

# Rassegna

**di Diritto della Moda  
e delle Arti**

dottrina  
e giurisprudenza  
commentata

Rivista semestrale  
Fasc. 1/2024

[dirittomodaearti.it](http://dirittomodaearti.it)

ISSN 2785-6259

# Rassegna di diritto della moda e delle arti

*Rivista semestrale*

## **Direttore scientifico**

Prof. Enrico Damiani

## **Comitato di direzione**

Enrico Al Mureden (Alma Mater Studiorum Università di Bologna), Andrea Barengi (Università degli Studi del Molise), Laura di Bona (Università degli Studi Carlo Bo), Enrico del Prato (Università degli Studi di Roma La Sapienza), Romolo Donzelli (Università degli Studi di Macerata), Laura Marchegiani (Università degli Studi di Macerata), Sandro Nardi (Università degli Studi di Foggia), Barbara Pozzo (Università degli Studi dell' Insubria), Stefano Villamena (Università degli Studi di Macerata).

## **Comitato scientifico**

Benedetta Agostinelli (Università Roma Tre), Luca Barchiesi (Università degli Studi di Macerata), Nathan Allix (Université Paris II Panthéon-Assas), Alessio Bartolacelli (Università degli Studi di Macerata), Giovanni Berti De Marinis (Università di Perugia), Charles-Edouard Bucher (Université de Nantes), Ermanno Calzolaio (Università degli Studi di Macerata), Ilaria Caggiano (Università degli Studi Suor Orsola Benincasa), Francesca Cangelli (Università degli Studi di Foggia), Marta Cenini (Università dell' Insubria), Tommaso Dalla Massara (Università degli Studi di Roma Tre), Manuel Espejo Lerdo De Tejada (Universidad de Sevilla), Chiara Feliziani (Università degli Studi di Macerata), Francesco Gambino (Università degli Studi di Macerata); Fabrizio Marinelli (Università degli Studi dell' Aquila), Manuel Garcia Mayo (Universidad de Sevilla), Lucilla Gatt (Università degli Studi Suor Orsola Benincasa), Juan Pablo Murga Fernández (Universidad de Sevilla), Guido Noto La Diega (University of Stirling), Andreas Rahmatian (University of Glasgow), Carmela Robustella (Università degli Studi di Foggia), Claudio Scognamiglio (Università degli Studi di Roma Tor Vergata), Antoine Touzain (Université Rouen-Normandie), Laura Vagni (Università degli Studi di Macerata), Camilo Zufelato (Universidade de São Paulo).

## **Comitato di redazione**

Caporedattrici: Giorgia Vulpiani (Caporedattrice sezione moda – Università degli Studi di Macerata), Chiara Iorio (Caporedattrice sezione arte – Università degli Studi di Macerata).  
Alessandro Berrettini (Università degli Studi di Camerino), Chantal Bomprezzi (Università di Bologna), Luca Antonio Caloiaro (Università degli Studi di Roma Unitelma Sapienza); Sara Cavagnero (Northumbria University), Maxime Cormier (Université Paris II Panthéon-Assas), Josephine Cuozzo (Università degli Studi di Roma La Sapienza); Martina D' Onofrio (Università degli Studi di Verona), Jeanne De Dinechin (Université Paris II Panthéon Assas) Francesca Ferretti (Università degli Studi di Camerino), Clémentine Hebrard (Université Paris II Panthéon-Assas), Eva Helesbeux (Université Paris II Panthéon Assas), Carlotta Ippoliti Martini (Alma Mater Studiorum Università di Bologna), Daria Onitiu (University of Edimburgh); Cristina Evangelhia Papadimitriu (Università degli Studi di Messina); Michele Spinozzi (Università Politecnica delle Marche); Maria Zinno (Università degli Studi di Roma La Sapienza).

## **Comitato di referaggio**

Alessandra Dignani (Università di Macerata), Matilde D' Ottavio (Università Politecnica delle Marche), Francesca Guaricci (Università di Macerata), Miriam Larocca (Università di Camerino), Emanuele Montagna (Università di Camerino), Tanya Tiberi (Università di Macerata).

Registrazione presso il Tribunale di Macerata al n. 652/2022. Direttore responsabile: Lisa De Leonardis.

Editore: Associazione per la promozione dello studio e della ricerca in materie giuridiche, con sede in Macerata (MC), via Carducci n. 67

## *The legal framework for Metaverse and its application in healthcare*

Alessandro Bernes (Università Ca' Foscari Venezia), Antonio Cerasa (Istituto di BioImmagini e Sistemi Biologici Complessi, IBSBC-CNR, Milano), Barbara Pasa (IUAV, Venezia), Emanuele Tuccari (Università di Pavia), Giorgia Vulpiani (Università degli Studi di Macerata)\*

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 (LawVerse), and operational resilience concerns, specifically for clinical metaverse content (MedVerse). Generally speaking, 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 legal rules should be in place to sufficiently safeguard, for instance, intellectual property rights and privacy in Metaverses. To address Metaverses' challenges, policymakers need a global, holistic perspective encompassing all sectors of law. Key strategies include fostering international collaboration and adopting an interdisciplinary approach, ensuring standard but also regulatory flexibility, in order to prioritize user protection, integrating ethical considerations, promoting education, and embracing continuous policy review and adaptation. The transnational and adaptive approach seeks to develop effective policies that protect rights and interests within the diverse and evolving landscapes of the Metaverse applied to healthcare sector, the so-called MedVerses.

SUMMARY: 1. Introduction. – 2. Expanding Metaverse Applications: MedVerse and LawVerse. – 3. Data protection, digital twin, AI generated content and user-generated content. – 3.1. Data protection in a specific Metaverse: the MedVerse. – 3.2. User-generated content, AI-generated content and intellectual property rights. – 3.3. NFTs, intellectual property and liability issues. – 3.4. Medical device: metaverse-related applications certified for medical purpose. – 4. Synthesis and provisional conclusions on the MedVerse implications.

1. In recent years, the impact of progressive digitalization on both industry and society has been significant<sup>1</sup>. Digital transformation is influencing every aspect of daily life by enhancing networking and operational efficiency<sup>2</sup>. Healthcare is a primary focus for digital companies due to the expanding application of digital solutions in clinical decision support, telehealth, healthcare IT systems, and more. Digitalization offers new opportunities to improve the efficiency and patient-friendliness of medical care<sup>3</sup>.

---

\* All the authors have collaborated intensively on this paper and are listed in alphabetical order. However, for the purposes of evaluation, paragraph 1 can be attributed to all 5 co-authors, while paragraph 2 and 3.2. can be attributed to Pasa, paragraph 3 both to Pasa and Tuccari; paragraph 3.1. to Tuccari; paragraph 3.3. to Vulpiani, paragraph 3.4. to Bernes; paragraph 4 to Cerasa.

<sup>1</sup> L.M. FONSECA, *Industry 4.0 and the digital society: concepts, dimensions and envisioned benefits*, in *Proceedings of the International Conference on Business Excellence*, 2018; 12(1), pp. 386-397, <https://doi.org/10.2478/picbe-2018-0034>.

<sup>2</sup> S. KRAUS, S. DURST, J.J. FERREIRA, P. VEIGA, N. KAILER, A. WEINMANN, *Digital transformation in business and management research: An overview of the current status quo*, in *International Journal of Information Management*, 2022 (63) 102466; doi: 10.1016/j.ijinfomgt.2021.102466.

<sup>3</sup> A.I. STOUMPOS, F. KITSIOS, M.A. TALIAS, *Digital Transformation in Healthcare: Technology Acceptance and Its Applications*, in *International Journal of Environmental Research and Public Health*, 2023, 20(4), p. 3407. doi: 10.3390/ijerph20043407.

