sciendo

Ius Novum

2025, vol. 19, no. 2, pp. 136–147

LEGAL FRAMEWORKS FOR THE APPLICATION AND DEVELOPMENT OF THE METAVERSE IN MEDICINE

ADAM KOZIEŃ*

DOI 10.2478/in-2025-0018

Abstract

The article analyses the gradually evolving sphere of the metaverse. This sphere is currently, in a sense, a fusion of technological development with the world of the Internet and artificial intelligence, from the perspective of legal considerations crucial to medicine. The article addresses an original issue within the realm of new challenges faced by the law in the era of advancing digitisation. Simultaneously, it has both a review and monographic character. The central thesis posited is that the use of the metaverse in medicine may pose a danger of violating human rights and freedoms, particularly in the areas of individual liberty, personal data protection, and the protection of personal rights, which is relevant from a legal standpoint. The aim of the research conducted was to analyse the application of the metaverse in medicine from a legal perspective and to identify the dangers posed by the metaverse in the context of the risk of infringing fundamental rights and individual freedoms. Additionally, the study aims to propose legislative recommendations in this regard. The subject of the research and its results are original in nature, encompassing not only Polish law but also international law. The application of the research may be significant not only for academia but also for the practice of law, especially in relation to legislative actions at the international, European Union, and national levels.

Key words: law, metaverse, medicine, personal data protection, protection of personal rights

* LLD, MBA, Department of Administrative Procedure, Faculty of Law and Administration, Jagiellonian University in Krakow (Poland), e-mail: a.kozien@uj.edu.pl, ORCID: 0000-0002-9301-9645

INTRODUCTION

The modern world is developing in a very dynamic way, especially in terms of modern technologies. Nowadays, however, these up-to-date technologies do not merely involve technological improvements in specific devices or the development of the Internet, but also include artificial intelligence, which is gradually advancing. In addition to this, there is an entirely new phenomenon that can radically change the way people function, namely the metaverse – currently being promoted especially by social media – which represents in a sense, a combination of technological development with the world of the Internet and artificial intelligence. The metaverse should be regarded as a virtually unlimited world (*metaversum*), which encompasses all people, and to some extent may even go beyond the modern understanding of the world and universe. The idea of the metaverse was, until recently, treated as hypothetical and akin to science fiction. It can be observed, however, that concepts formerly confined to science fiction are gradually shedding their fictional element and becoming part of the real world, in which the individual must properly situate themselves. One cannot respond to such a changing world solely in terms of threat or fascination but should – recognising certain dangers – attempt to adapt new technical and technological advances accordingly, so that they serve the good of the individual and the common good. In this regard, a key element is common law, which should impose certain requirements and formal frameworks on modern technological achievements, in order to prevent violations of individual rights and freedoms as defined at the level of international law, EU law, and the national legal systems of democratic states governed by the rule of law. The metaverse is also gradually appearing in medicine, where, by virtue of its specificity, it can particularly interfere with individual freedoms and rights.

RESEARCH METHODOLOGY

The purpose of the research conducted was to analyse, from a legal perspective, the metaverse as applied to medicine, to identify the dangers of the metaverse in terms of the potential violation of fundamental individual rights and freedoms, and to formulate legislative proposals in this regard.

In conducting the research, the following methods, specific to legal science, were used:

– the theoretical and legal method, to analyse the concept of the metaverse and legal institutions of relevance to the subject of the study;
– the formal-dogmatic method, to analyse legal regulations and sources of common law relevant to the research topic;
– the method of literature criticism, enabling analysis within the field of the research subject, as well as the identification of gaps in the current state of knowledge and development trends in modern science concerning the topic of the study.

