On the curiosities of the future: meta criminal law

Laura Maria Stănilă[1*]

[1] Faculty of Law, West University of Timișoara, Centre for Research in Criminal Sciences, Romania

Abstract: The new virtual realm – *Metaverse* – despite its entertaining potential and features, comes with a lot of threats and perils, and tends to seriously challenge the legal system. The lack of regulation, the increasing number of users and the occurrence of new acts that can be committed solely in Metaverse are just a few topics this article aims to address. The author proposes the creation of a new branch of law – Meta - Criminal Law and asks for immediate intervention of the national and international legislators to create a frame system to protect the users of virtual platforms and ensure their safety.

1 Metaverse as an Alternate Reality

Criticized by the scholars due to the inequalities risen based on economic limitations, Metaverse keeps being a hot topic in scholarly and Media discussions. „Unlike the previous disruptive iterations of internet-age projects, Metaverse has been proactively grappled with by various types of scholars and writers. The cautionary tales set by *The Matrix, Ready Player One,* and *Snow Crash* already paint a dystopian picture in the popular imagination. The equity markets are also punishing Facebook (meta) for several reasons including the overinvestment and poor reception of the meta project (in addition to declining user base)" [1].

As shown by the foreign literature, the physical world is no longer the necessary arena of human activity. Cyberspace gives us a new, non-spatial arena in which we can conduct many, if not all, of the activities we carry out in the physical world. The availability of this new, conceptual vector for human activity has various consequences for criminal law [2]. And, if that wasn't enough Metaverse as a newly created virtual world comes and further challenges the Law in general and Criminal law.

The term Metaverse is a combination of the prefix *meta* (Greek term for *transcendence*) and the suffix *verse* (short for *Universe*) and is used to denote "a computer-generated world with a consistent value system and an independent economic system connected to the world physics" [3]. *Metaverse* is a term applying to a wide range of technologies that aim to merge the social connections of the real world with the innovations of the digital age. The term *Metaverse* was first used in a 1992 dystopian sci-fi novel by writer Neal Stephenson, *Snow Crash*. The book describes a world where governments have been replaced by corporations, the global economy has collapsed, while citizens escape this bleak reality by accessing a virtual world through headsets. There, their avatars can roam the digital realm, own virtual

* Corresponding author: laura.stanila@e-uvt.ro

property, and socialize with other avatars. This dystopian future imagined by the author does not correspond to the foundation of the emergence and development of the Metaverse in our world. Instead, it has evolved through increased digitization and the emergence of new technologies and multiple innovations such as crypto-assets and blockchain, these configuring the so-called web *3.0 Metaverse* [4].

Metaverse is considered an extended reality platform (*extended reality* - XR), which however, faces multiple problems such as viruses, the current impossibility of imposing age limits on users because many virtual games are Metaverse worlds. This allows adults to interact with minors very easily and engage them in dangerous behaviours. In addition, the exponential growth of users, individuals, or companies, has made this virtual realm extremely crowded and therefore, a regulation and a planning of the situation in the future being as difficult as it is necessary. There are nearly 200 companies operating in the Metaverse. New technologies such as 5G or 6G and Web 3.0 will further accelerate social relations in the Metaverse by connecting the 7.9 billion users in the real world [5].

Because the lack of technical knowledge of non-IT public, it is necessary to define some specific terms used in reference to Metaverse analysis. Virtual reality (VR) and augmented reality (AR) are the main terms in the media, both being used for about 30 years, with VR emerging in the late 1980s and AR in the early 1990s. The key difference between them consists in the perception of the user. In VR, the user feels present within a simulated environment, while in AR the user feels present in a combined world of real and virtual content [6]. *Virtual reality (VR)* is an immersive and interactive simulated environment that is experienced in the first person and provides a strong sense of presence to the user. *Augmented reality (AR)* is an immersive and interactive environment in which virtual content is spatially registered to the real world and experienced in the first person, providing a strong sense of presence in a combined real/virtual space. *Extended reality (XR)* emerged to describe the full spectrum of VR and AR capabilities.

