Perceptions*, *19*, 644–652. https://doi.org/10.62441/nano-ntp.v19i3.5078

Bains, P., Ismail, A., Melo, F., & Sugimoto, N. (2022). Regulating the crypto ecosystem: The case of unbacked crypto assets. *International Monetary Fund*.

Benson, V., Turksen, U., & Adamyk, B. (2024). Dark side of decentralised finance: a call for enhanced AML regulation based on use cases of illicit activities. *Journal of Financial Regulation and Compliance*, *32*(1), 80–97. EDN: https://elibrary.ru/fgebbr. DOI: https://doi.org/10.1108/JFRC-04-2023-0065

Bhowmik, A. K. (2024). Virtual and augmented reality: Human sensory-perceptual requirements and trends for immersive spatial computing experiences. *Journal of the Society for Information Display*, *32*(8), 605–646. EDN: https://elibrary.ru/bxivih. DOI: https://doi.org/10.1002/jsid.2001

Brey, P. (2025). Will There Be a Metaverse? In *The Metaverse: A Critical Assessment. SpringerBriefs in Ethics* (pp. 33–57). Springer, Cham. https://doi.org/10.1007/978-3-031-93471-1_3

Chimni, B. S. (2022). The international law of jurisdiction: A TWAIL perspective. *Leiden Journal of International Law*, *35*(1), 29–54. EDN: https://elibrary.ru/gqkwgf. DOI: https://doi.org/10.1017/S0922156521000534

Han, E., Miller, M. R., DeVeaux, C., Jun, H., Nowak, K. L., Hancock, J. T., Ram, N., & Bailenson, J. N. (2023). People, places, and time: a large-scale, longitudinal study of transformed avatars and environmental context in group interaction in the metaverse. *Journal of Computer-Mediated Communication*, *28*(2), zmac031. EDN: https://elibrary.ru/qlwgxi. DOI: https://doi.org/10.1093/jcmc/zmac031

Hosseini, S., Abbasi, A., Magalhaes, L. G., Fonseca, J. C., da Costa, N. M., Moreira, A. H., & Borges, J. (2024). Immersive interaction in digital factory: Metaverse in manufacturing. *Procedia Computer Science*, *232*, 2310–2320. EDN: https://elibrary.ru/skunaz. DOI: https://doi.org/10.1016/j.procs.2024.02.050

Ioannıdıs, S., & Kontıs, A. P. (2023). The 4 Epochs of the Metaverse. *Journal of Metaverse*, *3*(2), 152–165. EDN: https://elibrary.ru/mwvqcn. DOI: https://doi.org/10.57019/jmv.1294970

Judge, B., Nitzberg, M., & Russell, S. (2025). When code isn't law: rethinking regulation for artificial intelligence. *Policy and Society*, *44*(1), 85–97. https://doi.org/10.1093/polsoc/puae020

Kim, H. S., Kim, S., & Lee, E. J. (2025). The mirror of the metaverse: an exploration of reciprocal effects between self-views and avatar-based self-presentation. *Human Communication Research*, *51*(3), 142–152. https://doi.org/10.1093/hcr/hqaf005

Komalavalli, C., Saxena, D., & Laroiya, C. (2020). Overview of blockchain technology concepts. In *Handbook of research on blockchain technology* (pp. 349–371). Academic Press. https://doi.org/10.1016/B978-0-12-819816-2.00014-9

McStay, A. (2023). The metaverse: Surveillant physics, virtual realist governance, and the missing commons. *Philosophy & Technology*, *36*(1), 13. EDN: https://elibrary.ru/rgzoum. DOI: https://doi.org/10.1007/s13347-023-00613-y

Niesel, Z. (2023). Crypto Contacts: Jurisdiction and the Blockchain. *Tulane Law Review*, *98*, 917.

Özkan, A., & Özkan, H. (2024). Meta: XR-AR-MR and mirror world technologies business impact of metaverse. *Journal of Metaverse*, *4*(1), 21–32. https://doi.org/10.57019/jmv.1344489

Panda, S. K. (2023). Revolution of the metaverse and blockchain technology. In *Metaverse and immersive technologies: An introduction to industrial, business and social applications* (pp. 97–125). https://doi.org/10.1002/9781394177165.ch4

Payer, A. (2023). The Territorial Principle as a Basis for State Criminal Jurisdiction: Particularly with Regard to Cross-Border Offences and Attempts, and to Multiple Parties to an Offence Acting in Different Countries. *International Criminal Law Review*, *23*(2), 175–238. EDN: https://elibrary.ru/ipnrgk. DOI: https://doi.org/10.1163/15718123-bja10151

Pesqueira, A. (2025). The Impact and Potential. In A. Pesqueira, & A. de Bem Machado (Eds.), *Navigating Privacy, Innovation, and Patient Empowerment Through Ethical Healthcare Technology* (pp. 217–254). IGI Global. https://doi.org/10.4018/979-8-3693-7630-