METAVERSE AS A MODERN TECHNOLOGICAL CHALLENGE

The metaverse is currently one of the more widely discussed and technologically developed issues. The metaverse[1] is related to the new era of the Internet that is currently being shaped, going beyond the currently accepted technological, cultural, and social patterns. This new era of the Internet is associated, firstly, with VR (virtual reality) or AR (augmented reality) technologies, and secondly, with the creation and coexistence of multiple 3D digital virtual worlds, as well as virtual reality itself. The term 'metaverse' was coined by Neal Stephenson in his 1992 science fiction novel *Snow Crash*, where it refers to a virtual world functioning in parallel to the real world. A current proponent and promoter of the metaverse is Mark Zuckerberg, the creator of Facebook, who sees the future of the organisation in the metaverse. The metaverse is also an area of interest for companies such as Microsoft, Apple, and Epic Games. At the same time, there are already metaverse-based platforms such as *Fortnite* and *Roblox*, which are related to gaming. It is also worth noting that VR technology enables sensory experiences in addition to movement through the virtual world, while AR technology, using elements from the metaverse, maps them onto the real world.

In this regard, it is worth pointing out that, nowadays, the sphere of the Internet and social media allows for virtual functioning; however, the division between the real world and the virtual world is still maintained, even though the virtual world is becoming increasingly similar to the real one. The idea of the metaverse is to create a digital world that would become the real world. Moreover, from a technological perspective, it is possible to create several virtual worlds, whether independent or overlapping. With the help of the metaverse, it will be possible to function in the virtual world as in the real world – thus to make contacts with others, run errands, shop, play games, and visit various places without leaving home. What is more, it will also be possible to connect different virtual worlds, between which one can move freely with appropriate technical equipment. An important aspect of the metaverse is also the fact that the person entering the virtual world feels as if they are actually moving and functioning within it. This raises the danger of the virtual world becoming blurred with the real world.

In order to function in the world of the metaverse, it becomes necessary to create avatars[2] of specific individuals, through which one can move around the metaverse as in the real world and also be recognised by other users. In the metaverse, where by definition one can function as in the real world, it is also necessary to introduce

---

1 See M. Sparkes, 'What is a metaverse', *New Scientist*, 2021, Vol. 251, Issue 3348; S. Mystakidis, 'Metaverse', *Encyclopedia*, 2022, Vol. 2, Issue 1; I.A. Filipova, 'Creating the Metaverse: Consequences for Economy, Society, and Law', *Journal of Digital Technologies and Law*, 2023, Vol. 1, No. 1; M. Kalyvaki, 'Navigating the Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction', *Journal of Metaverse*, 2023, Vol. 3, Issue 1; S. Kasiyanto, M.R. Kilinc, 'The Legal Conundrums of the Metaverse', *Journal of Central Banking Law and Institutions*, 2022, Vol. 1, No. 2.

2 B.C. Cheong, 'Avatars in the metaverse: potential legal issues and remedies', *International Cybersecurity Law Review*, 2022, Vol. 3.

virtual ownership of property, goods, and identities. It is therefore necessary to implement an appropriate structure not only technologically, but also economically. To this end, cryptocurrencies and non-fungible tokens (NFTs) are being introduced.

The existence of metaverse virtual worlds is also strongly linked to the functioning of artificial intelligence. The metaverse has the character of a virtual, digital world, which is based on information and communication systems, within which artificial intelligence is playing an increasingly important role. At present, artificial intelligence operates on software developed and controlled by humans. However, consideration must be given to the potential existence in the near future of neural networks, capable of learning, developing and thinking on their own, and therefore independently of human programming. This raises the futurological question of whether, at some point, a self-learning and self-thinking artificial intelligence could begin to govern the virtual world of the metaverse independently of humans. This is currently a wholly speculative question; but at the same time, if the question of creating metaverse virtual worlds had been raised ten years ago, the public reception would likewise have been that such an idea was entirely speculative and unrealistic.

METAVERSE IN MEDICINE

The metaverse can also be applied to life sciences,[3] including medicine. World 3.0 opens up new opportunities for life sciences and medicine.[4] As the metaverse becomes increasingly close to the real world, it can prove very helpful in medical contexts. An example of the application of the metaverse in medicine could be consultations or even treatment within the metaverse via avatars. In such a case, the patient's avatar would have access to the full medical records of the real patient, and the doctor could conduct a consultation on this basis. Of course, not all examinations would be possible in the metaverse, but consultations such as nutritional advice or telemedicine in general are feasible within the virtual environment. Such consultations would also eliminate geographical and social barriers.