The connection between these terms is explained in the Fig. 1 [6]:

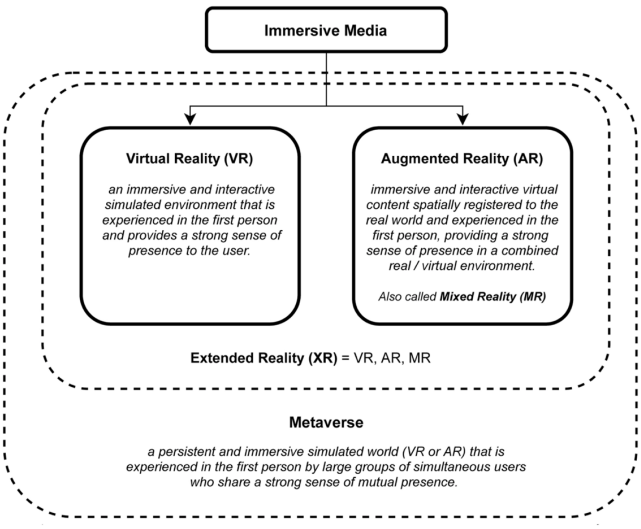

Fig. 1. Explanation of VR, AR and XR and the connection between them.

In general, the development of the Metaverse is expected to go through three successive phases (now in progress) as follows: (a) the digital twin, (b) the digital native, and finally (c) the sur-reality [3]. The first phase involves the creation of a mirror world, a digital copy of the real world in which we find the digital twins of people and things in physical reality; In

this first phase the Metaverse is a digital representation of physical reality. In this phase, the user's behaviour and emotions are imitations from the physical world, the virtual space being parallel to the physical world. The second phase focuses mainly on native content creation, where digital natives represented by avatars can produce innovations and insights within digital worlds, and these digital creations can only exist in virtual spaces. In this phase, the contents created massively in the digital world become equal to those created in the physical world, and the digital world can transform and innovate the production process of the physical world, thus creating more intersections between these two worlds. Finally, in the last phase, the Metaverse grows to maturity and transforms into a persistent and self-sustaining hyperreality that assimilates reality into itself. The perfect integration and mutual symbiosis of the physical and virtual worlds will be achieved in this phase, where the scope of the virtual world will be greater than that of the real world.

Finally, we must point out that there are several visions as regards Metaverse: for some Metaverse is the evolution of internet, or an embodied internet, for others, Metaverse includes immersive offline experiences that enable users to experience a different reality, or a combination of the physical and virtual world in a type of mixed reality [7]. For sure, Metaverse is one of the core topics of concern for several international bodies, including Europol.

2 Should we regulate Metaverse?

In our opinion, the need to regulate metaverse is imperative. It is obvious that Metaverse will bring together a range of digital activities [8] as shown in the Fig. 2 bellow:

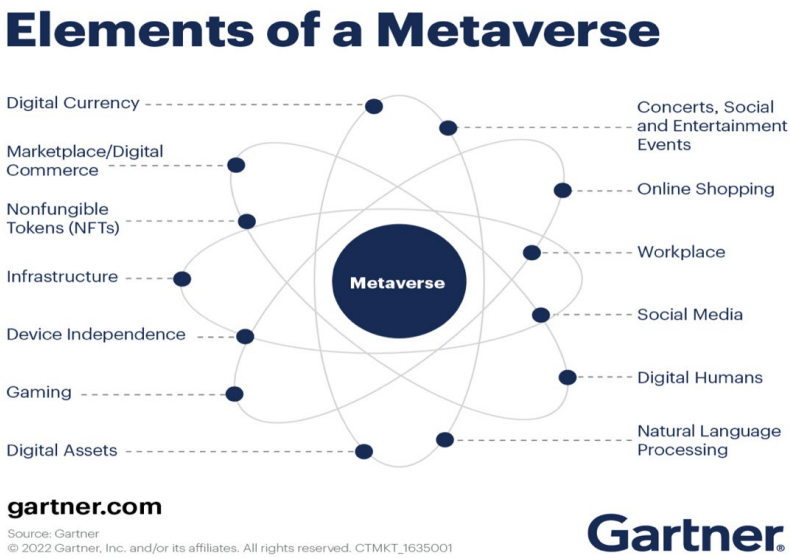

Fig. 2. Elements of a Metaverse.