Within healthcare IT systems, one particularly promising area is the Metaverse. Recently, the Metaverse has attracted significant attention from the research community, with substantial work already conducted on its concepts, design, and applications. A review of articles published on PubMed from 2021 to the present shows an exponential increase in publications related to the Metaverse and health. Starting with Siyaev and Jo's initial paper<sup>4</sup> on using the Metaverse for training aircraft engineers, hundreds of papers have since been published.

Preliminary evidence suggests that transitioning from a Psycho-Verse<sup>5</sup> to a Meta-Health<sup>6</sup> or Med-Verse<sup>7</sup> perspective will position healthcare as one of the main applications of the Metaverse. The growing accessibility and affordability of virtual reality technology have sparked increasing interest in exploring the potential benefits of virtual environments for improving mental health. Individuals suffering from mental health disorders such as depression, anxiety, and eating disorders often find it challenging to interact socially in the real world. For these individuals, the Metaverse can provide a secure environment where they can communicate with therapists.

The Metaverse is not merely a technique, program, device, or system. It is a 'federation' of multiple technologies, including artificial intelligence, tangible and multimodal interfaces, blockchain, and the Internet of Things. These technologies are shared by multiple users simultaneously, connecting 3D environments to cyber-physical devices and their data, thus enabling seamless interaction between the virtual and real worlds—known as the "phygital" space<sup>8</sup>—managed by AI algorithms.

Experts worldwide refer to a broader methodological shift that promises to revolutionize the use of immersive technology in medicine with the advent of the Metaverse in healthcare. The development of new technologies that provide a multisensory experience shared by multiple users, creating a deep feeling of presence, will transform the way medical devices are used for rehabilitation, VR devices are employed for training medical students, residents, and fellows, and AI algorithms are utilized to predict individual responses. This transformation will enhance patient participation, ultimately promoting neural plasticity and overall well-being.

However, before implementing this federation of technologies in the medical field, we must address potential challenges such as virtual worlds, scalability, legality, financial flexibility,

---

<sup>4</sup> A. SIYAEV, G.S. JO, *Towards Aircraft Maintenance Metaverse Using Speech Interactions with Virtual Objects in Mixed Reality*, in *Sensors*, 2021, 21, p. 2066. <https://doi.org/10.3390/s21062066>. In the last few years, several clinical trials are underway (as reported by the *clinicaltrials.gov* website): (a) *The Use of Metaverse in Nursing Education* - NCT05829395; (b) *Metaverse-Based Healthy Life Program for Youth* - NCT05332886; (c) *The Effect of Metaverse-Based Nursing Skills Laboratory* - NCT05706584; (d) *Support Groups in the Metaverse for Ukrainian Refugees* - NCT06142032; (e) *Positive Youth Development in the Metaverse - a Pilot Study* - NCT05858593; (f) *Effectiveness of Metaverse Space-based Exercise Video Distribution in Young Adults* - NCT06019156; (g) *Examining the Effect of Metaverse-Based Epilepsy Education* - NCT06195020; (h) *Comparing Machine Guided VR Based Training With Educator Guided Training in Metaverse* - NCT06288087; (i) *Multidimensional Rehabilitation Intervention in Colorectal Cancer Survivors* - NCT05956990.

<sup>5</sup> I. DUROSINI, M. STRIKA, S.F.M. PIZZOLI, G. PRAVETTONI, *Emotions and "Sense of Presence" in the Psycho-Verse: Psychological Support for Breast Cancer Survivors in the Metaverse*, in DE PAOLIS, L.T., ARPAIA, P., SACCO, M. (eds) *Extended Reality. XR Salento 2023. Lecture Notes in Computer Science*, 2023; vol 14219. Springer, Cham. [https://doi.org/10.1007/978-3-031-43404-4\\_28](https://doi.org/10.1007/978-3-031-43404-4_28).

<sup>6</sup> J. THOMASON, *MetaHealth - How will the Metaverse Change Health Care?*, in *Journal of Metaverse*, 2021; 1(1), pp. 13-16.

<sup>7</sup> A. CERASA, A. GAGGIOLI, F. MARINO, G. RIVA, G. PIOGGIA, *The promise of the metaverse in mental health: the new era of MEDverse*, in *Helijon*, 2022; 8(11): p. 11762. doi: 10.1016/j.helijon.2022.e11762; R.S. CALABRÒ, A. CERASA, I. CIANCARELLI, et al., *The Arrival of the Metaverse in Neurorehabilitation: Fact, Fake or Vision?*, in *Biomedicines*, 2022; 10(10) p. 2602. doi: 10.3390/biomedicines10102602.

<sup>8</sup> A. GAGGIOLI, A. CERASA, G. BARRESI, *Phygital Mental Health: Opportunities and Challenges*, in S. SCATAGLINI, S. IMBESI, G. MARQUES (eds), *mHealth and Human-Centered Design Towards Enhanced Health, Care, and Well-being. Studies in Big Data* 2023; vol 120, Springer, Singapore, [https://doi.org/10.1007/978-981-99-3989-3\\_2](https://doi.org/10.1007/978-981-99-3989-3_2).

decentralization, security, and interoperability, as this technology is still in its infancy<sup>9</sup>. This prospective review aims to generate new ideas and insights while gaining a better understanding of the Metaverse and the obstacles it may face in creating private and secure immersive spaces. This novel attempt seeks to foster an interdisciplinary approach to the Metaverse and explore its potential for future developments.

2. Major commercial companies are developing their own platforms in the Metaverse, both in Western capitalist economies and in Eastern countries such as China. For instance, Alibaba and TikTok have made significant investments in augmented reality glasses maker and VR headset maker Pico.

Users are also investing time and resources in the Metaverse. For example, a user recently purchased a plot of land in the virtual world The Sandbox for € 3.7 million, marking the largest purchase in a metaverse to date. Another individual spent € 396,000 to become a virtual neighbour of the famous singer Snoop Dogg.

Now, it is the turn of institutions to enter the Metaverse, aiming to extend access to public utility services in these virtual spaces. Public utility services refer to essential services provided by the government or private entities that are crucial for the well-being and functionality of a community and society at large. In providing essential healthcare services, including hospitals, clinics, and public health programs, or ensuring access to basic education services, these institutions must uphold democracy, human dignity, citizenship, and participation, guaranteeing citizen rights such as the right to health for a vast number of people. So far, although there is currently a period of reduced enthusiasm for Metaverses due to their complexity and the need for sensors or wearables in the real world, Metaverses still provide significant opportunities and challenges for the healthcare sector<sup>10</sup>. Notable advantages include the increasing use of virtual reality in medical training, the application of Metaverses in digital therapeutics, the integration of augmented reality in surgical procedures, radiology enhancements, and the incorporation of medical wearables for mental health<sup>11</sup>. Furthermore, Metaverses hold great potential for revolutionizing medical education and advancing public health. It's also important to remember that Metaverses may be difficult to access, particularly for individuals with low digital literacy, disabilities, or those living in areas with poor connectivity.

Metaverse technologies in medicine can be applied in various ways, including e-health, telemedicine, remote monitoring (such as geriatric nursing and drug therapy), surgery, and medical education and training. These fields can be significantly enhanced by virtual, augmented, extended, and mixed reality. The use of Metaverse technologies offers benefits for both professionals and patients<sup>12</sup>.

For professionals, the vast amount of data collected through VR/AR equipment can lead to more accurate patient diagnoses and improved healthcare services, including surgery, by providing virtual, real-time representations of patients' conditions. Additionally, medical education, training,

---

<sup>9</sup> [https://www.europarl.europa.eu/RegData/etudes/STUD/2023/751222/IPOL\\_STU\(2023\)751222\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2023/751222/IPOL_STU(2023)751222_EN.pdf).

<sup>10</sup> S.W. WANG, W. WANG, *A review of the application of digital identity in the Metaverse*, in *Security and Safety*, 2023, 2: 2023009. <https://doi.org/10.1051/sands/2023009>.

<sup>11</sup> A. GARAVAND, N. ASLANI, *Metaverse phenomenon and its impact on health: A scoping review*, in *Informatics in Medicine Unlocked*, 2022, 32, doi: 10.1016/j.imu.2022.101029.