It is also worth noting that the medical world of the metaverse could significantly assist in the training of future doctors, as it would allow for non-invasive examinations and consultations to be conducted in the virtual world. It could also prove useful for simulating, for example, a real surgical operation. It should be emphasised that there are currently projects aimed at establishing a medical facility in the metaverse, as well as the creation of a metaverse hospital in the United Arab

[3] See S. Surveswaran, L. Deshpande, 'A Glimpse into the Future: AI, Digital Humans, and the Metaverse–Opportunities and Challenges for Life Sciences in Immersive Ecologies', in: Byrne M. (ed.), *AI in Clinical Medicine: A Practical Guide for Healthcare Professionals*, Wiley-Blackwell, 2023.

[4] See also: https://www.cognizant.com/us/en/insights/perspectives/in-life-sciences-the-metaverse-opportunity-knocks-wf1135812 [accessed on 20 May 2023]; https://www.ey.com/en_ch/technology/how-can-life-sciences-and-healthcare-thrive-in-the-metaverse [accessed on 20 May 2023]; https://www.tcs.com/what-we-do/industries/life-sciences/white-paper/metaverse-healthcare-life-sciences-realize-business-value [accessed on 20 May 2023].

Emirates. The potential of so-called digital twins, or virtual models of real beings or objects, is also being recognised.

The benefits of the metaverse are also acknowledged by pharmaceutical companies that invest in clinical trials. Patient data, which is valuable from the perspective of research in life sciences and healthcare, is another issue of significance. At present, patients are usually not remunerated for providing their data. In the metaverse, NFT tokens could enable the encryption and subsequent transfer of ownership and value of data. Consequently, patients would be able to monetise their data and decide to whom it is shared as NFTs.

The development of the metaverse in medicine is being driven by regulatory pressures, significant shortages in the medical workforce, and a shift towards increasing trust with the patient, who is making numerous decisions. Education and training can be identified as the primary area of metaverse application in medical science. It is worth noting that 3D visualisations allow for the real development and upskilling of medical personnel without causing harm to patients. Training is also possible regardless of geographical, environmental, or cultural barriers. Simulations are often linked to gamification, which in this case takes place without risk. Technological advancements in simulations now allow for the engagement of all the trainee's senses, generating real feelings and experiences. Medical training can be provided not only for healthcare professionals, but also for pharmacists, in the form of visualising drug action and simulating experiences resulting from varied patient conditions. Nowadays, medical universities are training students using the metaverse, for example, in a virtual operating room with a virtual patient.

Another example of the introduction of the metaverse in medicine is the transformation of clinical trials. The metaverse, through the absence of geographical and physical limitations, can render these trials more decentralised and possible within patients' homes. In order to ensure the security and protection of patient data in this regard, NFTs should remain an important element, for instance, in the context of medical records. The metaverse can also facilitate so-called immersive therapies, that is, medical interventions using AR, VR, and MR. These can be applied specifically to cognitive therapies, rehabilitation, as well as psychiatric and psychological treatment. The metaverse may also be used in radiological diagnostics, since medical images are currently visualised on 2D screens. Enhancing diagnostics through 3D will enable better analysis of medical images and allow for the use of interactive and realistic medical experiences. In this context, medical devices are now emerging that use VR to train medical robots through machine learning algorithms.

The metaverse may also contribute to the development of telemedicine, which could be particularly significant given the shortage of personnel and technology in the healthcare industry. In this respect, augmented reality and the provision of medical services, such as diagnosis, consultation, treatment, care, and monitoring, in remote form are becoming increasingly crucial. Consequently, so-called digital twins, which enable simulations in three-dimensional form, may also prove important.

