Journal of Medical Extended Reality
Volume 2.1, 2025
DOI: 10.1089/jmedxr.2024.0028
Accepted October 8, 2024

Mary Ann Liebert, Inc. publishers

Open camera or QR reader and scan code to access this article and other resources online.

COMMENTARY Open Access

LawVerse: The Legal Framework for Clinical Metaverse Content

Barbara Pasa,[1] Alessandro Bernes,[2] Andrea Gaggioli,[3,4] Emanuele Tuccari,[5] Fabiana Zollo,[2] Giorgia Vulpiani,[6] Loris Pignolo,[7] Antonio Scala,[8,9] and Antonio Cerasa[10,*]

Abstract

The term *MedVerse* has been coined to describe how the infrastructure layers of the metaverse can be adopted in the health care sector, to enable the distribution of contents and interact with patients. In the last 2 years, a large amount of proof-of-concept metaverse-based technologies and applications have been proposed in several medical realms. However, the advent of such an expensive, hypercomplex technology promoted as a new instrument with a strong incentive to invest time and money in digital items (driving revenue for some categories) poses several legal challenges. Here, we discuss the main legal issues (the so-called *LawVerse*) related to their application to the clinical metaverses realms.

Keywords: metaverse; legal issues; data protection; intellectual property rights; non-fungible tokens; medical device

From Metaverses to the *MedVerse*

The European Union (EU) Parliament[1] defines metaverses as "*digital simulations of multidimensional spaces that can be based on visual, auditory, and tactile perception. They can simulate digitised reality, mirror worlds, digital twins, or be entirely decoupled from the physical layer and populated with AI algorithms.*" The metaverse has garnered significant attention from the research community lately, and a substantial amount of work has already been done on its ideas, design, and applications in several domains. In the last 2 years, there have been numerous attempts to develop new syllogisms with the goal of more clearly illustrating how this communication technology might be used. What emerged from this preliminary evidence was that moving from a *Psycho-Verse*[2] to a *Meta-Health*[3] or *Med-Verse*[4]

[1]Università IUAV di Venezia, Venice, Italy.
[2]Ca' Foscari University of Venice, Venice, Italy.
[3]Research Center in Communication Psychology, Catholic University of Milan, Milan, Italy.
[4]Applied Technology for Neuro-Psychology Lab, IRCCS Istituto Auxologico Italiano, Milan, Italy.
[5]University of Pavia, Pavia, Italy.
[6]University of Macerata, Macerata, Italy.
[7]S. Anna Institute, Crotone, Italy.
[8]CNR-ISC, Applico Lab, Rome, Italy.
[9]Big Data in Health Society, Rome, Italy.
[10]Institute of BioImaging and Complex Biological Systems (IBSBC-CNR), Catanzaro, Italy.

*Address correspondence to: Antonio Cerasa, PhD, Institute of BioImaging and Complex Biological Systems (IBSBC-CNR), via T. Campanella, 88100 Catanzaro, Italy, Email: antonio.cerasa76@gmail.com

© The Author(s) 2025. Published by Mary Ann Liebert, Inc. This Open Access article is distributed under the terms of the Creative Commons License [CC-BY] (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

perspective, the health care sector will be one of the main domains exploiting this kind of technology.[5]

The metaverse is a "federation" of multiple technologies (artificial intelligence [AI], tangible and multimodal interfaces, blockchain, and Internet of Things) shared by multiusers simultaneously to connect the 3D environments to cyber-physical devices and their data, thus enabling seamless interaction between the "virtual" and "real" world (also called, *phygital space*[6]) managed by AI algorithms. The two-way connection between the virtual and real worlds is provided by the digital twins: digital copies of real-world objects, systems, or processes that are in sync with the physical world. This implies that experiences in the virtual world might influence physical actions and vice versa. Furthermore, any changes made to the real world are mirrored in their virtual counterparts, enabling reciprocal feedback. For example, engaging with an avatar in the virtual world can cause haptic feedback to occur in the real world.[4]