The diversification of social relations in metaverse and the increase of number of users brings a whole new category of perils and threats for humans, jeopardizing their rights and freedoms. While the present criminal regulations tend to cover physical deeds committed in

the physical reality, and even the cybercrime rules deal with physical acts committed through computers, the deeds committed in Metaverse have no correspondence with the previous.

The key perils of Metaverse have been divided into three categories named as the three „M" s of Metaverse [9]: monitoring, manipulation, and monetization.

Monitoring. Aggressively targeting users for advertising purposes has exploited consumers, caused reduced personal privacy, and has made social media a polarizing force by allowing third parties to deploy customize messaging that is skilfully aimed at very specific demographic groups. This led to the amplification of existing biases in populations and spread misinformation, worsening in the Metaverse. The technology in Metaverse will not just track where users click, but where they go, who they are with, what they do, what they look at, even how long their gaze lingers, it will also track facial expressions, vocal inflections, and vital signs, while intelligent algorithms use such data to predict each person's real-time emotional state.

Manipulating. Nowadays custom targeted advertising has greatly increased the persuasive ability of promotional messaging and in Metaverse, such targeting will get far more personal, and the content will get much harder to resist.

Monetizing. Platform providers are commercial entities requiring substantial revenue to support the interests of the employees and shareholders. Until now, only a small part of the public has paid subscriptions for access to online platforms, so they must rethink their business model to increase the number of paying users. It was suggested that the most common industry model is to provide free access in exchange for widespread advertising, focusing largely on targeted ads that can be precisely delivered based on the unique behaviours and interests of individual users. That is why the platform providers are pursuing extensive tracking and profiling of their users.

Because the underlying technologies of the Metaverse are specifically designed to trick the senses, deliberately blurring the line between authentic and fabricated experiences, we can expect deceptive abuses of social media to be greatly amplified.

This context triggers the question: does Metaverse worth it?

Despite the risks, the immersive technologies of virtual and augmented reality have the potential to make our lives magical, unleashing creativity more powerfully than ever, even expanding what it means to be human. Still, to avoid potential problems, governments and industry players need to consider significant strict regulations.

In addition, a regulation of Metaverse should be considered promptly, before profound effects on Metaverse's infrastructure and business models be caused, so that they become difficult or even impossible to solve.

As shown in the previous section of the present study, users of Metaverse are extremely vulnerable. Their vulnerability is the result of multiple factors, among which two are popping: new types of deeds adapted to the specifics of the XR and VR realm and the lack of legal rules. The vulnerability of the users in the metaverse asserts the need for the immediate discourse around the rules, regulations or laws that would be implemented in these virtual worlds before the embodied internet materializes [10].

Three directions to address the issue of regulating Metaverse were identified by the scholars, as follows:

a) the harsh modernization of the way crime is viewed through extraterritoriality in the virtual world - including broadening the scope of punitive action and identifying the actors in Metaverse that would have to incur liability; this approach would be a complete review of the current schools of thought pertaining to criminal law and jurisdiction – identifying victims and perpetrators to include AI, AR players and imposition of liability on them.

b) formation of regulatory penal laws of the exact nature and scope of international or transnational laws; this approach is to be materialized after taking into consideration the

extent at which activities of criminal nature could take place in Metaverse. In this regard the universal jurisdiction principle has been proposed.

c) decentralizing the criminal legislation process by entrusting the corporations involved with regulatory powers. This third approach focuses on the fact that the regulations are made in effect of existing laws pertaining to technology that will interlink with Big Tech's Terms and Conditions of Service. Regulations acknowledge that criminal jurisdiction is intrinsically connected to state recognition and state sanctioned liabilities. Nevertheless, in technology, the development occurs at a too high rate for state action to respond by designing proper legal rules. For these reasons, the stakeholders should provide Terms and Conditions of use to establish the limits of users' actions, while in other situations are given the role of a mere intermediary.

