Vulnerability in the Age of Metaverse and Protection of the Rights of Users Under EU Law

Shabahang Arian

A. Metaverse: new frontier of digital life

Generally speaking, the metaverse represents an online three-dimensional space where individuals engage and interact as digital avatars in much the same way as they do in the real world.[1] Matthew Ball in his book "The Metaverse" refers to this space as an immersive, shared digital reality environment that offers the potential for exploration and customization by users, identical to the experience and freedoms they enjoy in the physical world. This digital space provides enormous opportunities for socialization, entertainment, shopping, other augmented reality services, and a variety forms of digital content.[2] Despite the current limitations in technology and infrastructure, preventing the development of immersive virtual worlds anytime soon, researchers are diligently examining the metaverse's potential and its impact of this transformative digital change.[3]

Although the metaverse is a relatively emerging technological frontier, it is not merely a singular innovation. In fact, this technology is developed and supported by a variety of diverse cutting-edge technologies including Extended Reality (XR), 5G connectivity, artificial intelligence (AI), the

1 Matthew Ball, 'The Metaverse: What It Is, Where to Find It, Who Will Build It, and Fortnite' MatthewBall.vc, [September 15, 2021b.], https://www.matthewball.vc/all/themetaverse. Accessed Sep 21, 2023. See also, Gideon Burrows, 'Your Life in the Metaverse: Everything You Need to Know About the Virtual Internet of Tomorrow'. [2022] J. Kim, 'Advertising in the Metaverse: Research Agenda' [2021] Journal of Interactive Advertising, *21*(3), 141–144.

2 Matthew Ball, 'The Metaverse: And How it Will Revolutionize Evertything'[2022]. Matthew Ball, 'Framework For The Metaverse' [2021a.] https://www.matthewball.vc/all/ forwardtothemetaverseprimer. Accessed Sep 21, 2023.

3 Ereni Markos & Lauren Labrecque, 'Blurring the Boundaries Between Real and Virtual: Consumption Experiences and the Self Concept in the Virtual World' [2009] Advances in Consumer Research, 36, 884–885. See also: J Brannon Barhorst et al., 'Blending the Real World and the Virtual World: Exploring the Role of Flow in Augmented Reality Experiences' [2021] Journal of Business Research, 122: 423-436.

Internet of Things (IoT), blockchain, cloud and edge computing, and the vast reservoir of data which powers the metaverse's dynamic landscape.[4] Enhanced by other technologies, the virtual reality and augmented reality provide immersive experiences that blur the boundaries between reality and virtual space. In this multifaceted technological ecosystem, the avatars serve as a bridge between individuals and their virtual selves, acting as digital twins that represent and interact on behalf of users.[5] A fundamental building block of the metaverse lies in the array of enabling devices including Mixed Reality (MR) and Virtual Reality (VR) headsets, haptic feedback systems, and cutting-edge environment rendering devices which through them, users can engage with and navigate these virtual spaces.[6] Real-time interactions between multiple users in virtual environments requires the use and adoption of these devices to both capture real-world objects and transmit the data.[7]

Moreover, the virtual-reality environments offer an unparalleled richness compared to traditional 2D media. This richness extends beyond mere social cues in the forms of text and audio message but also encompassing multidimensional visual elements and haptic sensations.[8] To fully immerse in the VR/AR experience, users must rely on specialized equipment, such as virtual reality headsets or wearable haptic gloves. For instance, Apple Vision Pro, Apple's latest innovation, is a wearable face computer that without any keyboard, mouse or touch, delivers the high-resolution displays directly to the user's eyes through eye tracking and gestures.[9] Another facet of this technological revolution is the use of VR haptic gloves which enable

4 Lik-Hang Lee et al., 'All One Needs to Know About Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda' [2021a]. https://doi.org/10.48550/ arXiv.2110.05352

5 Yogesh K. Dwivedi et al., 'Metaverse Beyond the Hype: Multidisciplinary Perspectives on Emerging Challenges, Opportunities, and Agenda for Research, Practice and Policy' [2022] International Journal of Information Management, 66, Article 102542.

6 Yassine Jadil, Nripendra Rana, & Yogesh Kumar Dwivedi, 'A Meta-Analysis of the UTAUT Model in the Mobile Banking Literature: The Moderating Role of Sample Size and Culture' [2021] Journal of Business Research, 132, 354–372.

7 Intel., 'Powering the Metaverse' [2021] https://www.intel.com/conten t/www/us/en/newsroom/opinion/powering-metaverse.html. Accessed Sep 21, 2023

8 Ralph Schroeder 'Social Interaction in Virtual Environments: Key Issues, Common Themes, and A Framework for Research'. In Ralph Schroeder (Ed.), 'The Social Life of Avatars' [Springer 2002]1-18.

9 Joshua Gans & Abhishek Nagaraj, 'What is Apple's Vision Pro Really For?' [2023] Harvard Business Review.https://hbr.org/2023/06/what-is-apples-vision-pro-really-for. Accessed Sep 21, 2023.

users to interact with virtual objects and surfaces in a natural and realistic manner. These gloves can effectively track the user's hand movements and can apply forces, textures, and even thermal cues to the user's skin.[10] In particular, the Emerge Wave-1 device, developed by a California-based tech company, facilitates the sense of touch in the metaverse and fosters emotional connections among metaverse participants.[11] This tabletop panel uses ultrasound waves to map virtual objects that they can see through virtual headsets and convert this into the feeling of touch through a technology called haptic feedback in order to provide a more realistic experience.[12] In this next-generation digital frontier, traditional forms of interaction, such as typing and tapping, are being replaced by a variety of sensory devices. With the use of headsets and a variety of sensory gadgets, users can constantly communicate with their friends and family.

These AR and VR technological advancements suggest that the metaverse is no longer a science fiction concept but rather is on the verge of becoming an integral part of digital experience. Thus, it is therefore expected that in the near future, the Metaverse will serve as a convergence point between the physical and digital worlds, allowing users to seamlessly navigate between the two, for a variety of purposes such as work, education and training, health care, exploration of personal interests, and vibrant social interactions.[13]Due to an embodied Internet, the metaverse offers a digital space in which users can experience an enhanced sense of presence and a new dimension of online interaction, more similar to real-life experiences.[14]

With its novel, unprecedented sensory experiences, this technology will transform the engagement in digital sphere in a radical way. As a result of this expansive technological domain, every aspect of our lives, including the services we engage with, and the information and content we access

10 Qi, Jiaming et al., 'HaptGlove—Untethered Pneumatic Glove for Multimode Haptic Feedback in Reality–Virtuality Continuum' [2023] Advanced Science. 10.1002/advs.202301044.

11 Emerge Wave 1. https://emerge.io/ Accessed Sep 21, 2023.

12 Victoria Masterson, 'Feel the Metaverse with Your Bare Hands- Using Ultrasonic Waves' [2022] https://www.weforum.org/agenda/2022/05/metaverse-vr-ultrasonic-tech-emerge/ Accessed Sep 21, 2023.

13 Dimitrios Buhalis, Daniel Leung, Michael Lin, 'Metaverse as a Disruptive Technology Revolutionising Tourism Management and Marketing' [2023], Tourism Management, Vol. 97, 104724.

14 Nick Clegg, 'Making the Metaverse: What It Is, How It Will Be Built, and Why It Matters' [2022] https://nickclegg.medium.com/making-the-metaverse-what-it-is-how-it-will-be-built-and-why-it-matters-3710f7570b04. Accessed Sep 21, 2023.

to, can be intricately mediated by this new digital space. This emerging technology has also a profound impact on our social connection, how we interact with others, the friendships we form, and the new digital manners that we engage in the social interactions.