The utilization of the metaverse in clinical medicine will be a novel approach to methods of treatment, providing some benefits concerning previous approaches (such as telemedicine or traditional individual virtual reality (VR) sessions).[7] For instance, while telemedicine provides routine treatment with convenience and accessibility, the metaverse transforms how patients and doctors engage with medical information. Depending on the clinical setting, telemedicine is a good option for routine care, while metaverse tools are best suited for complex simulations and immersive social training.[8] Another advantage is the ability to construct controlled, multiuser, and customized therapeutic environments that can be adapted to the unique requirements and conditions of each patient. Using AI tools, the metaverse also could enable the tailoring of therapeutic situations and surroundings to each patient's unique requirements, preferences, and treatment objectives. In mental health care, for instance, where the subjective nature of diseases requires individualized approaches for best results, this customization is essential. For instance, in the neurorehabilitation domain, the advent of the metaverse will allow to start a new era of treatments moving from standard individual therapy to multiusers therapeutic sessions controlled in a shared virtual world.[9] In the psychiatric domain, the employment of this "*service-oriented architecture that emphasizes social and content aspects will be used to exploit the 'synchronized brains' potential exacerbated by social interactions*."[10] However, before translating this "federation" of multiple technologies into the medical realm, we need to handle legal matters using a risk-adjusted strategy, keeping in mind that there can be exceptions to accommodate medical concerns (such as privacy, data protection, financial flexibility, decentralization, security, and intellectual property rights) as this technology is still in its infancy.

From the *MedVerse* to the *LawVerse* Framework

Metaverses will involve an extension of the legal and ethical issues that have arisen in research on virtual health communities, telehealth, and AI in health care.[11,12] Issues are not only connected to privacy and data protection but also to safe technological development and production, as well as a correct medical diagnosis and liabilities in contract and tort, due to the instrumental and supporting role played by new digital tools in the doctor–patient relationship, by considering the higher risks to which individuals might be exposed.

Furthermore, metaverses—as immersive and constant virtual 3D worlds, where people are actively involved in the creation of virtual worlds and interact by means of digital humans or digital twins of persons to carry out a wide range of activities—open many opportunities as well as challenges in other legal areas, such as intellectual property laws. The US Congress[13] and the European Parliament[1] both showed interest in legal matters brought up in the setting of metaverses. They raised apprehensions about the potential of metaverses to replicate and exacerbate existing challenges associated with contemporary online service platforms and applications. These concerns encompass issues such as the presence and moderation of illicit and harmful content online, the responsibility for consumer manipulation through advertising practices, data protection and privacy concerns, competition, and the protection of intellectual property rights. Additionally, there are concerns related to the ownership or contractually granted control of digital assets within the metaverses, legal complexities surrounding smart contracts, non-fungible tokens (NFTs), and the use of digital currencies involving virtual money transfers between avatars. Further worries extend to areas such as money laundering and gambling, as well as security issues arising from potential connections between the dark web and the metaverses.

For all these reasons, in this commentary, we described some legal concerns that underpin the use of the so-called *LawVerse* in public services, especially in the health care sector and medical setting (Fig. 1).

Data protection

Addressing the storage, handling, and protection of data in the metaverse is crucial, accompanied by accountability for potential data theft or misuse. In this regard, regulations and proposals are flourishing not only at supranational level—such as the General Data Protection Regulation ("GDPR"),[14] the "Artificial Intelligence Act" ("AI Act"),[15] and a Regulation on the "European Health Data Space"[16]—but also at national level, with the presentation of a series of interesting legislative proposals in the different EU Members States. Compliance with the "GDPR"—in case of special categories of personal data—necessitates "*explicit user consent for each specific purpose*," varying based on activities within the metaverse (Art. 9). Concerns arise as users' data are expected to be collected more extensively and continuously during their metaverse experiences, potentially making involuntary and ongoing consent challenging.