LEGAL ISSUES AND CHALLENGES IN APPLYING METAVERSE TO MEDICINE

INDIVIDUAL FREEDOM IN THE PERSPECTIVE OF THE APPLICATION OF THE METAVERSE IN MEDICINE

The danger of violating freedom and human rights can be identified as the first issue. It should be noted that freedom is linked to the very nature of man, so that it is not determined by the state but is primary in nature.[5] The freedom of the individual lies in the right, in a particular situation, to make choices or act according to their own will, provided that these actions are not prohibited by law.[6] Human freedom does not derive from 'law in the sense of the subject matter, and the law only establishes its limits'.[7] It should also be noted, following L. Garlicki, that the principle of freedom 'is one of the typical metanorms (general clauses) that determine the manner and direction of the interpretation of the entire system of constitutional norms and determine the system of values that the system is intended to serve'.[8]

It is therefore important to consider who in the metaverse will oversee the observance of freedoms and human rights, especially since the metaverse is, by design, global, transnational and supranational, and therefore, what legal order will be in force.[9]

A major threat to individual freedom in the metaverse can be the inequality that exists between metaverse administrators and individuals wishing to use and benefit from metaverse services. This inequality arises specifically from the position and power of the entities administering the metaverse. In order to use the metaverse, it is necessary to conclude an appropriate contract, which is essentially adhesive in nature. This may lead to violations of the autonomy of will and individual freedom.

Dangers may be identified not only in the private-law vertical relationship between the metaverse administrator and the user, but also in the private-law horizontal relationship between individuals using the metaverse, particularly with regard to personal property. A key element may also be the relationship between the state and the metaverse, as well as the question of whether states will exist in the metaverse world.

Threats to individual freedoms in the metaverse may also involve data protection, contractual relations between metaverse administrators and their users, copyright law, criminal law, and international law.

In addition, threats to individual freedom in the metaverse may also arise from new technologies, especially so-called 'artificial intelligence' and information systems. Mention should also be made of the danger of violating the principle of equality and non-discrimination, particularly in the context of so-called 'digital

---

5 B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej*, Warszawa, 2012, p. 201.

6 W. Skrzydło, S. Grabowska, R. Grabowski, *Konstytucja Rzeczypospolitej Polskiej. Komentarz encyklopedyczny*, Warszawa, 2009, p. 643.

7 B. Banaszak, *Konstytucja*…, op. cit., p. 202 [own translation].

8 L. Garlicki, *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa, 2012, p. 94 [own translation].

9 See also: M. Turdialiev, 'Legal Discussion of Metaverse Law', *International Journal of Cyber Law*, 2023, Vol. 1, Issue 3.

exclusion', especially affecting the elderly, the poor, and those living in sparsely urbanised areas, where access to the Internet is sometimes significantly hampered or not possible at all. There is also the key question of who can be a user of the metaverse, especially from the perspective of people with limited or no legal capacity. In this regard, it should be pointed out that when evaluating the implementation of the principle of equality, it is necessary to refer to it in the substantive sense. In this context, the Polish Constitutional Court noted that:

> 'A matter fundamental to the assessment of compliance with the principle of equality is thus the determination of the essential feature on account of which the laws have made a differentiation of the legal situation of their addressees. (…). Thus, it has been repeatedly pointed out that the differentiation of the legal situation of citizens is then unconstitutional if differential treatment is given to similar subjects or situations, and such differences in treatment do not find due constitutional justification. The Constitutional Court has also repeatedly emphasised the relationship between the principle of equality and the principle of justice (…).'[10]

In the search for such justification, the criteria of rationality, proportionality and fairness of the differentiations made were pointed out (…).[11] In other words, any deviation from the injunction to treat similar entities equally must always be based on sufficiently compelling criteria. These criteria must be:

– first, of a relevant nature, i.e. they must be directly related to the purpose and essential content of the provisions in which the controlled norm is contained, and serve to realise this purpose and content, i.e. the differentiations introduced must be rationally justified. They must not be made according to an arbitrary criterion (…);[12]
– secondly, proportional in nature, that is, the importance of the interest to be served by differentiating the situation of the addressees of the norm must be in appropriate proportion to the importance of the interests that will be violated as a result of unequal treatment of similar entities;
– third, must be in some connection with other values, principles or constitutional norms that justify different treatment of similar entities (…).[13]

As a result, therefore, a certain amount of differentiation may exist, but it must depend on objectified criteria and must not lead to 'digital exclusion', for example.