<sup>12</sup> H. ULLAH, S. MANICKAM, M. OBAIDAT, S.U.A. LAGHARI, M. UDDIN, *Exploring the Potential of Metaverse Technology in Healthcare: Applications, Challenges, and Future Directions*, in *IEEE Access*, 2023, vol. 11, pp. 69686-69707, doi: 10.1109/ACCESS.2023.3286696.

scientific research, and technological development can benefit from using this data to refine clinical evaluation processes, train algorithms, and advance artificial intelligence (AI).

For patients, the benefits include more personalized treatments, such as therapeutic applications for mental health and physical rehabilitation, reduced travel costs to physical hospitals, increased awareness of their health data through 3D models, and better explanatory information about their medical conditions and treatments.

However, as with any new technology, there are potential risks and challenges that must be addressed<sup>13</sup>. Implementing Metaverses in medicine and healthcare requires careful consideration<sup>14</sup>, especially regarding the extension of legal and ethical issues that have emerged in research on virtual health communities, telehealth, and AI in healthcare<sup>15</sup>. It is crucial to emphasize that challenges extend beyond privacy and data protection concerns. They encompass safe technological development, production integrity, and accurate medical diagnosis, along with contract and tort liabilities. New digital tools significantly influence doctor-patient interactions, raising awareness of heightened individual risks. Furthermore, Metaverses, as immersive and persistent virtual 3D environments where users actively create worlds and interact via digital humans or digital twins (DTOP), present numerous opportunities and challenges across legal domains, including intellectual property laws. Both the European Parliament<sup>16</sup> and the US Congress<sup>17</sup> have expressed interest in legal implications specific to Metaverses. They have highlighted concerns about potentially exacerbating existing issues seen in contemporary online platforms, such as illicit content moderation, consumer manipulation through advertising, data privacy, competition, and intellectual property protection.

Moreover, concerns extend to ownership or contractual control of digital assets within Metaverses, legal complexities involving smart contracts, NFTs, and virtual currency transactions among avatars.

Additional worries involve money laundering, gambling, and security vulnerabilities linked to potential connections between the dark web and Metaverses. Therefore, it is essential to outline legal concerns surrounding the development of the LawVerse framework, especially in public services like healthcare, focusing on medical device regulations, copyright, data protection, and decentralization. Our prospective review also delves into ethical considerations concerning the potential integration of Metaverses in healthcare settings.

3. Individuals engage in Metaverses by utilising avatars and specialised equipment like VR headsets, fostering an immersive experience. This involves the gathering of extensive data, encompassing biometric information and details about users' emotional and physiological reactions, constituting sensitive personal data subject to the European General Data Protection Regulation (GDPR)<sup>18</sup>. Consequently, their engagements necessitate careful consideration and an

---

<sup>13</sup> M. VAN HULSEN, K. ROHDE, J. VAN EXEL, *Preferences for investment in and allocation of additional healthcare capacity*, in *Soc Sci Med*, 2023; 320:115717. doi: 10.1016/j.socscimed.2023.115717.

<sup>14</sup> [https://ec.europa.eu/economy\\_finance/recovery-and-resilience-scoreboard/health.html](https://ec.europa.eu/economy_finance/recovery-and-resilience-scoreboard/health.html).

<sup>15</sup> B. SOLAIMAN, *From 'AI to Law' in Healthcare: The Proliferation of Global Guidelines in a Void of Legal Uncertainty*, in *Medicine and Law*, 2023; 42(2), pp. 391-406.

<sup>16</sup> [https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/intellectual-property-metaverse-episode-in-copyright-2022-06-30\\_en](https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/intellectual-property-metaverse-episode-in-copyright-2022-06-30_en)

<sup>17</sup> L. ZHU, *The Metaverse: Concepts and Issues for Congress*, U.S Congressional Research Service, 2022; R47224. <https://crsreports.congress.gov/product/pdf/R/R47224>.

<sup>18</sup> See <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

explicit «user consent» for every intended use of those personal data. The access to such sensitive data also raises the potential for invasive profiling methods, leading to detrimental outcomes like the loss of personal autonomy and decision-making control, or manipulation of vulnerable groups.

Addressing the storage, handling, and protection of data in the Metaverse is crucial, accompanied by accountability for potential data theft or misuse. Compliance with the GDPR necessitates explicit user consent for each specific purpose, varying based on activities within the Metaverse, such as attending a concert, participating in an auction, or engaging in research. Concerns arise as users' data is expected to be collected more extensively and continuously during their metaverse experiences, potentially making involuntary and ongoing consent challenging. 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 issue of interoperability and user movement within and across various Metaverses, along with the transfer of their data and assets, prompts considerations about data sharing and portability. Companies, often inclined towards proprietary rights over user data, will be required to create data sharing agreements. These agreements must adhere to data protection requirements, including obtaining user consent and fulfilling privacy notification obligations. Balancing proprietary interests with data protection standards becomes essential in facilitating seamless user experiences across different metaverse platforms.

Ensuring data protection in decentralized metaverse models poses additional challenges. 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. Nevertheless, tensions exist between blockchain technology and data protection regulations. To address this issue, some suggest the adoption of regulatory guidance, codes of conduct, and certification mechanisms. These measures aim to enhance legal certainty and ensure that decentralized metaverse models effectively navigate the complexities of both blockchain and data protection regulations.

The EU Parliament 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»<sup>19</sup>. It is important to note that any mix between the two is possible, in singular or multiple versions. The digital twin of a person (DTOP), for instance, not only replicates a distinctive person, but also constitutes a nearly instantaneous synchronized multipresence. 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 (or object or system). This is achieved through sensors that transmit information or two-way internet of things (IoT) 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 (or movements, actions, etc) 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. Employing a digital twin – a virtual model or simulation created from real-world data – offers substantial advantages in understanding and improving real-world objects, processes, or systems. This approach stands to

---

<sup>19</sup> M. MACIEJEWSKI, *Metaverse*, IPOL | Policy Department for Citizens' Rights and Constitutional Affairs, 2023; PE 751.222, p. 11 ([https://www.europarl.europa.eu/RegData/etudes/STUD/2023/751222/IPOL\\_STU\(2023\)751222\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2023/751222/IPOL_STU(2023)751222_EN.pdf)).

benefit patients greatly in the healthcare sector<sup>20</sup>. 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.

3.1. The main data protection issues of Metaverses arise punctually in the MedVerse. Indeed, the immersive experience of the MedVerse involves the collection of a large scale of data, including biometric information and details of users' emotional and physiological reactions, which constitute «special categories of personal data» subject to the GDPR.

Thus, the collection of such data requires – under Article 9, par. 2, GDPR – «the explicit consent of the user for any intended use»<sup>21</sup>. The informed consent must be specific to the purpose of the processing, taking on new dimensions in this case: patients must be informed, for example, about how their data will be used, the nature and fundamental characteristics of virtual therapy, and all the potential risks associated with VR technologies (from the psychological impact to the dangers of a possible sensitive data breach). Only in this way does it seem possible to ensure an explicit (informed, but above all conscious) consent of the patient to the collection of «special categories of data» for their subsequent processing in the digital therapeutic context.

Furthermore, according to Art. 9, par. 4, GDPR, «Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health»<sup>22</sup>.

To ensure the interoperability and movement of users, along with the transfer of their data and assets, agreements on data sharing and portability need to be established, focusing not only on obtaining users' consent, but also on fulfilling privacy notification obligations. This is intended to balance the interests of patients with those of data controllers, with a view to facilitating users' experiences in the MedVerse, while pursuing the ideal of legal certainty and the protection of individual rights.