Furthermore, according to Art. 9, par. 4, "GDPR,"[14] "*Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.*" Therefore, data security measures—to protect information security and individual rights in the new environments—must also play a central role (at national and supranational levels).[17]

Additionally, defining the roles of data controllers and processors in the metaverse poses a significant challenge due to the intricate interconnections among entities in each virtual universe. Establishing clear distinctions regarding responsibilities and actions on behalf of users becomes a complex task in this interconnected environment. The decentralized approach, where users have control over their data and its sharing, may offer potential solutions to data protection issues that are intricate in more centralized business models.[18]

The European "AI Act"[15] appears to be focused on a "risk-based approach": there is an absolute ban on placing certain AI systems on the market or putting them into service or use (see Art. 5, "Prohibited AI practices"), but there are also specific obligations provided for AI systems "admitted," but classifiable as "high risk." According to Art. 6 para 1, an AI system

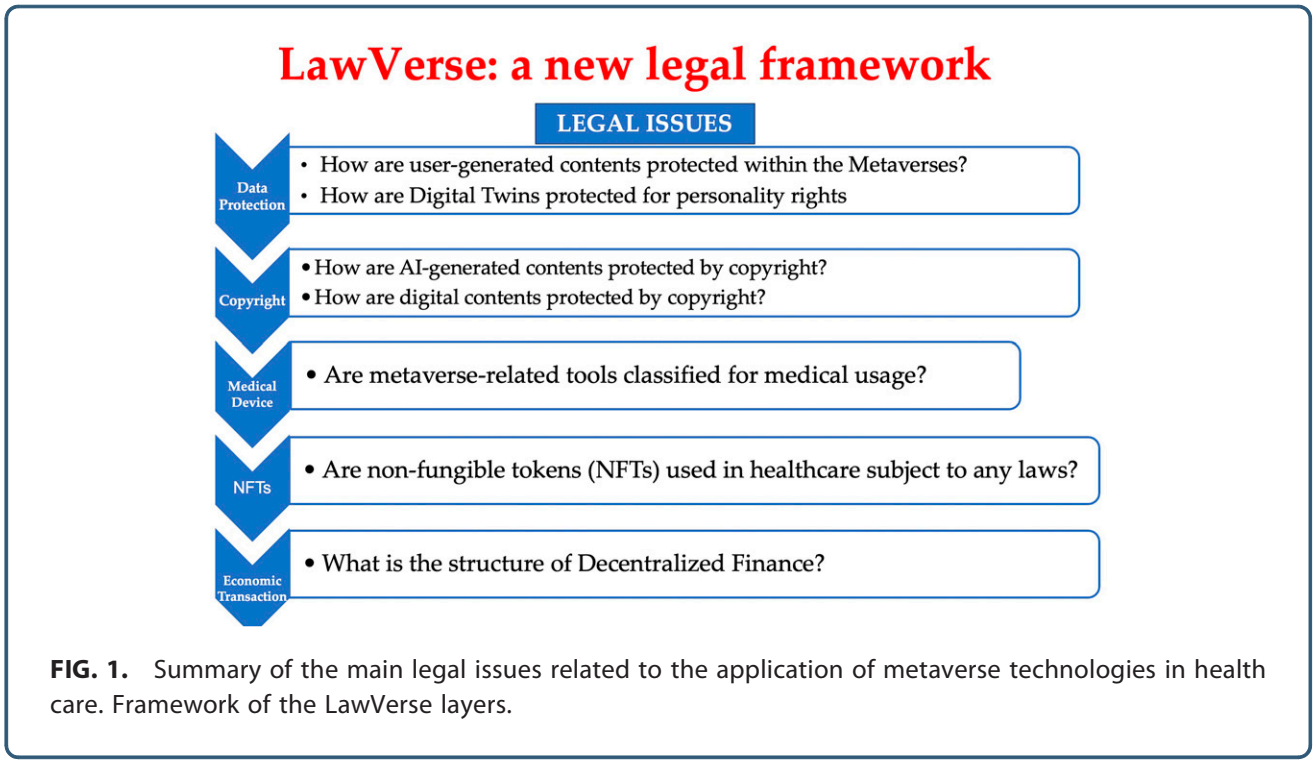


FIG. 1. Summary of the main legal issues related to the application of metaverse technologies in health care. Framework of the LawVerse layers.