Once fully built, this emerging digital space will have a legal impact on rights of users. with the range of cutting-edge technological capabilities, the metaverse holds the potential to create new opportunities for both present and future societies but it can also introduce contradictions and vulnerabilities, resulting in unanticipated risks, challenges and backlash. Thus, the Metaverse, like any other technological advancements, while improves our digital experiences, it also exposes consumers to new forms of vulnerability. A lack of engagement with regard to addressing the risks posed by the Metaverse exacerbates the scale of the challenges, vulnerabilities, and abuses arising from this emerging digital interaction. Therefore, it is crucial to address the potential risks and vulnerabilities that users may encounter as a result of interacting in the metaverse and to safeguard the rights of users at this early stage of Metaverse development.

B. Metaverse can change marketing and online shopping experience

As the Metaverse continues to evolve, provides marketers new opportunities for marketing and advertising. With users becoming increasingly engaged and spending more time in the metaverse, opportunities for brand promotion and consumer interactions in an entirely distinctive ways will be multiplying.

Research in the field of marketing indicates that various Extended Reality (XR) technologies, including virtual reality (VR), augmented reality (AR), and mixed reality (MR), hold substantial potential as effective marketing tools. These technologies create consumer experiences akin to physical stores.[15] Contrary to traditional online stores, in the metaverse, companies would have virtual stores instead of traditional websites where customers' avatars would be able to browse virtual shops, enjoy hyper-vir-

15 Mariano Alcaniz, Enrique Bigne, and Jaime Guixeres, 'Virtual Reality in Marketing: A Framework, Review, and Research Agenda' [2019] Frontiers in Psychology. Vol. 10. https://doi.org/10.3389/fpsyg.2019.01530. See also: Yogesh Kumar Dwivedi et al., 'Metaverse Marketing: How the Metaverse Will Shape the Future of Consumer Research and Practice[2023] Psychology & Marketing 40 (4), 750-776.

tual conversations with assistants, try on clothing or accessories, and purchase through virtual transactions. [16] Several retailers, such as Adidas, have already introduced features like Virtual Fitting Rooms (VFR), enabling consumers to "try on" clothing virtually before making online purchases in this shared space. The companies such as IKEA, for instance, has released an augmented reality catalog app, enabling customers to preview furniture in their homes before purchasing it.[17] Many global firms, including J.P. Morgan[18], luxury brands like Gucci and Ralph Lauren[19], and hotel groups like CitizenM and EV Hotel Corporation[20], have started investing in the Metaverse. They are establishing virtual branches, selling digital products, and even developing virtual hotels.

As a result, brands can open fully immersive virtual stores in the Metaverse, eroding physical boundaries and engaging a broad spectrum of audience on a global scale in highly compelling ways. The additional advantage of commerce in the metaverse can also be related to AI personalization. By utilizing AI algorithms to interpret user interactions, businesses in the metaverse can customize stores or products in real time in order to enhance the shopping experience of their customers. These immersive experiences have the potential to use data collected in virtual environments to tailor recommendations and offers to targeted consumers and create powerful emotional connections between consumers and brands.[21] As a result, it is

16 Miklos Savary, 'The Metaverse: TV if the Future?' [2008] *Harvard Business Review*, *86*(2), 30. Oliver James Scholten et al., 'Ethereum Crypto-Games: Mechanics, Prevalence and Gambling Similarities' [2019] CHI PLAY '19: Proceedings of the Annual Symposium on Computer-Human Interaction in Play, 379-389. Nannan Xi, & Juho Hamari, 'Shopping in Virtual Reality" A Literature Review and Future Agenda' [2021] Journal of Business Research, 134(1) 37–58.

17 Luke Soon, 'The Way of the Metaverse Enhance Human Experience' [2023], https://www.linkedin.com/pulse/way-metaverse-enhance-human-experience-luke-soon/?trk=pulse-article_more-articles_related-content-card . Accessed Sep 21, 2023.

18 Ron Shevlin, 'JPMorgan Opens a Bank Branch In The Metaverse' [2022], https://www.forbes.com/sites/ronshevlin/2022/02/16/jpmorgan-opens-a-bank-bra nch-in-the-metaverse-but-its-not-for-what-you-think-its-for/?sh=9e1cf2c158d3. Accessed Sep 21, 2023.

19 Queenie Wong, 'Shopping in the Metaverse Could Be More Fun Than You Think' [2022], https://www.cnet.com/tech/computing/features/shopping-in-the-metaverse-could-be-more-fun-than-you-think/. Accessed Sep 21, 2023.

20 Alicia Sheper & Will Speros, 'The Hotel Industry Enters the Metaverse' [2022]. https://hospitalitydesign.com/news/development-destinations/hotel-industry-nfts -metaverse/. Accessed Sep 21, 2023.

21 Ahmed Ismail, 'Virtual Shopping in The Metaverse: How Brand Engagement in Self-Concept Influence Brand Loyalty' [2023], 10.2139/ssrn.4494222.

more likely that consumers will engage with a brand when they perceive that it is aligned with their preferences.[22]

Moreover, the Metaverse enhances social interaction and togetherness, making it a key advantage for marketing. Human beings are inherently social, and the Metaverse provides a platform for shared experiences and social interactions. Joint consumption, spanning activities such as movie watching, gaming, event attendance, and shopping, is a multi-billion-dollar business, and the Metaverse aims to capture a significant share of this market.[23] Studies have shown that immersive virtual environments can enhance presence, enjoyment, realism, and synchrony among participants over time, offering numerous opportunities for interactive experiences like virtual events and product demonstrations.[24]

Consequently, as the Metaverse expands, there will be a profound shift in marketing in the metaverse as well, and therefore, digital advertising tools and techniques will undergo a fundamental transformation.[25] Metaverse marketing, in contrast to traditional advertising methods, is often perceived as non-intrusive, more interactive, and immersive, which can easily capture the attention of users and provide value to them. Two noteworthy marketing techniques are likely to play a significant role in marketing in the Metaverse:

I. Virtual product placement (VPPs)

There is a long history of product placement in cinema, exemplified by such iconic instances as Reese's Pieces in Steven Spielberg's 1982 masterpiece, "E.T. The Extra-Terrestrial".[26] The statistics indicate that this strategic

22 Shakeel Siddiqui & Darach Turley, 'Extending the Self in a Virtual World' [2022] in NA-Advances in Consumer Research. *Vol. 33* eds. Connie Pechmann and Linda Price, Duluth, MN: Association for Consumer Research, 647-648.

23 Thorsten Hennig-Thurau & Björn Ognibeni, 'Metaverse Marketing' [2022] NIM Marketing Intelligence Review. 14(2). 43-47.

24 Jeremy N. Bailenson et al., 'Transformed Social Interaction: Decoupling Representation from Behavior and Form in Collaborative Virtual Environments [2004] Presence Vol. 13(4), 428–441. https://doi.org/10.1162/1054746041944803.

25 Louis Rosenberg, 'Marketing in the Metaverse: A Fundamental Shift' [2022] https://futureofmarketinginstitute.com/marketing-in-the-metaverse-a-fundamental-shift/. Accessed Sep 21, 2023.

26 Charles Goldsmith 'Dubbing in Product Plugs: How "Spider-Man 2" made [2004] *Wall Street Journal*, B1.

collaboration not only contributed significantly to the movie's staggering $800 million box office earnings but also resulted in an increase of 85% in Reese's Pieces sales during the week immediately following the film's release. From a psychological perspective, the effectiveness of product placement and brand integration as non-traditional advertising methods lies in their ability to resonate with viewers on emotional, subconscious, and social validation levels.[27] These techniques are designed to exploit a natural inclination of human brain that tends to respond subconsciously to specific stimuli. In this way, by implicitly inserting a product into a movie or television program as a passive actor, without mentioning characters, viewers are likely to experience positive emotions, such as happiness or relaxation, associated with the product. [28] Thus, product placement serves as an effective marketing tool and increases the likelihood of the viewer purchasing the product in the future.[29]

In the Metaverse, advertisements will evolve into promotional elements and activities seamlessly integrated into immersive environments on behalf of sponsoring brands. These VPPs will be precisely tailored to individual users, ensuring that they encounter these promotional artifacts at specific moments and locations that are most relevant to them. The authenticity and seamlessness of VPPs within immersive worlds have the potential to deliver impactful advertising experiences. However, there is a need for vigilant regulation to prevent the abuse of VPPs, as they may become indistinguishable from authentic experiences, potentially deceiving users.