DATA PROTECTION IN THE PERSPECTIVE OF THE APPLICATION OF THE METAVERSE IN MEDICINE

One of the most important legal challenge is the issue of protecting personal data in the metaverse. In this regard, a problematic issue is the number and scope of personal data that will be placed in the metaverse space. The origins of legal regulations related

---

[10] Constitutional Tribunal ruling of 28 November 1995, K 1/95, *OTK ZU*, No. 3/1995, p. 183.
[11] Constitutional Tribunal ruling of 3 September 1996, K 10/96, *OTK ZU*, No. 5/1996, p. 281.
[12] Constitutional Tribunal ruling of 12 December 1994, K 3/94, *OTK*, 1994, part II, p. 141.
[13] For example, Constitutional Tribunal ruling of 23 October 1995, K 4/95, *OTK*, 1995, part II, p. 93; Constitutional Tribunal judgment of 16 December 1997, K 8/97, *OTK*, 1997, No. 5–6, item 70. See also judgment of the Supreme Court of 5 May 2010, I PK 201/09.

to the issue of personal data can be tracked back to the 1970s;[14] however, at the time, the issue was addressed in two ways – by creating piecemeal regulations as well as comprehensive ones (as an example, one can point to the Data Protection Act of 1970 of the German state of Hesse).[15] The need to develop and expand the protection of personal data was related to the ongoing computerisation of various areas of life and the creation of computerised systems,[16] capable of recording as well as processing numerous data, and consequently the emergence of *de facto* databases.[17] The lack of an adequate legal response would lead to the unlimited collection and processing of personal data. Consequently, this would create the danger of violating not only the right to privacy but also the very essence of human freedoms and rights.[18]

Legal protection of personal data occurs under international, EU, and individual country laws, but among these regulations, it is worth mentioning Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),[19] which holistically protects personal data within the European Union Member States. The introduction of the Regulation has allowed for full harmonisation within the European Union of the protection of personal data. It is worth noting that the Regulation does not apply only to European Union Member States but, in its scope, also applies to entities that provide services within the European Union.[20] Based on Article 3(1) of the Regulation, it 'applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not', and Article 3(2) states that the Regulation 'applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.'

Treating the metaverse as a real world in a virtual space can lead to a situation in which essentially all data about an individual will be stored and processed in the metaverse world. Some of this data will probably be provided on a mandatory basis

---

[14] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, 5th edn, Warszawa, 2011, p. 25.

[15] Ibidem, p. 25; W. Kilian, 'Ochrona danych w przedsiębiorstwach', in: Wyrzykowski M. (ed.), *Ochrona danych osobowych (zbiór referatów wygłoszonych na poświęconej problematyce ochrony danych osobowych konferencji naukowej w dniach 27–28 II 1998 r.)*, Warszawa, 1999, pp. 99 et seq.

[16] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…*, op. cit., p. 26.

[17] See also U. Seidel, *Datenbanken und Persönlichkeitsrecht*, Köln, 1972.

[18] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…*, op. cit., p. 27.

[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1.

[20] M. Krawczyk, 'Ochrona danych osobowych w Internecie', in: Surma A., Chodźko E. (eds), *Współczesne wyzwania cyfryzacji – przegląd i badania*, Lublin, 2019, p. 190.

and some on an optional basis. It is therefore necessary to minimise the amount of data provided obligatorily as much as possible, because, as for the data provided optionally, the principle of *volenti non fit iniuria* can be applied.

The problem, moreover, will be data that is not posted knowingly and directly, but rather data that is transferred unknowingly and indirectly, usually as a result of posting data knowingly and directly. In terms of data protection, applicable law will again be an important element, especially since, for example, EU regulations are very restrictive in this regard, in contrast to other legal orders. It should also be noted that nowadays personal data is a modern commodity, and from the perspective of metaverse administrators, as well as entities doing business there, it is relevant and valuable (it also has a quantifiable value). Another problem is also the so-called metadata, which is created as a result of the activities of a particular user. Metaverse administrators can also extract data from a user's software.