that meets both of the following conditions is classified as high risk: *"a) the AI system is intended to be used as a safety component of a product, or the AI system is itself a product, covered by the Union harmonization legislation listed in Annex I; b) the product whose safety component pursuant to point (a) is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment, with a view to the placing on the market or the putting into service of that product pursuant to the Union harmonization legislation listed in Annex I*." With regard to the first condition, Annex I explicitly includes the EU Medical Device Regulation 2017/745 ("MDR")[19] among the harmonizing regulations. Regarding the second condition, under the "MDR" all "high-risk" devices must undergo conformity assessment by a third party (Notified Body) in order to be placed on the market.

Therefore, a medical device that incorporates or is itself an AI system will be considered a "high-risk" AI system. In addition to the high-risk AI systems referred to in Art. 6, para 1, the AI systems listed in Annex III (*inter alia*, in the "biometrics" area) are "high risk" (Art. 6, para 2). However, according to Art. 6, para 3, "*an AI system referred to in Annex III shall not be considered to be high-risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making*."[19] Thus, in line with the "risk-based approach" mentioned above, high-risk AI systems will be allowed on the European market subject to compliance with certain mandatory requirements (such as management system and transparency obligations toward users) and a preliminary conformity assessment. This assessment of software compliance may raise many other data protection issues (e.g., in relation to deidentification techniques used, security measures taken; see Article 10, para 5, EU AI Act).[15] Metaverses (and in particular "MedVerse")—as a "federation" of multiple technologies (AI, tangible and multimodal interfaces, blockchain, and Internet of Things)—could be considered a "high-risk" environment.[20]

Personality rights and Intellectual Property rights

The digital twin of a person (DToP) not only replicates a distinctive person but also constitutes a nearly instantaneous synchronized multipresence.[21] This entails the capability to exist simultaneously in various locations within both the digital and physical realms. The DToP generates an intricate virtual model mirroring the physical person. This is achieved through sensors that transmit information or two-way Internet of Things connections, enabling synchronization between the digital and physical environments. It receives real-time updates and employs simulation, machine learning, and reasoning to support decision-making processes. Any alterations in the tangible world are mirrored in the digital representation of the twin. Due to these factors, DToP holds significant disruptive potential in the medical field. Additionally, through decentralized and encrypted databases, DToP technologies enable secure storage and transmission of data, ensuring that only the data owner can make any alterations. These technologies are integral to the metaverse concept, serving as a means for decentralized recording of digital ownership.

The issue of recognizing intellectual property rights for "works" generated by AI systems raises broader questions about the structure of copyright. This prompts a comprehensive evaluation, focusing on two fundamental queries: whether the input/output of the algorithmic processes can be legally appropriated and recognized by copyright, and how the notions of "free"/protected expressions of ideas should be understood in the era of generative AI.

Medical device: Metaverse-related applications certified for medical purpose

When the use of an electronic medical device takes place in the context of medical treatment, it usually seems to serve as a tool that helps to make decisions that pertain to the health professional. However, the application of certain regulations will differ depending on the purpose of each specific tool. The versatility of metaverse-enabled technologies raises the question of whether certain associated tools should even be classified as means for medical use. Depending on the factual circumstances, for example, an augmented reality (AR) headset worn by the patient may or may not meet the criteria of a medical device or its accessory. Only if the destination of the device meets some requirements it should be subject to medical device certification and all the safety and quality requirements set out by the European Regulation.[19] On the contrary, if the software acts just as an advanced videoconference tool, it would be difficult to consider them a medical device, considering the sole communication purpose between physicians and patients.