In the metaverse, Virtual Product Placement (VPP) entails the injection of simulated products, services, or activities into immersive environments, whether they are virtual or augmented. This virtual product placement is on behalf of paying sponsors and strategically placed in a manner that makes them visible solely to a specific and targeted audience, closely tailored to the user's unique characteristics such as age, location, prefer-

27 Chelsea Collins, 'The Psychology of Product Placement and Brand Integration'[2023] https://blog.hollywoodbranded.com/the-psychology-of-product-placement-and-brand-integration#:~:text=The%20human%20brain%20is%20wired,commercial%20for%20the%20same%20brand. Accessed Sep 21, 2023.

28 T. Wasserman 'How to Measure Product Placement' [2005] Journal of Adweek. Vol. 46(3), 18-20.

29 Chelsea Collins, 'The Psychology of Product Placement and Brand Integration'[2023] https://blog.hollywoodbranded.com/the-psychology-of-product-placement-and-brand-integration#:~:text=The%20human%20brain%20is%20wired,commercial%20for%20the%20same%20brand. Accessed Sep 21, 2023.

ences, habits and profiles. This advertising method creates a compelling illusion, making the inserted elements appear as natural components of the immersive environment. [30] Nevertheless, as mentioned, this targeted VPP is unique to each user and is not replicated for others sharing the same surroundings. As such, this personalized advertising can sometimes blur the lines between what content is authentic within the metaverse and what constitutes simulated objects, artifacts, or content, potentially leading to user confusion.

II. Virtual spokes people (VSPs)

An alternative approach for marketing and advertising in the metaverse is known as Virtual Spokespeople, or VSPs. In this method, interactive AI-driven avatars as conduits for conveying persuasive promotional content are employed to discreetly encourage users to consider and purchase specific products promoted by these AI avatars on behalf of sponsor brands. These AI-powered conversational agents equipped with a profound understanding of users' beliefs, interests, and behavioral patterns, enable to deliver persuasive messages fit with the users interests and aspirations.The presentation and demeanor of these AI-driven avatars are meticulously tailored by advanced AI algorithms, geared toward optimizing their impact on each individual user. Recent breakthroughs in Large Language Models (LLMs) and photorealistic avatars have rendered VSPs a viable and potentially pervasive tool within the metaverse.[31]

VSPs engage users through two distinct modes of interaction: passive observation and direct engagement. In the direct engagement approach, users directly interact with these AI-driven characters, engaging in dynamic conversations. Conversely, the passive method strategically positions two simulated spoken avatars in close proximity to users engrossed in conversation. During this exchange, the characters subtly introduce and discuss the sponsored brand, allowing users to overhear the discourse.[32] This

30 Louis Rosenberg, 'Marketing in the Metaverse: A Fundamental Shift' [2022] https://futureofmarketinginstitute.com/marketing-in-the-metaverse-a-fundamental-shift/ Accessed Sep 21, 2023.

31 Ibid.

32 Louis Rosenberg, 'The Metaverse Will Be Filled with Elves' TechCrunc 2022.https://techcrunch.com/2022/01/12/the- metaverse-will-be-filled-with-elves/ Accessed Sep 21, 2023.

advertising strategy leaves users pondering whether these individuals are ordinary users or virtual characters, adding an element of uncertainty to the metaverse experience artifacts, or content, potentially leading to users confusion.

C. Persuasion vs manipulation in the metaverse

Picture this scenario: A targeted user strolls down a virtual or augmented street filled with avatars and other objects. Suddenly, an avatar bearing a striking resemblance to his favorite celebrity approaches him while casually wearing a hoodie from the user's favorite brand. The link on the screen immediately appears which encourages the user to click on the hoodie and place the order.

Further along the path, two avatars engage in a conversation about the unique features of a brand-new laptop, prominently mentioning the specific brand. The user had recently been browsing the internet in order to obtain information regarding the purchase of a new laptop. AI-generated avatars are exclusively intended to target the user's attention and centered the conversation around his taste and preference. These avatars appear only on the user display and are hidden from the view of other participants. Different prices and products are also offered to different users in the same environment.

The user finds themselves perplexed, unable to distinguish which objects are authentic and which are AI-generated sopkespeople who are solely present for advertising purposes. The avatars engaging in conversation are equipped with real facial expressions and natural eye movements which makes it even more difficult to discern which is a real avatar and which is AI promotional avatars. Through AI and IoT technologies, the virtual space enhances the user's sensory experience by playing his favorite song in the background. The music playing happens to be a track from the user's favorite singer, a tune he had recently played. In this intricate web of experiences, determining whether a piece of content is promotional or non-promotional become a difficult task.

These examples illustrate the practice of nudging, in which subtle and even misleading tactics are employed to subliminally influence users' actions, primarily by targeting their "shallow cognitive processes", without

providing them with alternative choices.[33] There is the persuasive design business model which encourages the designers and developers to use all interfaces and tools of technology sometimes even at the developmental stage to nudge consumers in order to maximize their profits. Therefore, the design features and the choice architecture encourage users to follow certain path or "alters people's behaviour in a predictable way without forbidding any options or significantly changing their economic incentives." [34] In these situations, the companies self-consciously persuade users to change behaviors, make certain choices or take actions. By collecting data from users and employing sophisticated algorithms for analyzing the data, the emerging technologies now possess the ability to influence and persuade users more autonomously and strongly. As such, these technologies are often referred to as persuasive technologies. For instance, computers, originally designed for calculations, storage, and retrieval, have gradually evolved to include persuasive elements in their design. [35] Consequently, Captology (Computers as Persuasive Technologies) will be used by companies as a deliberate technique in the metaverse for the purpose of persuasion. This term refers to a set of methods and techniques used by companies to change consumer attitudes and behaviors as a result of their use of technological tools. As such, all technological tools and interfaces should be designed so that they encourage people to purchase particular products or subscribe to special wellness programs.[36]

The synergy of Artificial Intelligence (AI) and the Internet of Things (IoT) offers marketers a valuable tool set for comprehending customer behaviors and preferences. This knowledge can be leveraged to craft personalized and highly effective strategies within the metaverse for nudge practices and personalized marketing. [37] As a result of the introduction of marketing automation, facilitated by AI, marketers are able to increase

33 Paul Kuyer & Bert Gordijn, 'Nudge in Perspective: A Systematic Literature Review on The Ethical Issues with Nudging' [2023] Rationality and Society, *35*(2), 191–230, 192.

34 Richard Thaler & Cass R. Sunstein, 'Nudge: Improving Decisions About Health, Wealth and Happiness' [2008] Yale University Press, 6.

35 Brian Jeffrey Fogg, 'Persuasive Technology: Using Computers to Change What We Think and Do' [2003] Morgan Kaufmann Publishers, 1.

36 Ibid. 16-17.

37 Bharati Rathore, 'Virtual Consumerism an Exploration of E-Commerce in the Metaverse' [2017] International Journal of New Media Studies, 4(2), 61-69. Michael Rüßmann e al., 'Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries' [2015] Boston Consulting Group, 9.

precision and the effectiveness of their advertisements with less manual intervention. Nevertheless, this business model sometimes goes beyond personalization, and AI is poised to propel hyper-personalization, not only by suggesting purchases based on historical behaviors but by foreseeing needs before customers themselves consciously recognize them.[38]

D. Layers of vulnerability in the metaverse

Nonetheless, these persuasive techniques can potentially give rise to novel forms of deceptive strategies and manipulation within the metaverse. The metaverse heavily relies on artificial intelligence (AI) for various functions, including content creation, content analysis, data analysis, AI-driven voice navigation, speech processing, and overall social interactions involving computer vision.[39] As a result of the interaction with virtual or augmented reality environments, consumers will face different dimensions of vulnerability.

