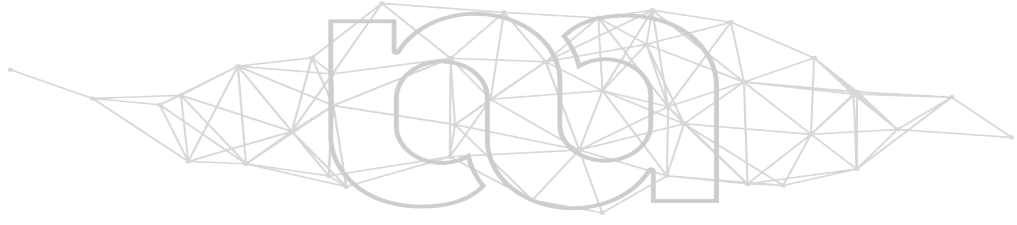
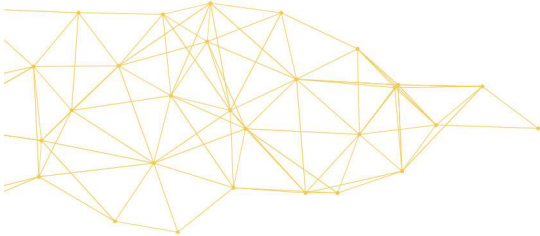


**Virtual worlds, real risks:
exploring user safety in the metaverse under
the Digital Services Act**

**Proceedings of the International Congress Towards a Responsible
Development of the Metaverse, 13-14 June 2024, Alicante**

Noémie Krack, Jean de Meyere
KU Leuven Centre for IT& IP Law



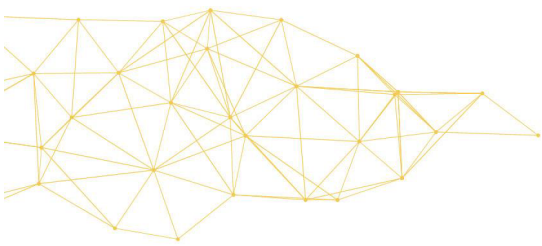
The Chair for the Responsible Development of the Metaverse (MetaverseUA Chair) was created by the University of Alicante (Spain) and financed by Meta Platforms under its [XR Program and Research Funds](#). The Program aims at supporting academic and independent research across Europe into metaverse issues and opportunities. The MetaverseUA Chair is a member of the [European Metaverse Research Network](#). Like all our work, this report has been produced completely independently. The ideas expressed in this paper are the sole responsibility of the author.

How to cite this paper:

Krack N., De Meyere J.. 'Virtual Worlds: Real Risks : Exploring user safety in the metaverse under the Digital Service Act' (2024) *Proceedings of the International Congress Towards a Responsible Development of the Metaverse*, Alicante, 13-14 June, 2024.

Funding acknowledgement:

The authors and their research received support from the European Union's Horizon 2020 research and innovation programme grant n° 951911- AI4Media and from Horizon research and innovation programme under grant agreements No 101135782- Manolo & n°101132449 i-Game.



Abstract

Recently, the British police launched its first investigation into a case of virtual "rape" in the metaverse. This paper delves into the complex considerations that user safety and content moderation could pose through the prism of the recently adopted Digital Services Act (DSA). We first explore the current state of platform operating metaverses. Metaverses are similar to current online platforms yet are differentiated by the use of XR technologies. Despite the low number of users on such platforms, specific issues related to the metaverse, such as the rise of disinformation or virtual sex crimes, have already been reported. This paper considers the following research questions: What legal challenges do specific metaverse platforms present in terms of user safety, and how does the DSA address these challenges? Attention will be brought to the impact of relevant obligations for user safety in metaverses. We continue our analysis by addressing the lack of risk assessment obligations for platform operating metaverses, as they currently do not meet the threshold to be bound by these obligations under the DSA. We conclude with recommendations for policymakers on how to tackle the challenges posed by increased risks in the metaverse.