The European AI Act[15] represents an ambitious attempt to regulate the risks arising from the structural and proven opacity, complexity, data dependency, and capacity for autonomous decision-making behavior of AI systems. In the perspective chosen by the European legislator, however, the space devoted by the regulation to the protection of the person appears rather meagre, at least if one looks at the risk that the technologies related to eHealth may turn into a means through which the therapeutic alliance, which is an immediate corollary of the care relationship, may be undermined or emptied of content. The question is whether the care relationship continues to be structured exclusively on the doctor–patient pair or should the IA system also be included in the middle. Also, the U.S. Food and Drug Administration (FDA), in addressing the challenges related to Software as[20] a Medical device have considered that AI should not replace physician decision-making, but be used to assist clinicians. Future legal research should address how to identify the conditions for comprehensible but at the same time comprehensive information of AI, as well as a proportionate, reasonable, and appropriate use of intelligent medical devices, which does not renounce certain aspects of our humanity, in a new "digital humanism," for a medicine "with" machines and not "of" machines.

Another legal question arises from the possible serious harm to which the patient is exposed because of the concrete usage of digital devices within the treatment. Who is liable for damage caused to the patient by the incorrect evaluation of the AI medical device used? The European AI Act[15,16] (Art. 6, par. 2,) affirmed that the use of such AI systems should be classified as high risk since they are intended to be used as a safety component of a product, or the AI system is itself a product that requires a third-party conformity assessment pursuant to the Union harmonization legislation (EU Regulation 2017/745).

NFTs, intellectual property, and liability issues

We must also consider the legal issues connected to those digital assets and products that are defined as "non-fungible": the NFTs. There is no specific legislation on these tokens, so many legal issues related to this type of asset arise and they primarily concern identifying their juridical nature. U.S. legal doctrine qualifies NFTs as digital personal properties, affirming the need to treat NFTs as items of actual personal property, with the subsequent applicability of the regulation of the sale of personal property, in such a way as to clearly distinguish the legal situation relating to NFTs from that relating to licenses on intellectual property.[22] In fact, according to this theory, property regulation is better suited to how NFTs are used, as the owner can enjoy and dispose them without any external interference. This would conflict with the online intellectual property license model, where the owner of a work's intellectual property rights can decide how the copyright can be used or sold.[23] This approach is shared, for example, by the High Court of the United Kingdom which ruled that NFTs "*are to be treated as property as a matter of English law*" (case *Osbourne v. Persons Unknown and Ozone Inc.*).[24] According to a different theory, NFTs could be classified as atypical debt securities, attributable to the documents of legitimation used to identify the person entitled to the service since the contract is formed in a separate act.[25] According to this reconstruction, an NFT does not incorporate the digital content transferred between the parties. Still, it represents only a computer sequence subjected to a hashing process and some algorithmic properties of the token. This certificate is then uniquely connected via a link to an off-chain site where the digital product, an object of the transaction, is stored. Additionally, the smart contract is limited to executing the contractual provisions governed by the parties in separate natural language contracts. Therefore, the NFT would not incorporate any rights but would result in an enabling title allowing access to digital content. This approach leads the NFT to a sort of digital key that allows access, for instance, to the "*hotel room booked on the basis of a natural language contract with the manager of the accommodation facility*," allowing those identified as entitled to benefit from the digital content.[26,27]

Economic transactions: The decentralization opportunity

The metaverse is characterized by social life and technological exchange, mainly regulated by blockchain technologies. Blockchain is a decentralized distributed ledger technology that stores transactional data across multiple computers in an unchangeable manner. A blockchain is a chain of safe data composed of discrete blocks, each of which comprises a time stamp, a list of transactions, and a cryptographic hash of the

block before it. By accomplishing this, data security, integrity, transparency, and interoperability across various health care systems are ensured, making it resistant to manipulation and fraud.[28]

Activities in metaverses are not controlled by a single company or provider. These digital worlds are governed by decentralized autonomous organizations (DAOs), which are organizations without hierarchy or a chief executive officer (CEO).[29] Decisions are collectively made by their members, who each have a stake in the organization. The tool enables individuals to collaborate and organize with strangers globally, promoting transparency and democratic management of spaces through specific consensus mechanisms.[29] These mechanisms are designed to prevent any individual from changing or manipulating anything without the group's approval. DAOs eliminate the need to trust individuals within the group. Instead, trust is placed solely in the DAO's code, which is completely transparent and verifiable by anyone.