The danger of a breach of personal data protection comes not only from metaverse administrators collecting and processing data, but also from other social network users and even cybercriminals. It should also be pointed out that in the medical field we are dealing with personal data that is particularly sensitive, as it relates to health, for example, which makes the case for ensuring the highest possible level of protection even stronger. It should further be noted that the metaverse world will be processing and collecting vast amounts of data, on a scale that may even exceed the scope of so-called Big Data,[21] which currently dominates the sphere of the Internet and social media.

PROTECTION OF PERSONAL RIGHTS IN THE CONTEXT OF METAVERSE APPLICATIONS IN MEDICINE

The protection of personal property poses another challenge. More broadly, not directly in relation to the metaverse, but with regard to the issue of violation of personal property on the Internet, the following views in legal doctrine can be identified:

– a distinction can be made between personal property that can be violated or threatened on the Internet;[22]

---

[21] See D. Boyd, K. Crawford, 'Critical questions for big data in Information', *Communication & Society*, 2012, Vol. 15, Issue 5, pp. 662–679; H.U. Buhl, M. Röglinger, F. Moser, J. Heidemann, 'Big Data. Ein (ir-)relevanter Modebegriff für Wissenschaft und Praxis?', *Wirtschaftsinformatik*, 2013, Vol. 55, Issue 2, pp. 63–68; R. Reichert, 'Big Data', in: Beyes T., Metelmann J., Pias C. (eds), *Nach der Revolution. Ein Brevier digitaler Kulturen*, Berlin, 2017, pp. 177–185; M. Schermann, H. Krcmar, H. Hemsen, V. Markl, Ch. Buchmüller, T. Bitter, T. Hoeren, 'Big Data – An Interdisciplinary Opportunity for Information Systems Research', *Business & Information Systems Engineering*, 2014, Vol. 6, Issue 5, pp. 261–266; D. Klein, P. Tran-Gia, M. Hartmann, 'Big Data', *Informatik Spektrum*, 2013, Vol. 36, pp. 319–323; V. Marx, 'The big challenges of big data', *Nature*, 2013, Vol. 498, pp. 255–260.

[22] P. Modrzejewski, 'Sposoby naruszania dóbr osobistych w Internecie – zagadnienia wybrane', *Studia Prawnoustrojowe*, 2019, No. 44, p. 295; J. Sadomski, *Naruszenie dóbr osobistych przez media*, Warszawa, 2003, p. 26.

– there are personal goods that can only be violated or threatened in the real world – such as the integrity of the home;[23]
– in principle, all personal property can be violated or threatened on the Internet.[24]

As regards the metaverse, it should be pointed out that any personal good can, in principle, be violated or threatened there. The issue of protection of personal rights in common law has the character of general norms, an open catalogue of legally protected goods, and is susceptible to dynamically changing circumstances in political, legal, social, economic, and cultural life.

A significant challenge to personal property in the metaverse is its global nature, which can significantly undermine the effectiveness of asserting one's rights and claims, and makes it necessary to develop effective redress mechanisms at the international level. In this regard, the Internet judiciary, which is already well known in China, for example, may also come to the fore.

The peculiarities of the metaverse mean that, in addition to the traditional forms of violating personal rights through, for example, insulting, posting compromising photos of others, writing untruths about others, or unlawfully using someone's name or creativity, other forms of violating personal rights can be identified. These may include: spamming, cookies,[25] data retention, personality profiling, phishing,[26] hacker attacks,[27] impersonation of a particular entity, sniffing, the Heartbleed bug, deep links, and cloud computing. The peculiarities of the metaverse can lead to violations of the same personal rights but in other forms (specific to the virtual space), as well as to the emergence of new forms of violations of personal rights. In principle, any personal good can be violated in the metaverse. These violations can be committed by both public and private law entities, especially administrators and users of the metaverse. Violations can occur in situations of hacking attacks or unauthorised access to a social network user's account. Nowadays, violations of personal rights can also result not only from the activities of IT systems controlled by individuals but also through the operations of so-called 'artificial intelligence'.