3 Metaverse and Criminal Law

Participating in online games that request the use of avatars sometimes involves committing crimes as part of that game. Metaverse is, manly, a realm of games and entertainment. It is interesting to note that certain deeds are impossible to commit in a virtual world due to code restrictions. In other words, if the designers create such a platform that allows crimes to be committed, they will be committed. On the other hand, the creation of "restrictive" codes regarding criminality does not guarantee that potentially harmful or dangerous acts will not be committed in that environment. The key question that is to be addressed in this matter is: for whom these risks consist of a threat? For the avatar or for the man behind it (using it)? In most cases, if someone commits such acts in a virtual world, they will most likely be warned, suspended, or permanently banned on the platform because, for now, the presence in the virtual world of the Metaverse is based on the idea of the game. However, the development direction of Metaverse with the increase of transactions on virtual properties, moving some businesses into the virtual environment and even creating virtual copies of real cities (such as Seoul [11]) or real spaces (e.g., museums in virtual format whose number of visitors increases every day [12]) shows that the game phase is starting to pass, and things are taking a serious turn. Could such conducts occur in the virtual world being sufficiently harmful to claim the intervention of criminal law and, therefore, the application of punishment in real life? In general, if an incident occurred in a virtual world result in injury, harm or endangerment of a real-life value, there could obviously be legal consequences in real life. But this is extremely difficult to achieve at the present time under the conditions in which the principle of the legality of incrimination forces the verification of the typicality conditions of the concrete act to make it possible to engage the criminal liability.

It has been shown that, „in general, developers of virtual worlds do not want real-world laws applied to their platforms. Mainly because they want to control their world to maximize revenue from users while allowing them to have an enjoyable experience. Users probably feel the same way because they don't want to get, say, a speeding ticket for driving 100 km/h in their virtual Bugatti through a virtual school zone. Whether the laws of the real world could apply to a virtual world will depend on how it is set up. But in general, the more realistic a virtual world is, the more likely it is that disputes will be resolved in a real-life court. But that doesn't mean that real-world law enforcement will solve the problems of the virtual world" [13].

In my opinion, the application of real-world criminal law in the Metaverse space depends on three conditions:

a) the will of the creator and the created code; in other words, The Terms and Conditions established to use the platform become part of the legal frame.

b) the typicality of the act; in this regard, the *nullum crimen sine lege* principle is restricting the intervention of criminal law, since the „deeds" committed in the virtual realm are very difficult to compare with the deeds committed in the physical world.

c) producing a consequence – state of peril or result – in the real world; in other words, it is necessary to admit a connection between Metaverse world and real world.

All these being displayed, certain virtual behaviours, obviously harmful or dangerous, committed in Metaverse cannot be included, now, in the pattern given by the classic criminalization rules: e.g., virtual rape [14, 15], virtual destruction, virtual murder [21].

In addition, it is worth to mention that growth of a specific criminal acts was observed by the users of platforms and scholars: theft and destruction of crypto-assets. For example, Elliptic has revealed that there was already illicit activity regarding the assets used in Metaverse MANA and SAND. Of these illicit activities, 99.5% consist of crypto-assets theft. [4] Thus, the most frequent criminal activity currently in the Metaverse virtuality is highlighted.