Pogorzelska, K. (2024). Does Using Satellite Data for Sustainable Development Justify Unsustainable Use of Outer Space? In *Regulation of Outer Space* (pp. 7–25). Routledge. https://doi.org/10.4324/9781003512677

Qin, R., Ding, W., Li, J., Guan, S., Wang, G., Ren, Y., & Qu, Z. (2022). Web3-based decentralized autonomous organizations and operations: Architectures, models, and mechanisms. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *53*(4), 2073–2082. https://doi.org/10.1109/TSMC.2022.3228530

Richter, S., & Richter, A. (2023). What is novel about the Metaverse? *International Journal of Information Management*, *73*, 102684. EDN: https://elibrary.ru/sxufzu. DOI: https://doi.org/10.1016/j.ijinfomgt.2023.102684

Rokhsaritalemi, S., Sadeghi-Niaraki, A., & Choi, S. M. (2020). A review on mixed reality: Current trends, challenges and prospects. *Applied Sciences*, *10*(2), 636. EDN: https://elibrary.ru/hgwqbi. DOI: https://doi.org/10.3390/app10020636

Ryngaert, C. (2023). Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. *German Law Journal*, *24*(3), 537–550. EDN: https://elibrary.ru/dbquas. DOI: https://doi.org/10.1017/glj.2023.24

Scharfman, J. (2024). Decentralized autonomous organization (dao) fraud, hacks, and controversies. In *The Cryptocurrency and Digital Asset Fraud Casebook, Volume II: DeFi, NFTs, DAOs, Meme Coins, and Other Digital Asset Hacks* (pp. 65–106). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-60836-0_3

Schuler, K., Cloots, A. S., & Schär, F. (2024). On DeFi and on-chain CeFi: how (not) to regulate decentralized finance. *Journal of Financial Regulation*, *10*(2), 213–242. EDN: https://elibrary.ru/kjghty. DOI: https://doi.org/10.1093/jfr/fjad014

Segovia, M., & Garcia-Alfaro, J. (2022). Design, modeling and implementation of digital twins. *Sensors*, *22*(14), 5396. EDN: https://elibrary.ru/whsffs. DOI: https://doi.org/10.3390/s22145396

Syed, T. A., Siddiqui, M. S., Abdullah, H. B., Jan, S., Namoun, A., Alzahrani, A., Nadeem, A., & Alkhodre, A. B. (2022). In-depth review of augmented reality: Tracking technologies, development tools, AR displays, collaborative AR, and security concerns. *Sensors*, *23*(1), 146. EDN: https://elibrary.ru/rxwauu. DOI: https://doi.org/10.3390/s23010146

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, *11*(1), 1. EDN: https://elibrary.ru/kwtfwh. DOI: https://doi.org/10.1186/s40163-021-00163-8

Wei, W. (2023). Using actor–network theory to revisit the digitalized tool in social design. *The Design Journal*, *27*(1), 49–67. https://doi.org/10.1080/14606925.2023.2279836

Wendehorst, C. (2023). Proprietary rights in digital assets and the conflict of laws. In *Blockchain and Private International Law* (pp. 101–127). Brill Nijhoff. https://doi.org/10.1163/9789004514850_007

## Сведения об авторе

**Маджумаев Мурад Мамедович** – кандидат юридических наук, ведущий научный сотрудник, старший преподаватель кафедры уголовного права, уголовного процесса и криминалистики Юридического института, Российский университет дружбы народов имени Патриса Лумумбы
**Адрес**: 117198, Россия, г. Москва, ул. Миклухо-Маклая, д. 6
**E-mail**: murad.mad@outlook.com
**ORCID ID**: https://orcid.org/0000-0003-3332-2850
**Scopus Author ID**: https://www.scopus.com/authid/detail.uri?authorId=58624042900
**WoS Researcher ID**: https://www.webofscience.com/wos/author/record/ABB-9737-2021
**Google Scholar ID**: https://scholar.google.com/citations?user=qpGC84MAAAAJ
**РИНЦ Author ID**: https://www.elibrary.ru/author_items.asp?authorid=1212027

## Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

## Финансирование

Исследование выполнено за счет гранта Российского научного фонда № 25-28-01478. https://rscf.ru/project/25-28-01478/

## Тематические рубрики

**Рубрика OECD**: 5.05 / Law
**Рубрика ASJC**: 3308 / Law
**Рубрика WoS**: OM / Law
**Рубрика ГРНТИ**: 10.07.45 / Право и научно-технический прогресс
**Специальность ВАК**: 5.1.4 / Уголовно-правовые науки

## История статьи

**Дата поступления** – 21 августа 2025 г.
**Дата одобрения после рецензирования** – 4 сентября 2025 г.
**Дата принятия к опубликованию** – 20 декабря 2025 г.
**Дата онлайн-размещения** – 25 декабря 2025 г.