One of the most important challenges is to ensure security in the metaverse world, especially data security, as it will be of particular importance in the virtual world. Technical security should protect against hacking attacks and cybercrime in the broadest sense. Particular attention should be paid to the security of both sensitive and health data.

---

[23] P. Modrzejewski, 'Sposoby…', op. cit., pp. 295–296. See P. Waglowski, *Ochrona dóbr osobistych i danych osobowych*, Warszawa, 2009, p. 4.

[24] P. Waglowski, *Ochrona…*, op. cit., pp. 4–5; P. Modrzejewski, 'Sposoby…', op. cit., p. 296.

[25] M.R. Siebecker, 'Cookies and the Common Law: Are Internet Advertisers Trespassing on Our Computers?', *Southern California Law Review*, 2003, Vol. 76, No. 4.

[26] J.A. Chaudhry, S.A. Chaudhry, R.G. Rittenhouse, 'Phishing Attacks and Defenses', *International Journal of Security and Its Applications*, 2016, Vol. 10, No. 1

[27] K. Anderson, *Hacktivism and politically motivated computer crime*, Portland, 2008; M.T. Simpson, *Hands-on ethical hacking and network defense*, Boston, 2013.

CONCLUSION

The idea of the metaverse fundamentally changes the approach to functioning in virtual space. The very idea of the existence of parallel virtual worlds, which are essentially duplicates of the real world, still seems abstract; however, it is in fact partially accessible. The existence of the metaverse world can be observed in various areas of life. It is also perceptible in the life sciences, and in this area particularly in medicine and health sciences. This raises major challenges in the legal field, since the metaverse world operates parallel to the real world, so the primary problem is determining the applicable law. Another issue is the danger of infringement of individual rights and freedoms, which may result from the dominant position of metaverse administrators, as well as the danger of so-called 'digital exclusion'. An important element is the digital security in the age of cybercrime, as well as the protection of personal data and personal property, and the role of artificial intelligence. Adaptation of the law in this regard concerns not only international law or civil law, but also administrative, criminal, economic, and EU law.

The dangers indicated above are only the most glaring, particularly from the perspective of medicine. Irrespective of the fact that these issues are international in nature, they will ultimately have to be addressed by the national legislature. The state, as an administrative apparatus, has relatively broad powers to interfere with this activity, but at the same time must bear in mind the need to be proportionate when doing so, as well as to uphold individual freedoms and rights. Regardless of the public law perspective, and therefore administrative and criminal law, a key element should also be interference at the civil law level, through, for example, the introduction of a specific contract for the use of services in the metaverse world, which would protect users of this form of activity in the sphere of the broader Internet.

Notwithstanding the above considerations, it should also be pointed out that a change in culture, customs, and society's attitudes towards the virtual world is necessary in this respect. This is an element that will evolve over time. In addition, a person using the metaverse world must not become dependant on the virtual world, which should serve only to assist in normal functioning. The virtual world will never replace the real world, because at best it will only faithfully imitate it. Contrary to appearances, the example of medicine demonstrates this very well, as a surgeon will not perform an operation in the virtual world. Moreover, one may ask whether the virtual world of the metaverse will ever match the beauty of the real world?

BIBLIOGRAPHY

Anderson K., *Hacktivism and politically motivated computer crime*, Portland, 2008.

Banaszak B., *Konstytucja Rzeczypospolitej Polskiej*, Warszawa, 2012.

Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, 5th edn, Warszawa, 2011.

Boyd D., Crawford K., 'Critical questions for big data in Information', *Communication & Society*, 2012, Vol. 15, Issue 5.

Buhl H.U., Röglinger M., Moser F., Heidemann J., 'Big Data. Ein (ir-)relevanter Modebegriff für Wissenschaft und Praxis?', *Wirtschaftsinformatik*, 2013, Vol. 55, Issue 2.