The primary vulnerability of consumers lies in the fact that the metaverse confuses users as to whether they are interacting with AI-driven avatars or authentic individuals. In general, businesses can utilize a variety of manipulation techniques to persuade consumers in 3D immersive spaces, compared to traditional 2D online marketing. Further, with the recent advancements in Conversational AI, exemplified by systems such as ChatGPT and LaMDA, it is likely that these conversational AI agents to be deployed in the metaverse in the near future. A key purpose of these AI interactive agents is to engage the target audience in a real-time dialog with predatory agents that can skillfully persuade them to purchase particular products or trick them into disclosing sensitive personal information. This can become even more deceptive when the industry uses simulated avatars with real-time voice and photorealistic digital personas that see, move, and express like real individuals, while in reality, they are controlled by AI.[40]

38 Louis Rosenberg, 'The Manipulation Problem: Conversational AI as a Threat to Epistemic Agency' [2023] Conference: Generative AI and HCI Workshop CHI 2023 (GenAICHI 2023).

39 Uptal Chakraborty, 'Metaverse and Web3: A Beginner's Guide: A Digital Space' [2022] BPB Publications.

40 Louis Rosenberg, 'The Manipulation Problem: Conversational AI as a Threat to Epistemic Agency' [2023]. Conference: Generative AI and HCI Workshop CHI 2023

The second reason for the high level of vulnerability of consumers in the metaverse is related to large quantities of detailed information about the users that will be exposed during their interactions in the metaverse. In fact, the convergence of Artificial Intelligence (AI) and the Internet of Things (IoT) plays a pivotal role in shaping the metaverse. As a result of the IoT's vast network of sensors and devices, companies are able to collect a wide range of metaverse data and meta-data in real-time. For example, a smart device installed in a home or store can be used to systematically monitor customer usage patterns, enabling businesses to fine-tune their services to meet the specific needs of each customer. As mentioned previously, there are numerous research prospects for enhancing sensory input within virtual worlds. To improve real-life experience by users, there is a need for enhancing visual, auditory, and tactile feedback in the metaverse, especially concerning avatar interactions and communication. The VR AR virtual interaction requires the use of many sensory technology equipment such as VR AR glasses, gloves, or other sensory devices beyond standard computing devices such as headphones, in order to create and experience senses including a sense of touching of virtual elements in the metaverse.[41]

As a result, the metaverse, along with its accompanying technological sensory tools, significantly increases the companies' ability to collect and analyze large amounts of behavioral, demographic, and biometric data from consumers for profiling and ultimately deploying these data for highly persuasive techniques tailored to each individual in a very personalized manner.

The collected data including the facial expressions, vocal inflections, avatars emotional reactions can algorithmically craft personalised advertising for each user, and trigger specific thoughts, feelings or interests in targeted user. Furthermore, large amounts of data generated in the metaverse can exploit the vulnerabilities of individuals, and companies exploit the vulnerabilities of consumers to maximize their profits. Therefore, the massive collection of data use to exploit people's interests and vulnerabilities particularly for purpose of marketing and targeting ads and selling more products and services.

(GenAICHI 2023). See also: Louis Rosenberg, 'The Metaverse Will Be Filled with Elves' TechCrunc 2022.

41 John Davis N. Dionisio, William G. Burns III & Richard Gilbert, '3D Virtual Worlds And The Metaverse: Current Status And Future Possibilities' [2013] ACM Computing Surveys 45, 3, Article 34, 38. DOI: http://dx.doi.org/10.1145/2480741.2480751, 34:15.

E. Protection of users in the metaverse under EU law

Nevertheless, the vulnerability of consumers should not be left unprotected. As a result, legal frameworks have been meticulously crafted so as to protect and uphold the rights of consumers in relation to the goods and services they receive. In order to establish a metaverse environment characterized by fairness and legal integrity, particularly within the marketing sphere, it is essential to meet the challenges inherent to this emerging digital landscape. In Europe, a number of robust and well-developed laws are in place to protect consumers against unfair business practices. These regulations cover a wide range of issues related to dark patterns, deceptive design, manipulative marketing tactics, invasions of privacy, unlawful data collection, exploitation of vulnerability through personalized marketing, and user's consent-related matters.

The purpose of this section is to shed light on the pivotal role that EU regulatory laws can play in preventing and mitigating unfair commercial practices and misconduct in the metaverse and analyze the legal dimensions of consumer vulnerability within this digital frontier. Accordingly, the article will investigate whether the existing EU legal frameworks can effectively tackle the challenges associated with the metaverse or if there remain regulatory voids that require further scrutiny, attention and resolution.

I. EU Data Protection Law and profiling

The emergence of metaverse technology will present a profound challenge concerning data and data protection. The metaverse relies heavily on technologies such as eye tracking, facial expression tracking, and emotional and behavioral monitoring, enabling extensive users surveillance. As a result, the metaverse, by its very nature, introduces novel categories of personal data, including facial expressions and avatars gestures and reactions, to data processing considerations[42] while simultaneously intensifying data gathering, especially concerning users' behavioral, emotional, biometric, and demographic aspects.

42 Leanne Mostert, 'Legal Issues in The Metaverse', Webber Wentzel. https://www.webberwentzel.com/News/Documents/2022/webber-wentzel-metaverse-part-1.pdf. Accessed 21 Sep 2023.

Metaverse service providers have inherent access to the actions, interactions, and communications of users through avatars in the metaverse. Companies may employ sophisticated advertising algorithms that are capable of monitoring personal characteristics in real-time. These traits include not only facial expressions, vocal inflections, and posture, but also physiological responses, such as heart rate and pupil dilation as well as emotional and psychological reactions often captured through wearable devices. This technological space significantly facilitates comprehensive consumer monitoring by companies, making it both easier and more feasible than ever before. This massive data collection enables companies to offer personalized communication[43] directly to the specific recipient[44] based on behavioral targeting and audience particular traits, hobbies, interests, behaviors, beliefs, intentions and shopping history, time of day, location, weather.[45]

In many instances, user data enables companies to offer different price ranges for the same product or service to specific groups of consumers based on their regions, age, affiliations, and more. Moreover, service providers and companies can monitor targeted consumers' browsing behaviors in the metaverse to determine if the user fits the "affluent customer" or "budget-conscious" profile. [46] Due to this, the information collected and inferred by behavioral tracking tools directly influences the prices.

Therefore, engaging in metaverse activities often involves the disclosure of substantial amount of personal data including what users do, see, say, feel and even touch in the metaverse.[47] It is clear that extensive data collection, coupled with emerging technologies such as IoT, AI, and machine learning has significantly elevated the metaverse's capacity for surveillance,

43 Alessandro Acquisti & Jens Grossklags, 'Privacy and Rationality in Individual Decision Making' [2005] IEEE Security and Privacy Magazine, 3(1), 26–33.

44 Sriram Kalyanaramanand & S. Shayam Sundar, 'The Psychological Appeal of Personalised Content in Web Portals: Does Customization Affect Attitudes and Behavior?' [2006] Journal of Communication, Vol. 56(1), 110-132.

45 Nadine Bol, et al., 'Understanding the Effects of Personalization as a Privacy Calculus: Analyzing Self- Disclosure Across Health, News, and Commerce Contexts' [2018] Journal of Computer-Mediated Communication, 23(6), 370–388.

46 Jakub Mikians et al., 'Detecting Price and Search Discrimination on the Internet' in HotNets Organizing Committee, Proceedings of the 11th ACM Workshop on Hot Topics in Networks (ACM 2012) 3-5.