Obviously, these facts require criminal intervention, and, at present, this is achieved through inadequate legislation, which is mainly intended to be applied to crimes committed in physical reality, by legal subjects recognized in this reality. In the Metaverse and its virtual worlds, we cannot yet discuss legal subjects because avatars do not have a legally recognized independent existence, distinct from the real-world actor. In this regard, in another study, I have proposed the creation of the meta-criminal law and of the categories of meta-criminality and meta-criminal justice. [16]

Trying to identify which present Romanian criminal rules could be applied to harmful or dangerous acts committed in Metaverse, some legal norms provided by Romanian Criminal Code of 2009 felt more adaptable to the virtual realm: Art. 207 – blackmail, Art. 208 – harassment, Art. 360-366 – Offenses against the safety and integrity of computer data, Art. 368 – public incitement, Art. 370 – the attempt to determine the commission of a crime, Art. 374 – child pornography. Still, reviewing the types of threats occurring or emerging in Metaverse identified by the scholars, one can easily notice they are far of being sufficient or efficient.

The specific threats of Metaverse that could require criminal intervention are categorized as follows [3]:

A. Threats to Authentication in Metaverse. In this category the scholars include identity theft in Metaverse, leading to the user's avatars, digital assets, social relationships, and her/his digital life to be leaked and lost; impersonation attack, consisting in pretending to be another authorized entity to gain access to a service or system in the metaverse. It was shown that hackers can invade the helmet and exploit the stolen behavioural and biological data gathered by the in- built motion-tracking system to create digital replicas of the user and impersonate the victim to facilitate social engineering attacks; e.g. avatar authentication issue may appear by creating multiple AI bots (i.e., digital humans) based on facial features, voice, video footage and other authentication items of the real user, which appear, hear, and behave identical to user's real avatar, in the virtual world (e.g., Roblox) by imitating user's appearance, voice, and behaviours .

B. Threats to Access Control in Metaverse, including unauthorized data access, misuse of user/avatar data.

C. Threats to Data Management in Metaverse, including *data* tampering attacks, false data injection attacks, threats to data quality of user generated content (UGC), threats to UGC ownership and provenance, threats to intellectual property protection.

D. Privacy Threats in Metaverse, including pervasive data collection, privacy leakage in data transmission, privacy leakage in data processing; privacy leakage in cloud/edge storage; rogue or compromised end devices; threats to digital footprints; identity linkability in ternary worlds, threats to accountability; threats to customized privacy.

E. Threats to Metaverse Network. In this category the scholars include several types of use of malware such as SPoF, DDoS, Sybil Attacks.

F. Threats to Metaverse Economy, including service trust issues in UGC & virtual object trading; threats to digital asset ownership; threats to economic fairness in creator economy.

G. Threats to Physical World and Human Society. This category is the most important, in my opinion, due to its evident connections between VR/AR and reality and includes threats to personal safety (e.g. an adversary can manipulate a VR device to reset the hardware's physical boundaries, thereby, a user in metaverse can be potentially pushed toward a flight of stairs or misdirected into a crowded street or other dangerous physical situations); *threats to infrastructure safety b*y sniffing the software or system vulnerabilities in the highly integrated metaverse. By this way, hackers may exploit the compromised devices as entry points and invade critical national infrastructures via malware attacks.

As regards the complexity of the Metaverse threats and perils presented above, I emphasize once more the imperative need to create a proper legal criminal framework to protect the users of the virtual worlds, their rights, and freedoms.

4 The Metaverse and the Criminal Justice System

The creation of new branches of law in general and a new branch of criminal law – the Meta-criminal law - in particular, applicable exclusively to Metaverse realities, is an idea difficult to accept and implement in practice. Still, it is not sufficient to design a new branch of law for Metaverse, we need to design a whole new system to enforce these rules and to punish the criminals who commit meta-crimes.