Moreover, defining the roles of data controllers and processors is a significant challenge due to the intricate interconnections between entities in a virtual universe as complex as the MedVerse. Establishing a clear distinction of responsibilities and actions on behalf of users becomes, in fact, a complex task in this interconnected environment also with specific reference to data processing

---

<sup>20</sup> K. BHUGAONKAR, R. BHUGAONKAR, N. MASNE, *The Trend of Metaverse and Augmented & Virtual Reality Extending to the Healthcare System*, in *Cureus*, 2022; 14(9):e29071. doi: 10.7759/cureus.29071; B. MARR, *How AI And Machine Learning Will Impact The Future Of Healthcare*, <https://www.forbes.com/sites/bernardmarr/2022/09/14/how-ai-and-machine-learning-will-impact-the-future-of-healthcare/?sh=3dbc07047e5>

<sup>21</sup> For an overview on the nature of “consent” see S. THOBANI, *I requisiti del consenso al trattamento dei dati personali*, Santarcangelo di Romagna, 2016, 5 ss.; C. IRTI, *Consenso “negoziato” e circolazione dei dati personali*, Torino, 2021, 74 ss. It is not possible here to recall in full a literature which, with the passage of time, has become almost endless. See, even with very different approaches, D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, 339; A. FICI, E. PELLECCIA, *Il consenso al trattamento*, in AA.VV., *Diritto alla riservatezza e circolazione dei dati personali*, I, a cura di R. PARDOLESI, Milano, 2003, 469 ss.; S. MAZZAMUTO, *Il principio del consenso e il potere di revoca*, in AA.VV., *Libera circolazione e protezione dei dati personali*, a cura di R. PANETTA, I, Milano, 2006, 993 ss., spec. 1026-1027; and, more recently, G. VERSACI, *Consenso al trattamento dei dati personali e dark patterns tra opzionalità e condizionalità*, in *Nuove leggi civ. comm.*, 2022, 1130 ss.; ID., *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2020, 61 ss., 137 ss., 168 ss.; V. BACHELET, *Il consenso oltre il consenso*, Pisa, 2024, 76 ss.

<sup>22</sup> See art. 2-septies of the Italian Personal Data Protection Code, headed «Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute». Thus the Italian Data Protection Authority establishes, every two years, guarantee measures.



risks. This risk is, moreover, aggravated by today's "top-down" (rather than "networked") approach to the relations between different data processors under the current regulatory framework inferable from the GDPR<sup>23</sup>.

The compliance with the GDPR – which, as we have already seen, mandates data storage, processing and protection, accompanied by accountability for the potential theft or misuse of data – requires also a data protection impact assessment (see Art. 35, par. 3, lett. b) GDPR) and the designation (by the controller and the processor) of a Data Protection Officer (DPO: see Art. 37, par. 1, lett. c) GDPR)<sup>24</sup>.

Further problems may then derive from the use of potentially very invasive profiling methods (see Art. 22 GDPR), with important risks relating to the possible reduction (up to the loss) of personal autonomy and decision-making control (especially with reference to vulnerable groups)<sup>25</sup>. This suggests that strong security measures should be implemented to ensure the protection of special categories of patients' data in order to better pursue the therapeutic purposes underlying the MedVerse processing. Among other measures, according to Art. 30 GDPR, the controller (and, where applicable, the controller's representative) maintains a record of processing activities under its responsibility, and the processor (and, where applicable, the processor's representative) maintains a record of all categories of processing activities carried out on behalf of a controller.

In this regard, regulations and proposals are flourishing not only at supranational level – in addition to the GDPR, an important debate concerned the "AI Act"<sup>26</sup> (and the Regulation on the "European Health Data Space" (EHDS))<sup>27</sup> – but also at national level, with the presentation of a series of interesting legislative proposals (in Italy, see, recently, the so-called "Lorenzin proposal", presented the 5th March 2024 to the Senate of the Republic<sup>28</sup>, concerning the regulation to address in a protected environment – the so called sand-box – the limits placed on the use of health data

<sup>23</sup> See *Handbook on European Data Protection law*, 2018, p. 101-113, available at [https://www.echr.coe.int/documents/d/ecbr/handbook\\_data\\_protection\\_ENG](https://www.echr.coe.int/documents/d/ecbr/handbook_data_protection_ENG)

<sup>24</sup> See G. GEORGIADIS, G. POELS, *Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review*, in *Computer Law & Security Review*, 44, 2022, 105640; P. LAMBERT, *The Data Protection Officer. Profession, Rules, and Role*, Routledge, London, 2017; G. M. RICCIO, *Artt. 37-39*, in G. M. RICCIO, G. SCORZA, E. BELISARIO (eds.), *GDPR e Normativa Privacy. Commentario*, Milano, 2018, 339 ss.; F. SARTORE, *La valutazione d'impatto nel GDPR*, in R. PANETTA (ed.), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato: commentario al regolamento UE n. 2016/679 (GDPR) e al novellato D.Lgs. n. 196/2003 (codice privacy)*, Milano, 2019, 333 ss.; C. SOLINAS, *La nuova figura del responsabile della protezione dei dati*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (eds.), *I dati personali nel diritto europeo*, Torino, 2019, 879 ss.; R. TORINO, *La valutazione d'impatto (Data Protection Impact Assessment)*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (eds.), cit., 855 ss.

<sup>25</sup> On this issue, see, among others, B. PARENZO, *Profilazione e discriminazione. Dal GDPR alla Proposta di Regolamento sull'IA*, in *Tecnologie e diritto*, 2023, p. 105 ss.; D. IMBRUGLIA, *Il diritto per l'intelligenza artificiale*, in G. MAGRI, S. MARTINELLI, S. THOBANI (eds.), *Manuale di diritto privato delle nuove tecnologie*, Torino, 2022, p. 225 ss.

<sup>26</sup> The different versions of the text of the AI Act (along with many other documents of great interest for the analysis and interpretation of EU regulatory intervention) are easily available online: <https://artificialintelligenceact.eu/>. See, among others, G. FINOCCHIARO, *Intelligenza artificiale. Quali regole?*, Bologna, 2024, 114-115. For some critical voices (no longer on the AI Act proposal, but directly) with reference to the final text of the AI Act (and how more could have been done in terms of protecting special categories of personal data), see <https://www.accessnow.org/press-release/ai-act-failure-for-human-rights-victory-for-industry-and-law-enforcement/>; <https://reclaimyourface.eu/eu-ai-act-will-fail-commitment-to-ban-biometric-mass-surveillance/>.

<sup>27</sup> On the "European Health Data Space", for an official overview, see: [https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space\\_en](https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en). And, for a policy comment, see L. MARELLI, M. STEVENS, T. SHARON, I. VAN HOYWEGHEN, M. BOECKHOUT, I. COLUSSI, A. DEGELSEGGER-MARQUEZ, S. EL-SAYED, K. HOEYER, R. VAN KESSEL, D. KREKORA ZAJAC, MIHAELA MATEI, S. RODA, B. PRAINSACK, I. SCHLÜNDER, M. SHABANI, T. SOUTHERINGTON, *The European health data space: Too big to succeed?*, in *Health Policy*, (135) 2023, 1 ss.

<sup>28</sup> See <https://www.senato.it/leg/19/BGT/Schede/FascicoloSchedeDDL/ebook/58053.pdf>.

by administrative and supervisory authorities and internal control structures of entities engaged in scientific research, and the so-called “AI proposal”, presented the 20th May 2024 to the Senate of the Republic, concerning also standards for the use of AI in healthcare, balancing innovation and data protection)<sup>29</sup>.

3.2. Regarding intellectual property matters, copyright is frequently viewed as a barrier for companies collaborating with online content and their user base. The legitimacy of profits accruing to copyright and related rights holders comes under scrutiny, particularly due to their detachment from the creation process and their redirection to the content “industrialization” and “serialization”, also through emerging AI technologies.

There is a call for a reassessment of the argument for the public to bear all costs associated with the production and access to knowledge, excluding those attributed to copyright. Who should bear these costs? Advocates argue for a more balanced approach that considers the interests of both content creators and the wider public in the realm of intellectual property. 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.