47 Louis Rosenberg, 'Regulation of the Metaverse: A Roadmap' [2022] 6th International Conference on Virtual and Augmented Reality Simulations (ICVARS 2022), DOI: 10.1145/3546607.3546611.

data gathering, privacy intrusions, and potential risks of exploitation and manipulation.

Clearly, in contexts involving the collection and sharing of user data, the paramount concern is the protection of individuals from potential exploitation of their vulnerabilities. European law has firmly entrenched privacy as a fundamental right, initially within Article 8 of the European Convention on Human Rights (ECHR)[48] back in 1950. Subsequently, in 2000, this recognition was extended to Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFR)[49], with Article 8 of the CFR explicitly recognizing the right to personal data protection in the context of automatic processing, thus reinforcing this fundamental right.

Taking a significant step forward, the EU introduced the General Data Protection Regulation (GDPR) in 2016[50], to meet the ever-increasing demand for information privacy within digital spaces, catering to the privacy expectations of individuals and consumers. The GDPR applies comprehensively to all forms of personal data processing. Within this regulatory framework, individuals, as data subjects, are empowered with the right to exercise control over their data, which must be duly respected by data controllers and all involved in data processing.

Utilizing user profiles derived from a wide range of data, businesses can include the name of the target, his/her demographic information and his/her browsing behaviors to reach particular members of the target audience.[51] Such data gathering, with advancements in artificial intelligence technology, leads to the problems of business manipulation and algorithmic discrimination. Using algorithmic decision making, companies offer discriminatory pricing based on online monitoring and profiling users. That can be included consideration of certain benefits and awards or increased pricing based on age, or particular health information, or unique user need

48 Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms [1950]as amended by Protocols Nos. 11 and 14, ETS 5.

49 Charter of Fundamental Rights of European Union [2012] OJ C 326, 26.10.2012, 391–407.

50 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) [2019] OJ L119/1.

51 Edith G. Smit, Guda Van Noort, and Hilde Voorveld, 'Understanding Online Behavioural Advertising: User Knowledge, Privacy Concerns and Online Coping Behaviour in Europe' [2014] Computers in Human Behavior, Vol. 32, 15-22.

and demand. As an example, companies may offer discounts to young people or increase their prices for older people, or by obtaining health information about the user, the company may offer a higher price since a specific drug related to the user's health issue is scarce in the geographical region where the user lives.

The companies often claim that such information collection about users allows them to provide personalized offers, recommendations, advertising, sales, and promotions to consumers[52] based on their needs, interests, and preferences.[53] However, in many circumstances, in such targeted advertising and marketing, the line between persuasion and manipulation is blurred.[54]

Personalization, as defined in the academic literature, involves the strategic creation, modification, and adaptation of content and distribution to optimize the fit with personal characteristics, interests, preferences, communication styles, and behaviors. In the context of the metaverse, personalization occurs in the form of personalized advertising which is created for an individual using information gathered through the individual's behaviors in the metaverse.[55] As such, personalization is a dynamic process that involves the interaction between companies and their consumers, the collection and processing of data, as well as the delivery of marketing outcomes. [56]

Therefore, three core elements can be understood in personalization: 'personal data' and 'automated processing' leading to 'various personalized decisions and outcomes' based on users' personal information and AI predictions and decisions. In analyzing whether data collection and processing by service providers in the metaverse are legitimate under EU laws, it is

52 Joanna Strycharz et al., 'Contrasting Perspectives – Practitioner's Viewpoint on Personalised Marketing Communication' [2019] European Journal of Marketing, 53(4), 635–660.

53 Sophie C. Boerman, Sanne Kruikemeier, and Frederik J. Zuiderveen Borgesius, 'Online Behavioral Advertising: A Literature Review and Research Agenda' [2017] Journal of Advertising, Vol. 46 No. 3, 363-376.

54 Joanna Strycharz & Bram Duivenvoorde, 'The Exploitation of Vulnerability Through Personalized Marketing Communication: Are Consumers Protected? [2021] Internet Policy Review, 10(4). Also see: Sandra Wachter 'Affinity Profiling and Discrimination By Association in Online Behavioral Advertising'[2021] *Berkeley Technology Law Journal*, *35*(2).

55 Jari Vesanen and Mika Raulas, 'Building Bridges for Personalisation: A Process Model for Marketing' [2006] Journal of Interactive Marketing' Vol. 20 No. 1, 5-20.

56 Jari Vesanen, 'What is Personalization? A Conceptual Framework' [2007] European Journal of Marketing, 41(5/6), 409–418. doi:10.1108/03090560710737534.

essential to address the question of what constitutes "personal information" in the metaverse and to what extent, "the collection" and subsequent "automated processing" of user information is permitted by EU regulations and rules. The the General Data Protection Regulation (GDPR) may apply to the metaverse as long as the data subject often represented by the avatar operator is located within the territorial boundaries of the European Union (EU) when the data undergoes processing.

To truly grasp the implications, it is imperative to first comprehend the expansive definition of personal data as outlined in Article 4(1) of the GDPR. This definition encapsulates any information, irrespective of nationality or place of residence, that pertains to an identified or identifiable natural person. It encompasses both objective data, such as name or address, and subjective data, which includes any information that evaluates, influences, or shapes an individuals' economic and social status or behavioral patterns, or potentially affecting their rights and interests. [57]

Crucially, the threshold for identifying an individual as 'identified' or 'identifiable' hinges upon their distinctiveness within a group of persons. In other words, an individual must be distinguishable from all other members of that group. Various means can facilitate this identification, ranging from traditional identifiers like names, addresses to the modern tools of surveillance, including IP addresses and cookies. [58] Notably, in the metaverse, personal data encompasses a diverse spectrum of information, transcending the confines of conventional data categories. For instance, elements such as facial expressions, eye movements, avatar gestures, and movements, when identifying a person, become part of the personal data context. According to recital 26 GDPR, to identify a person in the metaverse, 'all reasonable means' likely to be employed by the controller or by any other party to identify the person. Therefore, while data protection laws typically rely on identifiers such as names, phone numbers, and email addresses, the metaverse expands the boundaries and pushes the scope of personal data beyond conventional definitions. [59] As such, the personal data in metaverse may extend to include granular and inferential data such as facial expres-

57 A29WP, Opinion 4/2007 on the concept of personal data [2007] No. 01248/07/EN – WP 136, 6-8.

58 Ibid. 15-16.

59 Patrick Breyer v Bundesrepublik Deutschland [2016] European Court of Justice. Case C-582/14 Judgment of 19 October 2016, ECLI:EU:C:2016:779.

sions, eye movements, and avatar gestures as personal information.[60] As a result, the GDPR may need to encompass novel categories of personal data arising from interactions within the metaverse, which may be subject to processing by companies and service providers.

The General Data Protection Regulation (GDPR) lays down a comprehensive framework governing the processing of personal data, including within the ever-evolving landscape of the metaverse. Central to this framework is Article 4(2) of the GDPR, which casts a broad definition of what constitutes 'processing'. Article 4(2) defines processing as "any operation or set of operations performed on personal data, whether or not by automated means". These operations encompass a broad spectrum, ranging from the initial collection and recording of data to its subsequent organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, alignment, combination, restriction, erasure, or even its ultimate destruction.[61]

Principles outlined in Article 5(1)(a) of the GDPR further delineate the essential requirements for processing personal data within the metaverse. The Article acknowledges that in order for data controllers to process data of data subject, such data processing must be carried out lawfully, fairly, and in a transparent manner. In addition, Article 6 of the GDPR that sheds light on what constitutes lawful processing, highlighting a variety of conditions that must be met. Data controllers are thus faced with the legal obligation to identify and establish valid legal bases justifying their data processing activities. These bases serve as the cornerstone upon which lawful data processing hinges. The options delineated in Article 6 include data subject consent, necessity for the performance of a contract, or legitimate interests pursued by the controller or a third party, as stipulated in Article 6(1)(a), 6(1)(b), and 6(1)(f) of the GDPR, respectively. Each of these legal bases carries its own implications and requirements, demanding meticulous consideration and compliance within the metaverse's digital space.