Conclusions

The evolving nature of metaverses introduces a multifaceted legal environment that necessitates comprehensive frameworks and perhaps new practices to address intellectual property rights, personality rights, product safety, data protection, contract and tort liabilities, and operational resilience concerns. All concerns have a supranational or international scope and go beyond the perspective of a particular legal system. Examples of such challenges include how to create policies from a comparative standpoint and what laws should be in place to sufficiently safeguard intellectual property rights and privacy in metaverses. An adequate (supranational) legislation is undoubtedly one step away from the first European debate. The competition among the world's legal systems (e.g., the FDA) will undoubtedly enhance the way this technology is managed in the future.

Authors' Contributions

B.P.: Conceptualization, project administration, supervision, and writing—original draft. A.B.: Conceptualization, project administration, supervision, and writing-original draft. A.G.: Writing—original draft. E.T.: Original drafting. F.Z.: Writing—review and editing. G.V.: Writing-orginal draft. L.P.: Project administration. A.S.: Supervision. A.C.: Conceptualization, writing—original draft, and writing—review and editing.

Declaration of Generative AI and AI-Assisted Technologies in the Writing Process

During the preparation of this work, the authors did not use AI or AI-assisted technologies.

Ethics Approval and Consent to Participate

This study does not involve human participants and ethical approval was not required.

Author Disclosure Statement

The authors declare no competing interests.

Funding Information

This work was supported by the Ministry of Enterprises and Made in Italy, Fondo per la Crescita Sostenibile-Accordi per l'innovazione di cui al D.M. 31 Dicembre 2021 e D.D. 14 Novembre 2022 Progetto Cod. F/350201/01–04/X60 "TERSICORE XRM-Tele-Rehabilitation Solutions with Innovative Cores of Extended Reality based on Metaverse." The funding body did not play any role in the design of the study and collection, analysis, and interpretation of data and in writing the article.

References

1. Maciejewski M. Metaverse. IPOL | Policy Department for Citizens' Rights and Constitutional Affairs. 2023; PE 751.222.
2. Durosini I, Strika M, Pizzoli SFM, et al. Emotions and "Sense of Presence" in the psycho-verse: psychological support for breast cancer survivors in the metaverse. In: Extended Reality. XR Salento 2023. Lecture Notes in Computer Science. Vol 14219. (De Paolis, L.T, Arpaia, P, Sacco, M eds.). Springer: Cham; 2023; doi: 10.1007/978-3-031-43404-4_28
3. Thomason J. MetaHealth - How will the metaverse change health care? Journal of Metaverse 2021;1(1):13–16.
4. Cerasa A, Gaggioli A, Marino F, et al. The promise of the metaverse in mental health: The new era of MEDverse. Heliyon 2022;8(11):e11762; doi: 10.1016/j.heliyon.2022.e11762
5. Stoumpos AI, Kitsios F, Talias MA. Digital transformation in healthcare: Technology acceptance and its applications. Int J Environ Res Public Health 2023;20(4):3407; doi: 10.3390/ijerph20043407
6. Gaggioli A, Cerasa A, Barresi G. Phygital mental health: opportunities and challenges. In: mHealth and Human-Centered Design Towards Enhanced Health, Care, and Well-being. Studies in Big Data. Vol 120. (Scataglini, S, Imbesi, S, Marques, G. eds). Springer: Singapore; 2023; doi: 10.1007/978-981-99-3989-3_2
7. Riva G, Wiederhold BK, Mantovani F. Searching for the metaverse: Neuroscience of physical and digital communities. Cyberpsychol Behav Soc Netw. 2024;27(1):9–18; doi: 10.1089/cyber.2023.0040
8. Wu P, Chen D, Zhang R. Topic prevalence and trends of metaverse in healthcare: A bibliometric analysis. Data Science and Management 2024;7(2):129–143; doi: 10.1016/j.dsm.2023.12.003
9. Calabrò RS, Cerasa A, Ciancarelli I, et al. The arrival of the metaverse in neurorehabilitation: Fact, fake or vision? Biomedicines 2022;10(10):2602; doi: 10.3390/biomedicines10102602
10. Cerasa A, Gaggioli A, Pioggia G, et al. Metaverse in mental health: The beginning of a long history. Curr Psychiatry Rep 2024;26(6):294–303; doi: 10.1007/s11920-024-01501-8