The analysis will be grounded on two premises:

- (i) the necessity to maintain an anthropocentric approach towards the challenges posed by technologies, aligning with the increasing centrality of the ‘person’ in national and European legal systems since the latter half of the 20th century, and the goals of the EU digital agenda; and
- (ii) the aspiration to reconceptualize copyright law as a model of a more inclusive property paradigm.

Early as 2020, the European Parliament adopted the Resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies, which suggested an approach that take into account the degree of human intervention, the autonomy of AI, the importance of the role and the origin of the data and copyright-protected material used and the possible involvement of other relevant factors. The resolution enlightened how we need to distinguish between “AI-assisted human creations” and “AI-generated content”. In particular, it is the latter that creates challenges for intellectual property rights protection, such as questions of ownership, inventorship and appropriate remuneration, as well as issues related to potential market concentration. In fact, a work autonomously produced by artificial agents and robots might not be eligible for copyright protection, in order to observe the principle of originality, which is linked to a natural person, and since the concept of ‘intellectual creation’ addresses the author’s personality. This issue already emerged in the US case *Naruto vs. Slater*, where the US District Court for the Northern District of California denied the copyright protection of a picture taken by a monkey, for lack of “human creativity”<sup>30</sup>. Following the same logic, in 2023 the US courts admit that when

---

<sup>29</sup> See <https://www.senato.it/leg/19/BGT/Schede/FascicoloSchedeDDL/ebook/58262.pdf>.

<sup>30</sup> *Naruto, et al., Plaintiffs, v. David John Slater, et al., Defendants*. Case No. 15-cv-04324-WHO. 2016. <https://casetext.com/case/naruto-v-slater>

AI is used only as a “tool to assist an author” in the process of creation, the current IP framework should apply<sup>31</sup>.

Open Metaverses are marked by an extensive use of both user-generated content (UGC) and AI-generated content (so called AGC, also algorithm-generated content<sup>32</sup>). With user-generated content (UGC), individuals can modify fundamental aspects of digital environments and introduce entirely new features associated with their created content, such as virtual real estate, digital art, fashion and design items, avatars, and more. Copyright protection may apply to UGC if it adheres to the criteria of being the Author’s Own Intellectual Creation (AOIC), reflecting the creator’s personality and involving their free and creative choices—a standard referred to as the European AOIC test. However, accessing many of these Metaverses requires users to grant platforms a comprehensive license over their shared content, encompassing text, video, and images. This implies that users must provide the platform with substantial rights to utilize and distribute their UGC. Frequently, Terms of Service (ToS) not only impact the commercial utilization of copyrighted UGC, but also influence users’ freedom of expression online<sup>33</sup>. The platform’s standard contractual rules governing the availability, accessibility, visibility, and removal of such content can significantly impact users’ fundamental freedoms<sup>34</sup>.

In the content generation phase by the algorithm (AGC) equally substantial challenges arise<sup>35</sup>. Questions about the ownership of copyright for artistic works or patent rights for inventions produced by an AI system become paramount, also because patent law requires a comprehensive description of the underlying technology and that could pose challenges for certain AI technologies in view of the complexity of the reasoning.

A noteworthy case is the DABUS dispute, where Mr. Thaler, the owner and inventor of the AI machine DABUS, argued that also the AI can function as “inventor”. The machine, lacking human embodiment, currently lacks a fundamental requirement for acknowledging authorship: human intelligence in a physical form. The patent law protection of an AI invention was, for instance, denied by the UK Supreme Court in December 2023, on the grounds that the inventor must be a human, not a machine<sup>36</sup>. Nevertheless, there are no clear-cut answers to this issue. For instance, also the United States Copyright Office maintains that only human creativity qualifies for copyright or patent protection. Conversely, some offices, like the one in South Africa<sup>37</sup>, take a different stance, recognizing the concept of an artificial inventor. Alternative viewpoints suggest copyright or patent protection based on the assumption of a “joint creative effort” involving the machine and the author(s), who may be multiple individuals.

---

<sup>31</sup> Thaler v. Perlmutter US Copyright Office, United States District Court For The District Of Columbia 2023, Civil Action No. 22-1564 (BAH), <https://www.copyright.gov/ai/docs/district-court-decision-affirming-refusal-of-registration.pdf>.

<sup>32</sup> M.L.B. DOS SANTOS, *The “so-called” UGC: an updated definition of user-generated content in the age of social media*, in *Online Information Review*, 2022; DOI:10.1108/OIR-06-2020-0258.

<sup>33</sup> J.P. QUINTAIS, G. DE GREGORIO, J.C. MAGALHÃES, *How platforms govern users’ copyright-protected content: Exploring the power of private ordering and its implications*, in *Computer Law & Security Review*, 2023 (48), 105792. <https://doi.org/10.1016/j.clsr.2023.105792>

<sup>34</sup> K. Milityna, *Human Creative Contribution to AI-Based Output – One Just Can’t Get Enough*, in *GRUR International*, 2023; 72(10) pp. 939–949, <https://doi.org/10.1093/grurint/ikad075>

<sup>35</sup> European Commission Final Report 2020.

<sup>36</sup> Thaler (Appellant) v Comptroller-General of Patents, Designs and Trademarks (Respondent), [2023] UKSC 49, judgment issued on 20 December 2023, <https://www.supremecourt.uk/cases/uk-sc-2021-0201.html>

<sup>37</sup> See South African Patent Journal of 28<sup>th</sup> July 2021.

At present, the artificial intelligence system, the designer, the programmer, the user-content creator, could be considered an author, or none at all, and the resulting content might be considered communal property<sup>38</sup>.

The preference for analysing the protectability of AI outputs, rather than restricting considerations to the protection of input, stems from their role as the final expression of an «algorithmic “creative” process»<sup>39</sup>. This choice provides an ideal opportunity for more profound reflections on the meaning of creation, encompassing legal arguments related to the term “work” in Metaverses, and compliance with legal requirements.

Moreover, beyond legal aspects, there are systematic and political arguments that advocate for a more functional approach to understanding and addressing the phenomenon, particularly within the context of cognitive capitalism. Prominent brands are grappling with challenges related to the unauthorized use of registered trademarks in the Metaverses, with similar difficulties emerging in the realm of patent law. Legal complexities extend to VR and AR devices, which often serve as gateways to Metaverses. These devices fall within the scope of the European Regulation on general product safety (GPSR), requiring, among other things, suitable cybersecurity features for product protection. Additionally, the legal landscape may require the application of the Digital Operational Resilience Act (DORA), making sure that the financial sector in Europe is able to stay resilient in the event of a severe operational disruption, the Regulation on Markets in Crypto Assets (MiCA), which expressly does not cover non fungible tokens, which also raise some relevant legal issues.

Moreover, the European Commission issued the White paper on Artificial Intelligence and, in July 2024, the final text of the Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (so called Artificial Intelligence Act). For instance, the Regulation on Artificial Intelligence pays special consideration to the use of AI systems in healthcare services<sup>48</sup>. In particular, under Art. 6, par. 2, of the AI act, 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 harmonisation legislation listed in Annex II, which includes EU Regulation 2017/745 on medical devices. In this case, AI systems are also subject to the requirements set out by the AI act, as we will see in § 3.4.

As Metaverse’s content is disseminated and replicated across decentralized networks on Web 3.0 and blockchain-based platforms, issues arise regarding applicable law, jurisdiction, and the identification of infringers<sup>40</sup>. What happens, for instance, if the AI system is the “infringers” that

---

<sup>38</sup> A. ROTOLO, *Argumentation and explanation in the law*, in *Front Artif Intell.*, 2023 Sep 4;6:1130559. doi: 10.3389/frai.2023.1130559.