With regard to legitimate interests, as clarified by the European Court of Justice, a threefold assessment is required. First and foremost, the data

60 Leanne Mostert, 'Legal Issues in The Metaverse', Webber Wentzel. https://www.webberwentzel.com/News/Documents/2022/webber-wentzel-metaverse-part-1.pdf. Accessed 21 Sep 2023.

61 Richard Steppe, 'Online Price Discrimination and Personal Data: A General Data Protection Regulation Perspective' [2017] *Computer Law & Security Review*, *33*(6), 768–785.

controller must unequivocally demonstrate the genuine legitimate interest. Secondly, the specific data under consideration must be integral to the achievement of these interests, requiring a stringent focus on data minimization and relevance. Finally, the rights of the data subject must not be superseded by the interests pursued by the data controller, striking a balance between individual privacy and legitimate objectives of organizations.[62]

In scenarios involving contractual processing, such as interactions in the metaverse where users and service providers engage in contractual relationships, it is imperative that the scope of data collection remains tightly aligned with the essential data necessary for fulfilling the contract's intended purpose. If the data is being collected for monetization or additional services, this should be clearly stated by data controllers since it is firmly grounded in separate legal bases that require transparency and compliance with data protection laws. To foster transparency and safeguard user privacy, stringent limitations should be imposed on the retention of data by platform providers within the metaverse. personal data should only be stored for the minimal duration necessary to facilitate the virtual experiences. This curtailment serves to significantly diminish the capacity of providers to use users detailed profiles over time. In addition, the transition from physical access to virtual access has transformed data vulnerabilities, necessitating stringent safeguards against unauthorized access particularly with respect to online infrastructure such as cloud storage.[63]

The additional requirement that takes center stage as a critical pillar of data protection, is the concept of consent as expounded in Articles 4(11) and 7 of the GDPR. To meet GDPR standards, consent must be freely given and unambiguous, with a clear and specific focus on each processing operation. Data subjects must receive adequate information to make informed decisions regarding the use of their data. As such, the platform providers in the metaverse must be duty-bound to communicate comprehensively with the public about the nature of data tracking within their metaverse platforms, including the precise data types monitored and the durations for which they are retained. For instance, users engaging in virtual or augmented worlds should receive overt notifications if VR and

62 See A29WP, *Opinion 06/2014 on 'The Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC* (2014) No. 844/ 14/EN – WP 217, 33.

63 Benjamin Edwards, Steven Hofmeyr, Stephanie Forrest 'Hype and Heavy Tails: A Closer Look at Data Breaches' [2016] *J. Cybersecurity*, 2, 3-14.

AR devices capture biometric data, such as eye movements, gestures, gaze or information regarding health and emotional conditions.

Nevertheless, the metaverse, by its very nature, blurs the line between reality and simulation, resulting in a realm imbued with ambiguity and fluidity. Users may engage with avatar-based influencers, participate in sponsored events, or partake in various metaverse activities, all of which can involve the collection of personal data for advertising and communication purposes. To protect the rights of metaverse users, robust and transparent privacy standards should be implemented, offering individuals a genuine, clear, and meaningful choice regarding the processing of their data.

In addition, a notable challenge arises from the opacity of many consent forms and privacy policies. What holds greater importance, however, is ensuring that individuals within the metaverse are afforded a genuine and easily comprehensible choice, which allows them to fully understand the reasons behind and methods employed for processing their data, as well as who is responsible for processing those data.[64] Nonetheless, the issue of aligning consent forms with legal requirements continues to raise concerns, particularly with regard to the crucial element of transparency. Lengthy, complex, and unclear documents, exacerbated by integration of simulated and real worlds in the metaverse can lead to confusion and uncertainty of users, impeding their ability to make informed and voluntary choices. In addition to these concerns, there are also the deceptive design patterns known as "dark patterns" that are frequently employed by service providers to mislead users into granting consent or sharing more personal data than they intended. As a result, this violates principles such as fairness, data minimization, and transparency, and is contrary to the principle of data protection by design. [65]

Also, consent must be 'specific' necessitating that the processing purpose must be clearly specified. This aligns with the 'purpose limitation' principle stipulating that personal data should be collected for explicit and legitimate purposes, without further incompatible processing. This means the extent of processing included in the purpose must not be overly broad that data subjects cannot evaluate compliance with data protection laws or discern for what purpose exactly the data is collecting. Therefore, upholding these

64 F. Zuiderveen Borgesius et al.,'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation' [2017] *European Data Protection Law Review*, *3*(3), 353–368.

65 A29WP, *Opinion 15/2011 on the definition of consent* [2011] No. 01197/ 11/EN – WP 187.

standards ensures that data processing within the metaverse remains compliant, transparent, and respects the privacy rights of its diverse users.

As a result, price discrimination in the metaverse takes the form of personalized pricing which is rooted in online tracking and profiling consumers' behavior. According to Article 4(2) GDPR when companies use automated data processing to evaluate the economic status of individuals, this usage of algorithms for assessing the financial aspect of an individual falls within the scope of the profiling regulation. Profiling is classified as high-risk processing due to its potential impact on individuals' rights and invasion of privacy and confidentiality. Nevertheless, according to Article 22 of the GDPR the data subjects has the right to rectify data used for price discrimination and the right not to be subject to certain discriminatory pricing decisions. In such cases, the legal measures safeguard individuals' rights, allowing them to contest decisions, based solely on automated processing, including profiling.[66]

II. Manipulative business practice in the metaverse

In the burgeoning metaverse, users increasingly confront what are commonly referred to as 'dark patterns' within user interfaces. These manipulative tactics, often employed through conversational AI agents, pose unique threats to the agency of human users. Such practices deceive consumers by influencing their choices through deceptive design techniques, guiding them away from decisions that serve their best interests and instead aligning them with the commercial ends of companies. In order to personalize and persuade consumers for their products and services, firms frequently collect information about consumers' habits, preferences and interests through emerging technology. The metaverse introduces an additional level of vulnerability for consumers by offering a broad range of data for companies to gather and use for personalization and persuasion. While personalization offers advantages to both companies and consumers, it also harbors dangers. A dark design combined with an understanding of consumer vulnerability and emotional fragility may lead to misuse of this space by corporations. 'Persuasion profiling' is another method of abusing consumers, which involves companies identifying individual consumer mo-

66 F. Zuiderveen Borgesius & J. Poort, 'Online Price Discrimination and EU Data Privacy Law' [2017] *Journal of Consumer Policy*, *40*(3), 347–366.

tivations and interests and dynamically altering advertisements in real time to the consumer as a result.[67] In this way, firms can employ 'motivation analysis' by utilizing algorithms in order to take advantage of consumers' hidden vulnerabilities' in the decision-making process through exploitation of psychological and psychoanalytical methods.[68] In this way, companies leverage frailties and vulnerabilities for financial gain, adjusting prices for vulnerable demographics, exploiting local scarcities, or charging higher prices for consumers with specific health conditions. Consequently, data collected from users is leveraged against users by these companies, resulting in consumers' economic and privacy harm.[69]

Market manipulation is even more prevalent in the metaverse. As a result of the nature of metaverse, the line between the real and the simulated world can be blurred. In the metaverse, there are a number of manipulative tactics available in order to hiddenly shape one's choice architecture in order to influence his/her decisions without overtly coercing. By placing products within the environment or channel in which audiences interact, marketers can subliminally influence participants to purchase products. Alternatively by creating AI avatars customized to users' fantasies and aspirations and by triggering consumers' vulnerability and deceiving their perceptions, companies may influence consumers' choices and economic behavior. Dark pattern business marketing in the metaverse, therefore, may exert a covert influence on consumers' decision-making processes without their awareness. In 2019, the Council of Europe issued a Declaration on the Manipulative Capabilities of Algorithmic Processes, recognizing the growing capacity of contemporary machine learning tools "to predict choices" and "influence emotions and thoughts, and alter an anticipated course of action", sometimes in a subliminal manner. The potential dangers for democratic societies stemming from "employing such capacity to manipulate and control the manipulation not only economic choices, but also social and political behaviors" of individuals.[70] As a result of the integration

67 Maurits Kaptein and Dean Eckles, 'Selecting Effective Means to Any End: Futures and Ethics of Persuasion Profiling [2010], in Per Hasle at al. (eds), Persuasive Technology' Berlin Heidelberg: Springer, 82-93. Maurits Kaptein & Dean Eckles, Heterogeneity in the Effects of Online Persuasion, 26 J. INTERACTIVE MARKETING, [2012] 176, 176–88.