Keywords: Virtual Worlds, Real Risks, Exploring User Safety in the Metaverse under the Digital Services Act

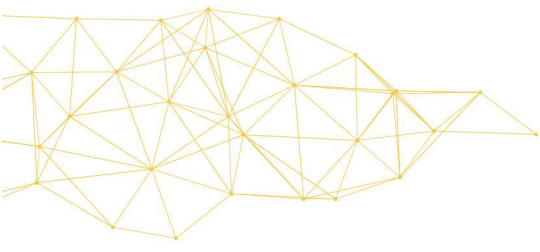


Table of Contents

1.Introduction	1
2.Virtual worlds and metaverse: what are we talking about?	1
2.1. Evolution: from Spielberg to Zuckerberg.....	1
2.2. Metaverse and virtual worlds?	2
2.3 Further classification of metaverses.....	6
2.4.Virtual safety, real harms	6
2.5 .Safety in EU policy and regulatory instruments on metaverses	10
2.6 . Content moderation in the metaverse: challenges and considerations	11
3.The Digital Services Act : regulating metaverses?	13
3.1. <i>Lex generalis</i> for content moderation and user safety	13
3.2. Provider of metaverses and the scope of the DSA	14
3.2.1. Dissemination to the public.....	15
3.2.2. Online platforms allowing contracts	16
3.2.3. Very Large Online Platforms and general metaverse	16
3.2.4. The DSA and metaverse(s): potential, yet many questions remain	16
3.3. Liability of metaverse providers in EU law	16
3.4. Metaverses as online platforms: obligations in the DSA.....	18
3.4.1 .Obligations applicable to all intermediary services.....	18
3.4.2. Obligations applicable to providers of hosting services and online platforms.....	19
3.4.3 . Obligations applicable to online platforms, to the exception of MSE.....	20
3.5. DSA, online platforms & virtual risks	21
3.6. Metaverse & DSA VLOPS regime.....	22
3.6.1. Systemic risks	23
3.6.2. Shortcomings	24
3.7. Towards a general metaverse and potential impact based on DSA' Scope	25
4. Recommendations for policymakers to address user safety challenges in the metaverse	25

1. Introduction

The emergence and development of the Metaverse come with a plethora of legal considerations; however, the most pressing issue appears to be content moderation and addressing the question of liabilities. This paper explores complex considerations of liability and accountability that such a case could pose through the prism of the recently adopted Digital Services Act (DSA). The newly enforced legislation aims to create a safer digital space where the fundamental rights of users are protected. This contribution assesses whether the new regulation fulfills its promises in the context of the metaverse.

While numerous challenges are associated with metaverse regulation, our analysis focuses on user safety on metaverse platforms through the lenses of the Digital Services Act exclusively. We also do not investigate specific questions such as the protection of minors online or the regulation of commercial transactions, or advertisement in the metaverse. Issues related to advertising are also out of the scope of this paper.

2. Virtual worlds and metaverse: what are we talking about?

2.1. Evolution: from Spielberg to Zuckerberg

The term Metaverse appears in the 1992 novel *'Snow Crash'* by Neal Stephenson. In his dystopian description of the 21st Century, Hiro, the hero of the story, can log into the metaverse, 'a computer-generated universe that his computer is drawing onto his goggles and pumping into his earphones'¹. The Metaverse is presented as an alternative online real virtuality that users can escape to, translating the physical world in the virtual environment.

Science-fiction continued developing on the concept of virtual reality and the Metaverse. In *Futurama*, characters are able to physically visit the Internet using 'net suits'. They are represented with avatars in the online environment that presents itself as a city, where each building represents a different online service². In 2018, Steven Spielberg also explores the concept of the Metaverse in *Ready Player One*. In the movie, individuals can escape a bleak dystopian future by joining 'The Oasis', an alternate virtual society by relying on VR helmets and haptic technology³.