<sup>39</sup> A. ROTOLO; G. SARTOR, *AI and law : logic-based approaches*, in M. SELLERS, S. KIRSTE (eds), *Encyclopedia of the philosophy of law and social philosophy*, Dordrecht, Springer, 2020, <https://hdl.handle.net/1814/76348>; J.C. GINSBURG, L.A. BUDIARDJO, *Authors and Machines*, *Columbia Public Law Research Paper* No. 14-597, in *Berkeley Technology Law Journal*, 2019, 34(2). <http://dx.doi.org/10.2139/ssrn.3233885>

<sup>40</sup> A distinction has arisen between the various existing metaverses, open and closed, in relation to Web 3.0, which is important to highlight. Open Metaverses operate differently from closed ones. Activities in open Metaverses are decentralized using blockchain technology, meaning they 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 CEO. Decisions are collectively made by their members, who each have a stake in the organization; trust is placed solely in the DAO's code, which is transparent and verifiable by anyone. Their economic framework known as Decentralized Finance (DeFi) is exemplified by platforms such as The Sandbox. DeFi operates through decentralized applications (DApps) that execute transactions via blockchain, eliminating the need for intermediaries and making it accessible to the public. The decentralized finance model is a crucial part of the Web 3.0 system, representing a significant shift in the management of economic transactions, including contracts, ownership matters,

violates intellectual property rights? The question leads to the AI accountability issue. There are already some court cases against AI systems able to autonomously produce texts, music and paintings that were trained with protected works without the authorization of the intellectual property owner.

Furthermore, users and AI-generated content alike can create and manage multiple digital identities, each characterized by unique attributes. These digital representations go beyond static images, incorporating elements such as physical features, gestures, sounds, and movements to accurately reflect our identity and personality. It is crucial to protect against the potential misuse of avatars, particularly when they are manipulated for fraudulent activities on behalf of their creators. Securing our avatars is essential as they function as extensions of our digital identity in metaverses and have the power to influence the proprioceptive remodelling of our 'self'<sup>41</sup>. This not only poses a threat to one's reputation, but may also result in real-world liabilities for the individuals involved<sup>42</sup>. The complexity of this issue raises numerous legal concerns, starting with the protection of personality rights<sup>43</sup>. This includes rights like the right of publicity, preventing the commercial exploitation of one's image without permission or compensation, and the right to privacy, ensuring individuals are not publicly represented without their consent.

3.3. We must also take into account 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.

US legal doctrine qualifies NFTs as digital personal properties, affirming the need to treat non-fungible tokens 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. In fact, according to this theory, property regulation is better suited to how non-fungible tokens are used, as the owner can enjoy and dispose of 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<sup>44</sup>. This approach is shared, for example, by the High Court of the United Kingdom which, in the case *Osbourne v. Persons Unknown and Ozone Inc.*, ruled that non-fungible tokens «are to be treated as property as a matter of English law»<sup>45</sup>.

---

and other legal considerations, within Metaverses. See, E.A. HENRIKSSON, *Data protection challenges for virtual reality applications*, *Interactive entertainment law review*, 2018, 1(1), pp. 57-61, <https://doi.org/10.4337/ielr.2018.01.05>; P.M. YELLOWLEES, K.M. HOLLOWAY, M.B. PARISH, *Therapy in Virtual Environments—Clinical and Ethical Issues*, in *Telemedicine Journal and E-health*, 2021, 18(7), pp. 558-564, <https://doi.org/10.1089/tmj.2011.0195>.

<sup>41</sup> J. LIN, M.E. LATOSCHIK, *Digital body, identity and privacy in social virtual reality: A systematic review*, *Front. Virtual Real* 2022; 3:974652, doi: 10.3389/fvrr.2022.974652.

<sup>42</sup> B.C. CHEONG, *Avatars in the metaverse: potential legal issues and remedies*, in *Int. Cybersecur. Law Rev.*, 2022, 3, pp. 467-494, <https://doi.org/10.1365/s43439-022-00056-9>.

<sup>43</sup> G. RESTA, *The New Frontiers of Personality Rights and the Problem of Commodification: European and Comparative Perspectives*, *Tulane European and Civil Law Forum*, 2011; (26):33.

<sup>44</sup> S. REIS, *Toward a Digital transfer doctrine? The first sale doctrine in the digital era*, in *Northwestern University Law Review*, 2015, pp. 173-207; J. FAIRFIELD, *Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property*, in *Indiana Law Journal*, 2022, 1261.

<sup>45</sup> *Osbourne v. Persons Unknown and Ozone Inc.* [2022] EWHC 1021 (Comm), <https://www.bailii.org/ew/cases/EWHC/Comm/2022/1021.html>. See also Supreme Court of Singapore, *Janesh s/o*

According to a different theory, non-fungible tokens 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<sup>46</sup>. 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»<sup>47</sup> allowing those identified as entitled to benefit from the digital content. Another approach defines the non-fungible tokens as financial products, with the consequent applicability of the rules connected to financial products<sup>48</sup>.

Given the possibility of identifying different types of tokens that perform different functions, identifying the legal nature of non-fungible tokens is not a simple matter. It requires a case-by-case approach, as suggested by the European Union, to identify the most suitable discipline for protecting the interests involved. Although for some types of NFTs, their qualification as digital properties seem simple, other NFTs make this classification more problematic. Take, for example, the use of NFTs for the service of judicial documents, recently permitted by some courts in the United States and the United Kingdom.

One of the most interesting issues on NFTs concerns the possible safeguards in case of intellectual property infringements: think about the minting of an unauthorized work, or the illicit use of a trademark on a digital product<sup>49</sup>. In this regard, *Hermès v. Metabirkin* case<sup>50</sup> and *Juventus football club* case<sup>51</sup> represent some interesting examples where the judges applied to NFTs the intellectual property rules of non-digital goods. The first case concerns the sale of the “Metabirkin”, inspired by the Hermès Birkin model, created by Mason Rothschild and sold as NFTs. The famous fashion house Hermès sued Rothschild for trademark infringement, although on Rothschild’s site there was a disclaimer stating that “in no way are Metabirkin associated with

---

Rajkumar v Unknown Person [2022] SGHC 264. On this judgment, see P. MEZEI, *Hop up the Roller Coaster- New Hopes for digital Exaustion?*, in *GRUR International*, 71(11), 2022, pp. 1017–1018.

<sup>46</sup> G. NAVA, *I non fungible token*, in R. GIORDANO, A. PANZAROLA, A. POLICE, S. PREZIOSI, M. PROTO (eds.), *Il diritto nell’era digitale*, Milano, 2022, pp. 237-282.

<sup>47</sup> Authors’ translation.

<sup>48</sup> P. CARRIÈRE, *La cripto-arte e i non fungible tokens (NFTs): tentativi di inquadramento giuridico*, in *dirittobancario.it*, 2021.

<sup>49</sup> P. CAGLAYAN AKSOY, Z. OZKAN UNDER, *NFT e copyright: challenges and opportunities*, in *Journal of Intellectual Property Law & Practice*, 16,10, 2021, pp. 1115-1126; M.R. GARCIA TERUEL, H. SIMON-MORENO, *The digital tokenization of property rights. A comparative perspective*, in *Computer Law and Security Review*, 2021, 41, pp. 1-21; A. GUADAMUZ, *The treachery of images: non-fungible tokens and copyright*, in *Journal of Intellectual Property Law & Practice*, 2021, pp. 1-19; B. BODO, A. GIANOPOULOU, P. MEZEI, J.P. QUINTAIS, *The Rise of NFTs: These Aren’t the Droids You’re Looking For*, in *European Intellectual Property Review*, 2022, 44, 5, pp. 265-282.