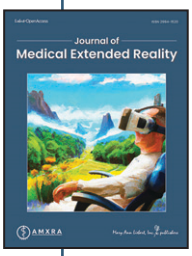
11. van Hulsen MAJ, Rohde KIM, van Exel J. Preferences for investment in and allocation of additional healthcare capacity. Soc Sci Med 2023;320: 115717; doi: 10.1016/j.socscimed.2023.115717
12. Solaiman B. From 'AI to Law' in healthcare: The proliferation of global guidelines in a void of legal uncertainty. Medicine and Law 2023;42(2): 391–406.
13. Zhu L. The Metaverse: Concepts and Issues for Congress. U.S Congressional Research Service; 2022. R47224. Available from: https://crsreports.congress.gov/product/pdf/R/R47224
14. 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). Available from: http://data.europa.eu/eli/reg/2016/679/oj
15. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Available from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689
16. Available from: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en
17. Handbook on European Data Protection law-2018 edition. ISBN 978-92-9491-901-4. Available from: https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition
18. BLume P. An alternative model for data protection law: Changing the roles of controller and processor. International Data Privacy Law 2015; 5(4):292–297; doi: 10.1093/idpl/ipv017
19. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.
20. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103 (INL)). Available from: https://www.fda.gov/medical-devices/digital-health-center-excellence/software-medical-device-samd
21. Mourtzis D. Digital twin inception in the Era of industrial metaverse. Front Manuf Technol 2023;3:1155735; doi: 10.3389/fmtec.2023.1155735
22. Wang R, Lee JA, Liu J. Unwinding NFTs in the shadow of IP law. American Business Law J 2024;61(1):31–55; doi: 10.1111/ablj.12237
23. Fairfield J. Tokenized: The law of non-fungible tokens and unique digital property. Indiana Law Journal, Forthcoming 2021. https://www.repository.law.indiana.edu/ilj/vol97/iss4/4
24. Available from: https://www.bailii.org/ew/cases/EWHC/Comm/2022/1021.html
25. Abhari S, Morita P, Miranda P, et al. Non-fungible tokens in healthcare: A scoping review. Front Public Health 2023;11:1266385; doi: 10.3389/fpubh.2023.1266385
26. Cellini R, Cuccia T, Lyrvall J. On the price dynamics of non-fungible tokens: The 'Bored Apes' case. PLoS One 2023;18(11):e0287881; doi: 10.1371/journal.pone.0287881
27. Yaghy A, Alberto NRI, Alberto IRI, et al. The potential use of non-fungible tokens (NFTs) in healthcare and medical research. PLOS Digit Health 2023;2(7):e0000312; doi: 10.1371/journal.pdig.0000312
28. Haleem A, Javaid M, Singh RP, et al. Blockchain technology applications in healthcare: An overview. Int J Intelligent Netw 2021;2:130–139; doi: 10.1016/j.ijin.2021.09.005
29. Goldberg M, Schär F. Metaverse governance: An empirical analysis of voting within Decentralized Autonomous Organizations. J Business Res 2023;160:113764; doi: 10.1016/j.jbusres.2023.113764

Cite this article as: Pasa B, Bernes A, Gaggioli A, et al. (2025) *LawVerse*: the legal framework for clinical metaverse content. *Journal of Medical Extended Reality* 2:1, 13–19, DOI: 10.1089/jmedxr.2024.0028.

Abbreviations Used

AR = augmented reality
CEO = chief executive officer
EU = European Union
VR = virtual reality

Publish in Journal of Medical Extended Realty



- Immediate, unrestricted online access
- Rigorous peer review
- Compliance with open access mandates
- Authors retain copyright
- Highly indexed
- Targeted email marketing

liebertpub.com/jmedxr