Reality is never too far from fiction: on 3 June 2003 already, Linden Lab launched the public version of *Second Life*, announcing that they "pioneered real-time 3D streaming technologies and advanced compression capabilities to create a persistent, contiguous landscape where residents can discover a world of exploration, socializing, creativity, self-expression, and fun unlike any other."⁴. At the time, the term metaverse was not used by Linden Lab. Later, Linden Lab refers to *Second Life* as "the original metaverse"⁵.

Other platforms have then emerged which offers user the possibility of navigating a virtual world: video-games like Roblox, Minecraft or Fortnite are all worlds in which users control

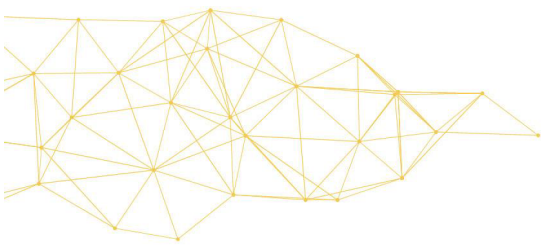
¹ Neal Stephenson, *Snow Crash* (Bragelonne 2009).

² 'A Bicyclops Built for Two', *Futurama* (19 March 2000).

³ *Ready Player One* (Directed by Steven Spielberg, Warner Bros, Amblin Entertainment, Village Roadshow Pictures 2018).

⁴ PRESS RELEASE: Your Second Life Begins Today. | Linden Lab' (20 March 2008) <https://web.archive.org/web/20080320014250/https://lindenlab.com/pressroom/releases/03_06_23> accessed 22 May 2024.

⁵ Linden Lab' <<https://lindenlab.com/press-release/original-metaverse-second-life-celebrates-20th-birthday>> accessed 22 May 2024.



an avatar that can evolve in a virtual environment together with a large number of other users⁶. In that sense, those virtual worlds have similarities with online platforms which allow users to produce and share content amongst themselves.

Yet, those different platforms are different from the Metaverse envisioned by Stephenson or Spielberg: users are able to control an avatar in a 3D-environment, but they are not themselves immersed in this environment – unlike Wade Watts in Ready Player One or Fry in Futurama. Such platforms can be considered as ‘proto-metaverses’⁷. They present themselves with similar objectives to those of virtual worlds. However, they lack some of the characteristics element to qualify as a virtual-world. For example, Second Life is solely accessible using a web browser. While it is a permanent, online 3D world, its lack of integration between virtual and real elements does not allow the service to meet the immersiveness criteria of virtual worlds. However, recently, the emergence of VR and XR technology opened the path for such developments.

In the end of 2021, Mark Zuckerberg showed its interest in pioneering the realm of virtual reality. Facebook changed its name to Meta and a large effort was put in developing ‘the metaverse’⁸. This was made possible with the acquisition back in 2014 of VR company Oculus, for approximately \$2 billion⁹. In 2021, Meta launched Horizon Quest¹⁰, an online application accessible through the Meta Quest VR-headsets. Meta presents Horizon Quest as the place to find ‘a community, games, events or everything in between’¹¹. In 2023, Meta abandoned the purely VR-based approach to Horizon Quest, by allowing users to join the virtual world through their phone or web browsers¹².

2.2. Metaverse and virtual worlds?

Throughout this time, various definitions emerged, trying to define technological characteristics for the metaverse and/or virtual worlds. While recent work from the European Commission shows both terms are interchangeable¹³, the Commission Staff

⁶ ‘Roblox, Fortnite, Minecraft... : ces projets de Metaverse auxquels va se frotter l’ex-Facebook’ (*Les Echos*, 30 October 2021) <<https://www.lesechos.fr/tech-medias/hightech/roblox-fortnite-minecraft-ces-projets-de-metaverse-auxquels-va-se-frotter-lex-facebook-1359837>> accessed 31 May 2024.