68 Ibid.

69 Ryan Calo, 'Digital Market Manipulation' [2014] 82 Geo. Wash. L. Rev. 995.

70 Declaration by the Committee of Ministers on the Manipulative Capabilities of Algorithmic Process, (13 Feb 2019).

of AI, machine learning, and IoT technologies into the metaverse, this space is highly susceptible to AI manipulation and deceptive design. Nevertheless, regulation provides consumers with the means to safeguard themselves from such business practices, and it oversees market activities in order to determine what constitutes manipulation and what constitutes persuasion.

In this regard, a number of EU laws have the potential to safeguard individuals against these predatory business practices and the extensive data collection and data-driven technology used for consumer surveillance and detailed profiles in order to predict consumer behaviors.

For instance, both the Digital Markets Act and the Digital Services Act both have tackled the issue of dark patterns. The recent proposal of the European Union, the Digital Services Act (2022), prohibits companies and service providers from employing dark patterns "to deceive or nudge" recipients of their services "via the structure, design, or functionalities of the online interface or part thereof".[71] (DSA, Recital 39). These practices are defined as actions that "materially distort or impair, either purposefully or in effect, the ability of service recipients to make autonomous and informed choices or decisions", infringing upon users' fundamental rights, including the right to informed consent and freedom of choice (DSA, Recital 67).

Furthermore, Article 5(b) of Directive 2005/29/EC on Unfair Commercial Practices (UCPD) introduces a set of novel criteria for evaluating whether a commercial communication and practice is fair or not. These criteria are designed to take into account the impact of digital asymmetry on consumer decision-making processes. According to this article, commercial practices that significantly distort or have the potential to distort the economic behavior of the average consumer are prohibited. In Gut Springenheide GmbH, the Court established a benchmark for defining "the average consumer", which was described as a person who is "reasonably well-informed and reasonably circumspect and observant".This approach also has been adopted by UCPD in recital 18 which refers to average consumer as a person "who is reasonably well-informed and reasonably observant and circumspect, taking into account social, cultural and linguistic factors as

71 Amendments adopted by the European parliament on 20 January 2022 on the Proposal For a Regulation of the European Parliament and the Council on Single Market For Digital Services (Digital Service Act) and amending Directive 2000/31/EC(COM (2020)0825- C9-0418/2020-2020.

interpreted by the Court of Justice". [72]Also, a materially distorted economic behavior of the consumer is defined by Article 2(e) of the UCPD as the use of commercial practices that substantially impair the consumer's ability to make informed decisions, leading the consumer "to make transactions that they would not otherwise have made". Accordingly, Article 5(4) of the UCPD expressly prohibits aggressive commercial practices as unfair. A commercial practice is considered aggressive if, within its specific context, taking into account all relevant features and circumstances, it significantly impairs or is likely to significantly impair the average consumer's freedom of choice or conduct concerning the product, thereby causing them, or likely to induce them, to make transactional decisions they would not otherwise have made (as defined in Article 8 of the UCPD)As a result, this provision prohibits certain aggressive pesuasive commercial practices in the metaverse, such as dark pattern design, setting and features that aggressively nudges consumers to click on the link for purchasing products or to subscribe the services.

Crucially, under Article 5(a) of the UCPD, businesses are held accountable for unfair marketing practices when they fail to meet "the requirements of professional diligence". This concept, in reference to Article 2(h) of the UCPD, denotes "the standard of specialized skill and care that traders are reasonably expected to exhibit toward consumers, commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity". This underscores that the assessment of the fairness or unfairness of business practices should be based not on how businesses "generally behave" but rather how they "ought to behave". [73]

The UCPD provides a comprehensive legal framework governing business practices that impact consumers' economic interests at various stages, from pre-contractual interactions through to post-contractual phases. The recent Commission notice on the interpretation and application of the UCPD reaffirms that the Directive encompasses dark patterns and dedicates a specific section (4.2.7) to elucidate how its pertinent provisions can be applied to data-driven business-to-consumer commercial practices. Moreover, it underscores that the UCPD can be effectively employed to challenge the fairness of such practices, including dark patterns, within the

72 Gut Springenheide and Tusky v Oberkreisdirektor des Kreises Steinfurt [1998] Case C-210/96, ECLI: EU:C:1998:369.

73 Federico Galli, 'AI and Consumer Manipulation: What is the Role of EU Fair Marketing Law?'[2020] 35-64.

context of business-to-consumer commercial relationships. This, of course, is in addition to other regulatory instruments, such as the GDPR, that also play a role in regulating these practices. [74]

It must additionally be mentioned that Article 5.2.2 of the AI Act recognizes that other manipulative or exploitative practices facilitated by AI systems that is not directly addresses in the Act, can be addressed through existing data protection, consumer protection, and digital service legislations, in order to safeguard individuals' against risks of AI systems including protecting the right of users to make informed choices and decisions.

In general, UCPD safeguards consumers from dark patterns and misleading business practices. This includes all forms of AI manipulation whether AI systems present information to the consumers. AI systems programmed in the metaverse can intentionally omit or conceal certain important information about products and services. Many dark patterns often involve false information that induces consumers to make decisions they would not otherwise make. Therefore, it is essential to take into account the metaverse environment, interface, and features when assessing the presentation of information. Article 6 of the UCPD safeguards consumers against misleading practices, including those containing false information that deceives or is likely to deceive the average consumer. This provision underscores the importance of how information is presented to consumers, particularly relevant in the context of dark patterns. Similarly, Article 7 addresses misleading omissions, which become pertinent when dark patterns are used to withhold information from consumers, compelling them to make specific transactional decisions. This often occurs in scenarios like cost-traps, where consumers are led to believe that a digital service requires a one-time payment, only to discover later that subsequent payments are necessary to continue using the service.[75] According to the Commission's notice, the concept of "professional diligence" encompasses essential principles such as "honest market practice," "good faith," and "good market practice. These principles underscore the normative values that are pertinent to a specific field of business activity. Consequently, when businesses are in the process of designing the interface through which they will engage with

74 BEUC, '"Dark Patterns" and The EU Consumer Law ACQUIS; Recommendations for Better Enforcement and reform [2022], https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf., 6. Accessed Sep 21, 2023.

75 Ibid.

consumers, it becomes imperative for them to adhere to these principles.[76] In practical terms, this means that traders must take measures to ensure that consumers are not misled or unduly influenced by a user interface that guides them towards making specific decisions without affording them the opportunity to fully comprehend the implications of those decisions. In essence, any manipulative practice that significantly distorts or is likely to distort the economic behavior of an average or vulnerable consumer could potentially run afoul of the trader's professional diligence requirement.