<sup>50</sup> *Hermès International, et al. v. Mason Rothschild*, Case 1:22-cv-00384-JSR US Southern District of New York. <https://casetext.com/case/hermes-intl-v-rothschild-9>

<sup>51</sup> Court of Rome, 20 July 2022, *Dir. & Giust.*, 2022, p. 197, , annotated by V. IAIA, *La tutela del marchio Juventus si spinge nel metaverso*, in *Dir. ind.*, 2022, p. 487 ss. annotated by A. RAINONE, *Uso illecito del marchio altrui sulla blockchain: il principio di neutralità tecnologica e la rivoluzione mancata dei registri distribuiti*, in *Giustiziacivile.com* 16 January 2023, annotated by L. PANDOLFELLI, *La tutela del marchio nella creazione e commercializzazione di non-fungible token (NFT)*. On this topic, see also G. FACCI, *Il diritto d’immagine dei calciatori al tempo degli NFT (Non-fungible token)*, *Resp. civ. prev.*, 2023, p. 179 ss.

Hermès.” It is interesting to note that, in the motion to dismiss, Rothschild argued that he could use the term “Metabirkin” pursuant to the 1989 *Rogers v. Grimaldi* case<sup>52</sup>. More specifically, he argued that using the name of a famous trademark connected to a work of art does not constitute an infringement of the trademark, according to the First Amendment, if the name does not mislead with regard to the association with the mark itself. So, following that case, Rothschild affirmed that the Metabirkins were an autonomous work of art, comparable to the paintings of Andy Warhol’s Campbell soups, and their association with the Birkin brand could not mislead anyone. The District Court denied his motion and Hermès won the lawsuit. The District Court found that Rothschild’s NFTs were not protected speech under the First Amendment and ordered Rothschild to pay damages to Hermès for trademark infringement, trademark dilution, and cybersquatting. In the second case, Juventus Football Club, that owned as trademarks the words ‘JUVE’, ‘JUVENTUS’ and the team’s uniform, requested that the Court prohibit the unauthorized production and marketing by another company of NFT cards depicting a photograph of a former player wearing the team’s uniform. The Court of Rome pointed out that the registration of trademarks also pertains to “downloadable electronic publications” and that the football club itself was active in the field of crypto games and non-fungible tokens. As a result, the creation and marketing of the cards led to the counterfeiting of Juventus Football Club’s brands, concretizing the risk of confusion caused by the identity of the signs used. According to the Court, as the football club operates in the NFT sector, the marketing of NFT cards constitutes a hypothesis of unfair competition as a result of the unauthorized use of other people’s trademarks and the appropriation of the merits related to the trademarks used. There is also a danger of damage related to the possible vulgarisation of the trademark and in relation to the infringement of the rights of exploitation of the trademark itself. It, therefore, seems appropriate to affirm the extension of trademark and intellectual property protection to non-fungible tokens, as an artist who sees their work reproduced in NFT without authorization could sue the person who carried out the unauthorized minting.

There are also many liability issues regarding NFTs, which are difficult to solve. For instance, what would happen in the case of a subject that purchases an NFT that, after payment, receives only a jpeg file not linked to an NFT or a different NFT? In applying the sales rules, the purchaser could invoke the termination of the contract and the return of the price for the sale of *aliud pro alio*, in addition to compensation for the damage. The difficulty may lie in identifying the alienating subject, given the pseudonym of the blockchain. This issue is related to the blockchain accountability. At that point, the buyer could sue the platform where the NFTs were put on sale, asking for the seller’s identification.

Another issue could be the following: in theory, given the characteristics of the blockchain, NFTs could overcome the traditional problems concerning the authenticity and origin of the work, but this would be reliable only if the initial information recorded on blockchain were true, as these technologies are limited to recording what is entered, not certifying its veracity. Also, all the issues related to blockchain, and smart contracts are relevant.

3.4. When the use of an electronic medical device, or in general a technological device, takes place in the context of medical treatment, it usually seems to serve as a tool that helps to make decisions which pertain to the health professional. However, the application of certain regulations

---

<sup>52</sup> *Ginger Rogers v. Alberto Grimaldi, Mgm/ua Entertainment Co., and Pea Produzioni Europee Associate, S.R.L.*, 875 F.2d 994 (2d Cir. 1989), United States Court of Appeals, Second Circuit, 5<sup>th</sup> of May 1989.

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. In other words, shall the software and apps applied in Metaverses fall under the definition of “medical device”?

According to Article 2, paragraph 1, of European Regulation 2017/745 of April 5, 2017 on medical devices<sup>53</sup>, a medical device is «any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes: - diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease, - diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability, - investigation, replacement or modification of the anatomy or of a physiological or pathological process or state, - providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations, and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means»<sup>54</sup>. Depending on the factual circumstances, for example, an 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 aforementioned Regulation. On the contrary, if the software acts just as an advanced video-conference tool, it would be difficult to consider them a medical device, considering the sole communication purpose between physicians and patients.

The legal issues seem to intensify when the medical device is equipped with AI that does not merely collect data, but also generates outputs that translate into decisions both in terms of diagnosis and/or in terms of medical treatment on behalf of the physicians<sup>55</sup>. In the care relationship, the law leaves to the decisional role of the doctor the usage of a digital device, which is instrumental to the healthcare activities. The doctor should be considered the sole responsible for the treatment, since the stage of its definition: in order to fulfil the fundamental right to therapeutic self-determination, the doctor must inform the patient of the contents and consequences of the activities, but also of the instruments implied, as well as on the risks and benefits. In this sense, patients must be given accurate, adequate, and appropriate information to make an informed decision about their care. In addition, doctors need to consider the psychological, age and maturity conditions of the patient (especially for children and for the elderly and frail). However, it seems unrealistic that physicians can explain how digital technologies or even more algorithms work. Nevertheless, health professionals should also consider health

---

<sup>53</sup> Regulation (EC) No 178/2002 of the European Parliament and of the Council of 5.5.2017 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.

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745>

<sup>54</sup> See ECJ, 7.12.2017, C-329/16, Snitem e Philips France c. Premier ministre and Ministre des Affaires sociales et de la Santé, <https://curia.europa.eu/juris/liste.jsf?language=en&num=C-329/16>

<sup>55</sup> D. YANG, J. ZHOU, R. CHE, Y. SONG, Z. SONG, X. ZHANG, Q. WANG, K. WANG, C. ZHOU, J. SUN, L. ZHANG, L. BAI, Y. WANG, X. WANG, Y. LU, H. XIN, C. POWELL, C. THUEMLER, N. CHAVANNES, W. CHEN, L. WU, C. BAI, *Expert consensus on the metaverse in medicine, Clinical eHealth* (5) 2022, [doi.org/10.1016/j.ceh.2022.02.001](https://doi.org/10.1016/j.ceh.2022.02.001) European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017IP0051>; M. Veale, F.Z. Borgesius, *Demystifying the draft EU artificial intelligence act: Analysing the good, the bad, and the unclear elements of the proposed approach*, in *Computer Law Review International*, 2021; 22(4): p. 97–112.



concerns caused by access to Metaverses, such as motion sickness, also known as cybersickness, which mostly includes symptoms such as nausea, disorientation, drowsiness, headaches, eye strain, etc. This is particularly problematic in the case of minors and old people.

Another legal question arises from the possible serious harm to which the patient is exposed as a result 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? AI itself cannot be considered obliged to pay, so it could be the hospital, the doctor, or the manufacturer, depending on the type of harm that occurred in the misdiagnose. In this sense, the Regulation on Artificial Intelligence (so called AI act) pays special consideration to the use of AI systems in healthcare services. In particular, under Art. 6, par. 1, of the Regulation, 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 harmonisation legislation listed in Annex II, which includes EU Regulation 2017/745 on medical devices. In this case, AI systems are also subject to the requirements set out by the AI act.

Considering that the aforementioned AI Act lacks the provision of civil remedies, the European Commission has proposed the AI Liability Directive (AILD) and the revised Product Liability Directive (PLD) to complement the AI Act. However, it is remarkable to ascertain whether the doctors made an erroneous decision despite having accurate data or not. In the latter scenario, the responsibility lies more on the producer rather than the healthcare provider. For the manufacturer, the challenge will be to create medical devices adapted to the new legal framework based on a risk-preventive approach. For medical practitioners, in this case, the combination of Metaverse, AI, and technologies raises the standard of care within the professional service provided by the doctor. This underlines the importance of appropriate education, training and preparation, in order to secure the highest degree of professional competence possible, as well as to safeguard and protect patients' health<sup>56</sup>. Not only specific rules, but also best practices and guidelines may be necessary around issues including deontological, ethics and regulatory compliance.