⁷ Emmie Hine, ‘Content Moderation in the Metaverse Could Be a New Frontier to Attack Freedom of Expression’ (2023) 36 *Philosophy & Technology* 43.

⁸ Mike Isaac, ‘Facebook Renames Itself Meta’ *The New York Times* (28 October 2021) <<https://www.nytimes.com/2021/10/28/technology/facebook-meta-name-change.html>> accessed 22 May 2024.

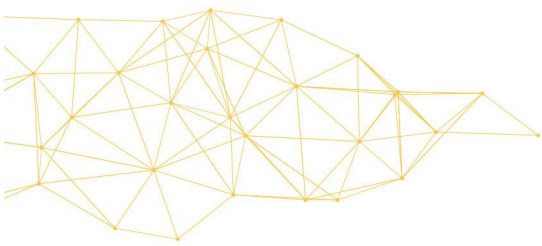
⁹ ‘Facebook to Acquire Oculus’ (*Meta*, 25 March 2014) <<https://about.fb.com/news/2014/03/facebook-to-acquire-oculus/>> accessed 22 May 2024.

¹⁰ Amandine Jonniaux, ‘Horizon Worlds : Meta lance son monde en réalité virtuelle’ (*Journal du Geek*, 13 December 2021) <<https://www.journaldugeek.com/2021/12/13/horizon-worlds-meta-lance-son-monde-en-realite-virtuelle/>> accessed 22 May 2024.

¹¹ ‘Meta Horizon Worlds sur Meta Quest’ (*Oculus*) <<https://www.meta.com/experiences/quest/2532035600194083/>> accessed 22 May 2024.

¹² ‘Meta Horizon Worlds Begins Expansion to Mobile and Web | Blog Meta Quest’ <<https://www.meta.com/fr-fr/blog/quest/horizon-worlds-web-mobile-social-vr-free/>> accessed 31 May 2024.

¹³ ‘Virtual Worlds Fit for People | Shaping Europe’s Digital Future’ (1 February 2024) <<https://digital-strategy.ec.europa.eu/en/policies/virtual-worlds>> accessed 31 May 2024.



Working Document related to the EU Initiative on Web 4.0 and virtual worlds¹⁴ provides a useful starting point.

The document defines **virtual worlds** as “**persistent, 3D, real-time, immersive environments that blur the line between real and virtual**, serving purposes such as socializing, working, learning, conducting transactions, playing, and creating.”¹⁵ From this definition, we can identify the following key characteristics of virtual worlds:

→ **Persistence**

Persistence in virtual worlds refers to the continuous and unbroken existence of the digital environment, regardless of whether users are actively engaged with it. This means that the virtual world and its contents, including objects, environments, and data, remain intact and operational even when users are offline¹⁶. For instance, changes made by a user, such as building structures or altering the environment, are preserved and will be visible when the user or others log back in. This persistence allows the creation of a consistent and reliable virtual experience, fostering a sense of continuity and stability¹⁷.

→ **Real-time interaction**

Real-time interaction allows users to communicate and engage with each other instantaneously, just as online¹⁸. This real-time communication can include text chat, voice calls, or even video conferencing, enabling a seamless and dynamic exchange of information. The ability to interact in real time enhances the social and collaborative aspects of virtual worlds, making them more engaging and lifelike. It supports activities ranging from casual conversations to complex collaborative projects.

→ **Immersiveness & 3D**

Immersiveness in virtual worlds is achieved through the deployment of various

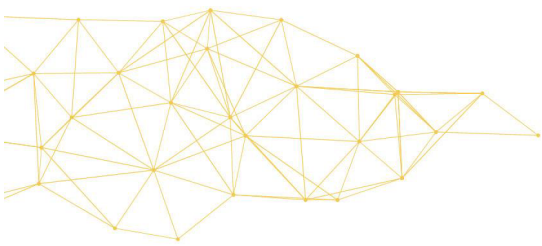
¹⁴ European Commission, Communication from the Commission to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition 2023 [COM(2023) 442/final].