Therefore,in the context of the metaverse, instead of employing subtle strategies like using silent characters, the traders and marketers can utilize AI-driven avatars that are virtually indistinguishable from real humans by average consumers and engage users in promotional conversations or showcasing virtual products. The content they display cannot be identifiable as advertising or non-advertising material and the entire presentation in the metaverse deceive and confuse users. If such deceptive design and settings effectively nudge consumers' behaviors, leading them to enter transactions they would not have otherwise chosen and compromise consumers' free will and infringe upon their right to make informed choices and give consent, all of the mentioned practices in the metaverse constitute unfair commercial practice under the UCPD. In this context, such business practices fall under the category of dark patterns and are explicitly prohibited under EU laws. This prohibition aims to protect consumers from manipulative tactics that undermine their autonomy and ability to make informed decisions in the digital environment.

III. Children as vulnerable users in the metaverse

Children are among the potential users of metaverse platforms, and they require special protection due to their age and credulity in the new digital metaverse space.

Children's participation in gaming and exposure to advertising in metaverse environments necessitates careful regulation. Augmented Reality (AR) and Virtual Reality (VR) spaces can exacerbate the vulnerabilities of children. Article 5(3) of the Unfair Commercial Practices Directive

76 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. Commission notice Guidance on the Interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council Concerning Unfair Business-to-Consumer Commercial Practices in the Internal Market (2021), 127.

(UCPD) delineates an average vulnerable consumer as an individual particularly susceptible to specific practices or products due to mental or physical infirmity, age, or credulity. Consequently, robust measures must be implemented to shield children from targeted advertising designed to exploit their vulnerability. Moreover, the UCPD places an additional condition, stating that a commercial practice is unfair when the trader could reasonably be expected to foresee that the marketing practice might distort the economic behavior of the average vulnerable consumer. Courts generally consider a vulnerability reasonably foreseeable if the company engaged in the practice knew or should have known that it could negatively impact vulnerable users.

In this regard, data collection and advertising practices for children in metaverse spaces must adhere to a path of utmost clarity and transparency. Advertising content must be unambiguously distinguishable from non-advertising content, ensuring children can make informed distinctions. Strict prohibitions are imperative against manipulative techniques, such as in-game purchase inducements or privacy disclosures, facilitated through dark pattern designs or techniques. Article 5.2.2 of the AI Act, for example, prohibits AI practices that have a significant potential to manipulate individuals through subliminal techniques beyond their consciousness or exploit vulnerabilities in specific vulnerable groups, such as children or persons with disabilities, with the potential to cause psychological or physical harm.

Additionally, the extensive data collection within metaverse spaces, including personal information, raises profound concerns, especially concerning children. Studies have shown that children's awareness and understanding of data flows and processing are substantially influenced by the presence or absence of visual cues. Therefore, it is essential to provide clear cues to children regarding data collection and processing. The transition from our evolved cognitive systems, which rely on sensory cues for detecting threats in the physical environment, to online contexts where these cues are often absent or manipulated, can explain why privacy boundaries are different in the digital world. Unlike the physical world, where we can see, hear, or feel the presence of others, online environments lack these sensory cues, which makes it challenging to navigate privacy concerns.[77]

77 Kaiwen Sun, et al., 'They See You're a Girl If You Pick A Pink Robot With A Skirt: A Qualitative Study of How Children Conceptualize Data Processing and Digital Privacy Risks' In *Proceedings of the 2021 chi conference on human factors in computing systems* [2021], 1-34.

Therefore, any entity collecting, using, sharing, or storing children's data must adhere to and comply with the stringent GDPR Privacy Protection requirements related to children. Under GDPR, if an advertiser or operator collects, uses, or discloses personal information from children under 16, they must first obtain verifiable parental consent before taking any such actions. It must be noted that under the GDPR[78] , article 6(1a), the processing of data can be lawful when the data subject has been given the consent for processing his/her information. With respect to the children and adolescents, GDPR implies that the minors above the age of 16 have the option of giving consent to the processing of their personal data; however, children under this age must have parental consent (GDPR, Art. 8). For data privacy, therefore, GDPR requires operators to provide clear and easily understandable privacy notices regarding the children data collection, use, and disclosure practices. Privacy practices should be communicated in a transparent manner, and prominently displayed so that parents can easily access them. The GDPR states that processing of minors' personal data by means of automated processing[79] (Art. 4.4 GPR) and behavioral advertising must comply with Articles 13 and 14 of the GDPR, be informed by minors and their parents, and be transparent about the legal basis for processing. Accordign to Article 13, the data controllers are obliged to provide informaiton related to the identity and the contact details of the controller, the contact details of the data protection officer, the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; or the legitimate interests pursued by the controller or by a third party, the recipients or categories of recipients of the personal data, the period of storing the data, etc., to the data subject when the personal information is collected and processed.

In summary, due to their age and credulity, children require special protection within the new digital metaverse space. Regulations are needed to govern children's gaming, advertising, and data privacy, with a focus

78 Regulation 2016/679/EU 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 - GDPR) [2016] OJ L119/1.

79 The Council of Europe Guidelines on Artificial Intelligence and Data Protection [2019]. See also: Alessandro Mantelero, 'Personal Data for Decisional Purposes in the Age of Analytics: from an Individual to a Collective Dimension of Data Protection'[2016] 32 Comp. Law & Secur. Rev., 238 ff.

on transparency and safeguards to protect them from potential harm and manipulation.

F. Conclusions

In conclusion, the evolving digital landscape of the metaverse presents multifaceted challenges that demand continuous adaptation and cooperation between regulatory bodies, businesses, and technology providers. Ensuring fair business practices in the metaverse necessitates a comprehensive approach rooted in professional standards, good faith, and transparency. Subliminal advertising and manipulative tactics, such as dark patterns, undermine consumer trust and violate the right of users to make informed decisions.

The metaverse, is highly driven by sophisticated algorithms and extensive data collection. While personalization enhances user experiences and is valued by companies and consumers, it raises concerns about privacy invasion. Excessive data processing, fueled by big data, could lead to manipulative practices. In this complex terrain, the delicate balance between personalization and privacy must be maintained. Advanced advertising algorithms in the metaverse have reached a level where they can assess personal traits, including facial features, vocal inflictions, and even vital signs. This data profiling for advertising, if unregulated, risks exploiting users' profound personal information for the commercial interests of companies. While the General Data Protection Regulation (GDPR) has made significant progress in digital privacy, additional provisions may be needed to address emerging types of data and new methods of profiling in the metaverse. Stricter regulations are imperative to limit the scope and use of biometric, emotional and behavioral data for automated decision-making and profiling based on special personal data categories and minimizing the discriminatory effects.

In addition, in this digital space, distinguishing between manipulation and persuasion is paramount. The metaverse, driven by AI-powered nudging, poses significant risks. Marketers, utilizing AI- generated avatars for advertising, can subliminally connect products with consumers' fantasies and aspirations. A manipulation is often subtle, emotional, and involves subtly influencing decision-making without conscious awareness, usually for commercial purposes. Regulations must curtail manipulative practices that exploitation of consumer vulnerabilities, ensuring financial gains for

corporations do not occur through dark patterns and manipulative business practices especially with regard to new methods of Virtual Product Placement and Virtual SpokesPeople marketing.

In the metaverse, vulnerable users must be given special attention. Empowering and protecting vulnerable consumers, particularly children, against exploitative practices is essential. It is important for advertisers and operators to adhere to self-regulatory guidelines in order to engage young users responsibly. In summary, the metaverse relies heavily on advanced advertising algorithms and data collection techniques. Robust regulations are imperative to restrict the extensive data collection by companies and protect users from being exploited for promotional purposes. This includes avoiding subliminal advertising, clearly informing audiences of promotional content, and refraining from directly inciting purchases or nudging users toward transactions. Ongoing regulatory vigilance and technological adaptation are crucial to maintain fairness and legal standards for commercial practices in metaverse.