Chaudhry J.A., Chaudhry S.A., Rittenhouse R.G., 'Phishing Attacks and Defenses', *International Journal of Security and Its Applications*, 2016, Vol. 10, No. 1.

Cheong B.C., 'Avatars in the metaverse: potential legal issues and remedies', *International Cybersecurity Law Review*, 2022, Vol. 3.

Filipova I.A., 'Creating the Metaverse: Consequences for Economy, Society, and Law', *Journal of Digital Technologies and Law*, 2023, Vol. 1, No. 1.

Garlicki L., *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa, 2012.

Kalyvaki M., 'Navigating the Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction', *Journal of Metaverse*, 2023, Vol. 3, Issue 1.

Kasiyanto S., Kilinc M.R., 'The Legal Conundrums of the Metaverse', *Journal of Central Banking Law and Institutions*, 2022, Vol. 1, No. 2.

Kilian W., 'Ochrona danych w przedsiębiorstwach', in: Wyrzykowski M. (ed.), *Ochrona danych osobowych (zbiór referatów wygłoszonych na poświęconej problematyce ochrony danych osobowych konferencji naukowej w dniach 27–28 II 1998 r.)*, Warszawa, 1999.

Klein D., Tran-Gia P., Hartmann M., 'Big Data', *Informatik Spektrum*, 2013, Vol. 36.

Krawczyk M., 'Ochrona danych osobowych w Internecie', in: Surma A., Chodźko E. (eds), *Współczesne wyzwania cyfryzacji – przegląd i badania*, Lublin, 2019.

Marx V., 'The big challenges of big data', *Nature*, 2013, Vol. 498.

Modrzejewski P., 'Sposoby naruszania dóbr osobistych w Internecie – zagadnienia wybrane', *Studia Prawnoustrojowe*, 2019, No. 44.

Mystakidis S., 'Metaverse', *Encyclopedia*, 2022, Vol. 2, Issue 1.

Reichert R., 'Big Data', in: Beyes T., Metelmann J., Pias C. (eds), *Nach der Revolution. Ein Brevier digitaler Kulturen*, Berlin, 2017.

Sadomski J., *Naruszenie dóbr osobistych przez media*, Warszawa, 2003.

Schermann M., Krcmar H., Hemsen H., Markl V., Buchmüller Ch., Bitter T., Hoeren T., 'Big Data – An Interdisciplinary Opportunity for Information Systems Research', *Business & Information Systems Engineering*, 2014, Vol. 6, Issue 5.

Seidel U., *Datenbanken und Persönlichkeitsrecht*, Köln, 1972.

Siebecker M.R., 'Cookies and the Common Law: Are Internet Advertisers Trespassing on Our Computers?', *Southern California Law Review*, 2003, Vol. 76, No. 4.

Simpson M.T., *Hands-on ethical hacking and network defense*, Boston, 2013.

Skrzydło W., Grabowska S., Grabowski R., *Konstytucja Rzeczypospolitej Polskiej. Komentarz encyklopedyczny*, Warszawa, 2009.

Sparkes M., 'What is a metaverse', *New Scientist*, 2021, Vol. 251, Issue 3348.

Surveswaran S., Deshpande L., 'A Glimpse into the Future: AI, Digital Humans, and the Metaverse – Opportunities and Challenges for Life Sciences in Immersive Ecologies', in: Byrne M.F. (ed.), *AI in Clinical Medicine: A Practical Guide for Healthcare Professionals*, Wiley-Blackwell, 2023.

Turdialiev M., 'Legal Discussion of Metaverse Law', *International Journal of Cyber Law*, 2023, Vol. 1, Issue 3.

Waglowski P., *Ochrona dóbr osobistych i danych osobowych*, Warszawa, 2009.

Cite as:

Kozień A. (2025), *Legal frameworks for the application and development of the metaverse in medicine*, Ius Novum (Vol. 19) 2, 136–147. DOI 10.2478/in-2025-0018