¹⁵ *ibid.*

¹⁶ John David N Dionisio, William G Burns Iii and Richard Gilbert, ‘3D Virtual Worlds and the Metaverse: Current Status and Future Possibilities’ (2013) 45 ACM Computing Surveys 1.

¹⁷ Akbobek Abilkaiyrkyzy and others, ‘Metaverse Key Requirements and Platforms Survey’ (2023) 11 IEEE Access 117765.

¹⁸ ‘Integration of Sensing, Communication, and Computing for Metaverse: A Survey | ACM Computing Surveys’ <https://dl.acm.org/doi/full/10.1145/3659946?casa_token=I03Yt1MFGf4AAAAA%3AS4BUfIFV0b2M5G_Cpls46AzKXT3CXupUEtkDiuD9hWtia2T9m2VhBDMRO0gwWQBEDQ89ulAjXev6mA> accessed 31 May 2024.



technologies such as the Internet of Things (IoT)¹⁹ and extended reality (XR)²⁰. These technologies work together to create an environment that fully engages the user's senses, making them feel as though they are truly part of the virtual space. IoT can bring real-world data and interactivity into the virtual environment, while XR technologies, including virtual reality (VR) and augmented reality (AR), provide more tangible and engaging experience. Immersiveness is key to making the virtual world feel real and captivating, drawing users into the experience.

The use of technology to create three-dimensional environments is an important aspect allowing users to immerse themselves in the virtual world. These 3D worlds can be generated through various means, including the integration of Internet-of-Things (IoT) devices or the deployment of virtual avatars. IoT devices can enhance the virtual experience by providing real-world data and interactions, while virtual avatars allow users to navigate and interact within these 3D spaces, adding depth and realism to the virtual environment.

The integration of real and virtual elements is a significant feature of virtual worlds, blending physical and digital experiences. This integration can involve the incorporation of real-world data into the virtual environment, the use of augmented reality to overlay digital information onto the physical world, or the creation of hybrid spaces where virtual and real elements coexist. Integration of real and virtual elements reinforces the realism of virtual worlds.

The **Metaverse** is then defined as an “interoperable network of virtual worlds.”. This seems in line with other definition and literature on the metaverse, which describes four major characteristics for the Metaverse²¹, which serves as the next step in the evolution of the Internet from a merely virtual realm to an extended and augmented reality: realism, ubiquity, interoperability and scalability.

To be realistic, the Metaverse should allow ‘users to feel psychologically and emotionally immersed in the alternative realm²² by comprising a virtual world allowing their users to immerse themselves in the online environment. The Metaverse should be ubiquitous, meaning that users can access it through all their devices and that their virtual avatars seamlessly travel across virtual worlds. Interoperability refers to the use of standards allowing different implementations to render virtual worlds in a similar fashion that allow users to navigate across them with no hindrance of their virtual immersion. Finally, scalability means that the server architecture behind the Metaverse allows the presence of a massive number of users simultaneously²³.

The Metaverse in that sense currently does not exist. Rather, several providers such as Meta or LindenLab offer virtual worlds that are accessible to their users. As they

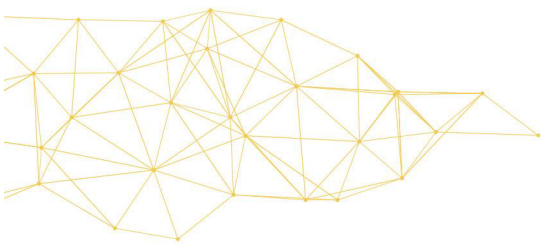
¹⁹ Md Ariful Islam Mozumder and others, ‘Overview: Technology Roadmap of the Future Trend of Metaverse Based on IoT, Blockchain, AI Technique, and Medical Domain Metaverse Activity’, *2022 24th International Conference on Advanced Communication Technology (ICACT) (2022)* <https://ieeexplore.ieee.org/abstract/document/9728808?casa_token=LJ5-5XZjdRkAAAAA:-ZISqStm9HCH81T1Driv7r0Sp4o36wxJ3VU_jul-b7u1imdtMz-x3PEGao5e4loeX437xMoJFLM> accessed 31 May 2024.