Will we ever have criminal meta-trials that will involve the administration of virtual evidence exclusively in virtual space, and the punishments will be executed in virtual prisons? This would probably be the natural direction of development. Until then, however, we are already facing a collision of the two worlds in terms of the criminal process, because Metaverse could be successfully used in the instrumentation of criminal cases from physical reality as it allows the virtual reconstruction of the commission of crimes and judicial bodies and jurors, in legal systems who have courts with juries, to ascertain with their own senses how things actually happened and how the crime was physically committed.

For example, in an ongoing trial in Florida, USA, in which a man was accused of trying to kill his neighbour, a motion was filed by the defence attorney asking that jurors hear expert testimony in question using virtual reality glasses. The court was demanded, without precedent, to allow the jurors to be placed „in the driver's seat by using the latest technology – virtual reality headsets that promise to give them a glimpse of the alleged crime from the defendant's perspective". Defence counsel stated that, because the expert testimony was admissible and the virtual reconstruction was merely an extension of the expert testimony, he hoped his motion would be found admissible because it would allow the jury to participate as if they were behind the wheel, and to observe that the defendant „had no intent to commit a crime" [17].

In China, the administration of evidence in the criminal trial using VR technologies was already permitted, since 2018 [18].

Moreover, there are real initiatives of the scholars of advocating for the large-scale use of virtual reality to facilitate the criminal proceedings and the discovery of the truth, as far back as 16 years ago [19].

Even if there are certain preoccupations in the use of VR technologies in the present criminal justice system, this is only the beginning. We will have criminal meta-trials that will involve the administration of virtual evidence exclusively in the virtual space, and the punishments will be executed in virtual prisons.

The benefits of the use of VR in the criminal trial and in the criminal justice system are obvious and numerous: it makes possible to virtually reconstruct of the commission of crimes allowing judicial bodies and jurors (in case of legal systems that have courts with jurors), to ascertain with their own senses how things happened and how the crimes were committed. Another benefit is that VR could be used in training people working in the judiciary or even in re-educating process of convicted criminals, with the aim of their rehabilitation and social reintegration.

Computer simulations are currently used in the criminal justice system for research purposes, but the extensive use of immersive virtual environments offers unique possibilities within the criminal justice system, as it would operate in an environment where operational workers have absolute control over the people's reactions they work with.

5 Conclusions

Trying to conclude, several ideas should be remembered. Metaverse represents a new „Wild West" [20] where, for now, intervention by means of criminal law is very limited.

The multitude, complexity, and emergence of social relations in Metaverse generate a whole new category of perils needing to be addressed by the legislators, to ensure the users of the of the virtual platforms' safety. In this regard, I propose a step-by-step approach: in a first phase a set of guiding principles should be established (initial minimum intervention); this first phase should be followed by designing sectoral norms for the regulation of social relations in Metaverse – e.g. specific rules for Meta-data protection, Meta-electronic commerce, Meta-copyright etc. - (intermediate intervention); finally, specific criminal rules frame should be established (maximum intervention).

If we do not act proactively, if we do not accept the (virtual) reality, it is very possible to allow virtual chaos to be installed and cause irremediable harms to our society.

References

1. U.W. Chohan, SSRN Papers, 1-9, DOI: 10.2139/ssrn.4038770, (2022)
2. S.W. Brenner, Vanderbilt J. of Entertainment & Tech. L., **11(1),** 1-97, (2008)
3. Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T.H. Luan, X. Shen, *A Survey on Metaverse: Fundamentals, Security, and Privacy,* IEEE Communications Surveys & Tutorials, **25,** (1), 319-352, DOI: 10.1109/COMST.2022.3202047, (2022)
4. Elliptic Metaverse Report, URL: https://www.elliptic.co/hubfs/Crime%20in%20the%20Metaverse%202022%20final.pdf, accessed: 14.02.2023, (2022)
5. M. Stephens, *Metaverse Governance*, URL: https://standards.ieee.org/wp-content/uploads/2022/06/XR_Metaverse_Governance.pdf, accessed: 14.02.2023, (Institute of Electrical and Electronics Engineers New York, USA, 2022)
6. L. Rosenberg, Metaverse 101: Defining the key components. VentureBeat, February 5th, URL: https://venturebeat.com/business/metaverse-101-defining-the-key-components/, accessed: 14.02.2023, (2023)
7. Europol, Policing in the metaverse: what law enforcement needs to know, an observatory report from the Europol Innovation Lab, Publications Office of the European Union, URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Policing%20in%20the%20metaverse%20-%20what%20law%20enforcement%20needs%20to%20know.pdf accessed: 14.02.2023, (2023)