The potential of Metaverses in healthcare appears unlimited, but the legal sphere often catches up to technological developments after the fact, once they have been implemented, potentially used widely to help patients, or caused harm to individuals that do not have robust legal avenues for redress. Metaverses and digital technologies surely would improve the direct relationship doctor-patient, but they shall never substitute the fundamental decisional and informative role played by those who provide healthcare services, as well as the producers/providers' liability.

4. The integration of the Metaverses in the healthcare sector brings about unique challenges and considerations for upholding legal and deontological ethics. The last two years have seen an exponential increase in the interest in this type of technology in clinical medicine. For this reason, the new term MedVerse<sup>57</sup> has been coined in order to explain how the metaverse-related technologies could be applied to improve medical practice. For instance, According to Yang and

---

<sup>56</sup> European Parliament Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).

<sup>57</sup> A. CERASA, A. GAGGIOLI, F. MARINO, G. RIVA, G. PIOGGIA, *The promise of the metaverse in mental health: the new era of MEDverse*, in *Heliyon*, 2022 Nov 23;8(11):e11762. doi: 10.1016/j.heliyon.2022.e11762.

colleagues' proposal<sup>58</sup> this kind of platform would offer the chance to create an online environment where clinicians and patients could interact while receiving clinical care (dissection, diagnosis, consultation). Mesko<sup>59</sup> further proposed that real-world medical technologies such as chatbots, cellphones, and telehealth systems may someday be replaced by a virtual university in the metaverse, where instructors may teach pupils about the inner workings of the circulatory system. For the healthcare sector, the core element will be the ability to construct multi-user situations where multiple patients may cooperate to complete social activities for rehabilitative purposes. Particularly in psychiatric<sup>60</sup> and neurological disorders<sup>61</sup>, the metaverse-related tools will be employed to exploit the "synchronized brains" potential exacerbated by social interactions.

These virtual environments have the potential to greatly improve patient care through innovative treatment methods, greater accessibility, and personalized experiences. However, they also bring new ethical questions that practitioners must address. Exploring the deontological aspects within the context of the MedVerse requires an examination of how traditional ethical duties are impacted by this emerging digital landscape.

#### *Confidentiality in virtual worlds*

Upholding patient confidentiality is a challenging issue in the emerging MedVerses. Within this digital landscape, extensive data encompassing behavioural, biometric, and interaction information can potentially disclose sensitive patient details<sup>54</sup>. Therefore, practitioners must ensure that these digital spaces adhere to data protection regulations (such as GDPR) and implement strong security measures to safeguard patient confidentiality. This responsibility remains crucial regardless of the technological environment used to deliver therapy.

#### *Informed consent*

In the MedVerse, obtaining informed consent takes on new dimensions. Patients need to be informed about how their data will be used, the nature of virtual therapy, and any potential risks associated with VR technologies such as psychological impacts, data privacy, or personality rights concerns. Practitioners must ensure that patients fully understand these aspects, respecting their autonomy in the digital therapeutic setting.

#### *Non-maleficence and beneficence in virtual therapy*

The principles of avoiding harm and acting in the best interest of the patient require careful consideration of the potential impacts of VR-based therapies, digital twins (DTOP) and other persistent virtual 3D environments. While these technologies offer innovative ways to address mental health issues, practitioners must critically assess the evidence supporting their efficacy and safety. Any intervention in the MedVerse should be backed by robust research to ensure it meets ethical standards<sup>53</sup>. Additionally, practitioners must remain vigilant in monitoring the well-being of their patients during virtual therapy sessions<sup>57</sup>. They should be prepared to recognize signs of distress or adverse reactions and have protocols in place to provide immediate support or referral to appropriate care<sup>56</sup>. This is particularly important, for example, in the context of disaster mental health, where virtual reality offers a potentially effective tool for psychological resilience training and counselling.

---

<sup>58</sup> D. YANG, J. ZHOU, R.C. CHEN, Y.L. SONG, Z.J. SONG, X.J. ZHANG, Q. WANG, C.Z. ZHOU, J.Y. SUN, L.C. ZHANG., L. BAI, Y.H. WANG, X. WANG, Y.T. LU, H.Y. XIN, C.A. POWELL, C. THUEMMLER, N.H. CHAVANNES, W. CHEN, L. WU, C.X. BAI, *Expert consensus on the metaverse in medicine*, in *Clin. eHealth*, 2022, 5, p. 1–9.

<sup>59</sup> B. MESKO, *The promise of the metaverse in cardiovascular health*, in *Enr. Heart J.*, 2022, eha231.

<sup>60</sup> A. CERASA, A. GAGGIOLI, G. PIOGGIA, G. RIVA, *Metaverse in Mental Health: The Beginning of a Long History*, in *Curr Psychiatry Rep.*, 2024 Jun;26(6):294-303. doi: 10.1007/s11920-024-01501-8]

<sup>61</sup> R.S. CALABRÒ, A. CERASA, I. CIANCARELLI, L. PIGNOLO, P. TONIN, M. IOSA, G. MORONE, *The Arrival of the Metaverse in Neurorehabilitation: Fact, Fake or Vision?*, in *Biomedicine*. 2022 Oct 17;10(10):2602. doi: 10.3390/biomedicine10102602

*Justice and accessibility*

The availability of technologies can create disparities in accessing equitable healthcare. While MedVerse can make mental health services more accessible to some, it may also exclude those who lack the necessary technology and the skills to use it in compliance with the LawVerse legal framework. To prevent digital exclusion, healthcare practitioners need to address at least the basic legal rules and work towards solutions that make virtual health services accessible to all, ensuring that everyone can benefit from digital innovation.

*Professional competence in virtual worlds*

Practitioners have a responsibility to stay competent in their field, which now involves understanding the emerging technologies and approaches behind MedVerse. This includes not only being informed about VR and its applications in healthcare, but also about the LawVerse: the legal, ethical, and social implications of these technologies must be part of our actual educational programmes, by engaging in continuous interdisciplinary education and training on these evolving technologies, participating in professional development opportunities specifically focused on virtual health law and ethics, collaborating with interdisciplinary teams to ensure comprehensive care, and seek consultation or supervision when needed to enhance competencies in MedVerse. As the legal landscape continues to evolve with technology, practitioners must also stay informed about new laws and regulations governing virtual spaces and the provision of mental health services within them. This involves understanding legal challenges and regulatory requirements when practicing across state or national boundaries.

*Autonomy and transparency*

The principle of autonomy should extend to interactions within the MedVerse. Practitioners must ensure that patients have control over their virtual experiences and that these technologies are used in ways that respect patient choices and privacy, including considerations around the design of virtual spaces and the extent to which patients can control their data and digital representations. On the other hand, fairness and transparency are crucial when discussing the potential and limitations of the MedVerse with patients. Practitioners should provide clear information about what patients can expect from virtual therapies, including any uncertainties or developing aspects of the technology.

*Ethical boundaries*

In immersive and game-like settings like the MedVerses, the lines between professional and personal interactions can become blurred, especially with the more casual and seemingly private nature of online communication. Maintaining the integrity of the therapeutic alliance in health treatment depends on preserving professional boundaries. These boundaries foster a safe space for exploration and are built on trust, respect, and the correct use of power. Therapists, and doctors, in general, must consistently nurture a professional relationship and refrain from actions that could be misunderstood or lead to boundary violations. From this respect, defining clear boundaries can help define the roles of both professional and patient for instance, in virtual therapy sessions, reinforcing professionalism and therapeutic goals for a clear and purposeful interaction.