²⁰ Lorenzo Cappannari and Antony Vitillo, ‘XR and Metaverse Software Platforms’ 135.

²¹ Dionisio, Iii and Gilbert (n 16).

²² *ibid.*

²³ *ibid.*



aggregate different virtual worlds, those services could qualify as (proto)-metaverses²⁴ under the definition of the EU Staff Working document. However, as they operate independently, they do not meet the above-described requirements of interoperability, ubiquity and scalability.

Our article does not, however, solely focus on the Metaverse as the next step in the development of the Internet, but on the current limitations of the European legislative framework regarding existing platforms. Therefore, it is important that we define and use terms that are relevant with this objective.

Given the absence of a clear common definition at the moment, we will use the term “metaverses” in this article to describe “one or more virtual worlds operated by one intermediary service”. This definition works best as this article focuses on user safety and the liability of online intermediaries. In the next section, we further describe the concept and introduce the notion of a ‘general Metaverse’ or ‘the Metaverse’ that would meet the conditions of realism, ubiquity, interoperability and scalability.

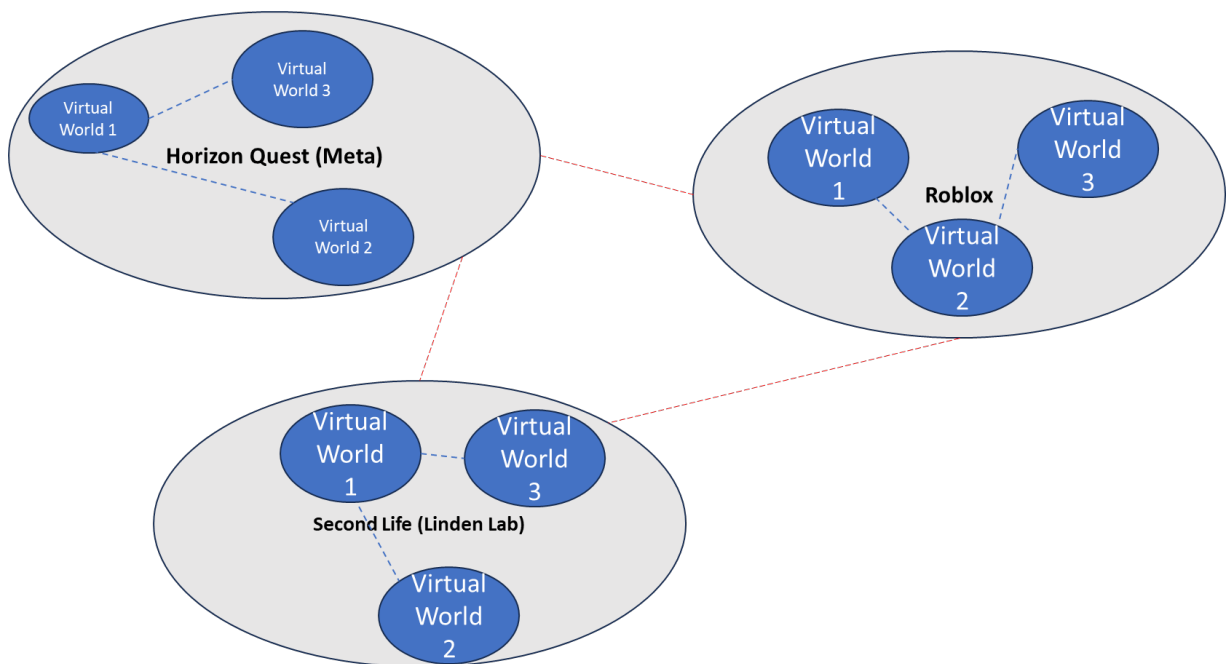
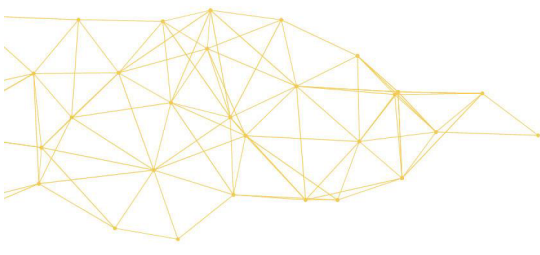