8. URL: https://www.gartner.co.uk/en/articles/what-is-a-metaverse, accessed: 14.02.2023, (2023)
9. L. Rosenberg, Regulating the Metaverse, a Blueprint for the Future, DOI:10.1007/978-3-031-15546-8_23, (Springer, 2022)
10. S. Jathavedan, The Buzz Around the 'Metaverse', URL: https://www.khuranaandkhurana.com/2022/10/12/metaverse-blurred-lines-for-criminal-law/, accessed: 14.02.2023, (2022)
11. G. Lawton, How Seoul is creating a metaverse for a smarter city, URL: https://venturebeat.com/ai/how-seoul-is-creating-a-metaverse-for-a-smarter-city/, accessed: 14.02.2023, (2022)
12. A. Romano, These 12 Famous Museums Offer Virtual Tours You Can Take on Your Couch, URL: https://www.travelandleisure.com/attractions/museums-galleries/museums-with-virtual-tours, accessed: 14.02.2023, (2022)
13. S. Chung, The Problems with Trying to Apply Real-World Laws in the Virtual Metaverse, URL: https://abovethelaw.com/2022/02/the-problems-with-trying-to-apply-real-world-laws-in-the-virtual-metaverse/, accessed: 14.02.2023, (2022)
14. W. Soon, A researcher's avatar was sexually assaulted on a metaverse platform owned by Meta, making her the latest victim of sexual abuse on Meta's platforms, watchdog says., URL: https://www.businessinsider.com/researcher-claims-her-avatar-was-raped-on-metas-metaverse-platform-2022-5, accessed: 14.02.2023, (2022)
15. A. Diaz, Disturbing reports of sexual assaults in the metaverse: 'It's a free show', URL: https://nypost.com/2022/05/27/women-are-being-sexually-assaulted-in-the-metaverse/, accessed: 14.02.2023, (2022)
16. L. Stănilă, Dreptul penal al viitorului: spre un meta-drept penal? [Criminal Law of the Future: Towards a Meta-Criminal Law?] in L. Stănilă, (coord), Dreptul penal al Viitorului. Generații [Criminal Law of the Future. Generations], 103-117, (Universul Juridic, Bucharest, 2022)
17. R. Olmeda, Is Virtual Reality the Future of Expert Testimony in Court?, URL: https://www.govtech.com/public-safety/is-virtual-reality-the-future-of-expert-testimony-in-court, accessed: 14.02.2023, (2022)
18. J. Nafarette, Chinese Courtroom Uses VR to Revisit Crime Scene, URL: https://vrscout.com/news/chinese-courtroom-vr-crime-scene/, accessed: 14.02.2023, (2018)
19. J.N. Bailenson, J. Blascovich, A.C. Beall, B. Noveck, Law & Policy, **28(2)**, 246-270, DOI:10.1111/j.1467-9930.2006.00226.x, (2006)
20. A. Woon, The metaverse is not above real-world law. The Straits Times, URL: https://www.suss.edu.sg/docs/default-source/media-coverage/20220125-st---the-metaverse-is-not-above-real-world-law.pdf?sfvrsn=5f6655cb_0, accessed: 14.02.2023, (2022)
21. J. Brassel, Murder in the Metaverse could be a real crime, URL: https://www.beyondgames.biz/21556/murder-in-the-metaverse-could-be-a-real-crime/ accessed: 14.02.2023, (2022)