Figure 1: a schematic representation of the definition of virtual worlds, metaverses and the general Metaverse.

Metaverses (here, Horizon Quest, Second Life and Roblox) aggregate multiple virtual worlds and the user has the possibility to navigate between them, using an avatar. In red, a potential general Metaverse could be created by allowing users to travel through virtual worlds hosted by different service providers.

²⁴ We use the term proto-metaverse to designate virtual reality structures that do not rely on XR technology, such as Second Life.



2.3 Further classification of metaverses

Currently, various platforms offer services that can be considered (proto-)metaverses. Users on these platforms can only communicate with others on the same platform. In this configuration, a metaverse functions similarly to online platforms like Facebook or Reddit: users can interact and share within the platform but are confined to its architecture and ecosystem.

When different virtual worlds become interoperable and form a network, they create a metaverse—an interoperable network of virtual worlds. Typically, these services consist of a metaverse operated by a single entity. For example, Meta Horizon Worlds comprises various virtual worlds through which users can navigate. From the perspective of platform regulation and the Digital Services Act, regulation usually applies at this level.

To achieve the integration necessary for a fully unified Web 4.0, an additional step is required: the establishment of what we call a "general Metaverse", or more simple "the Metaverse". This potential general Metaverse would encompass most online users, enabling the creation and dissemination of physical content online by everyone. Although this concept is currently far from being realized, it could emerge from either the concentration of most users on a single platform or interoperability between various metaverse providers. While it would form the foundation of a new online experience, such interoperability would introduce additional liability and regulatory challenges.

2.4. Virtual safety, real harms

Metaverses are often praised as a revolutionary technology that can enhance human interaction and build connections. However, its success is strongly linked to the safety of the experience. Some users have reported that online abuse might drive them to quit a metaverse²⁵. A 2018 study found that among social VR users surveyed, 49% of women reported experiencing at least one instance of sexual harassment, 30% of men reported racist or homophobic comments, and 20% of men experienced violent comments or threats²⁶.

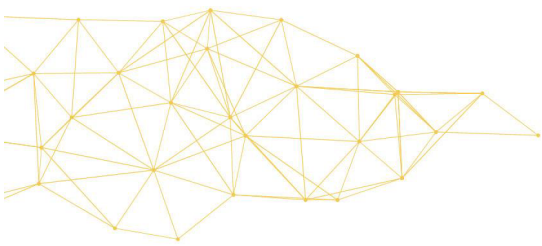
Our research on user safety and the Digital Service Act (hereafter DSA) was prompted by a case of alleged gang rape of a minor by a group of adult men in a metaverse in January 2024²⁷. Such virtual sexual abuse is not new. Already in the 90's, the case of a cyberspace rape depicted in the famous J. Dibbel paper²⁸ brought to light issues of online abuse pertaining to free speech and safety online. The paper already sparked debate on the repercussion of online events on real-life such as emotional effect similar to victims of

²⁵ Guo Freeman and others, 'Disturbing the Peace: Experiencing and Mitigating Emerging Harassment in Social Virtual Reality' (2022) 6 Proceedings of the ACM on Human-Computer Interaction 85:1.

²⁶ Jessica Oultaw, 'Virtual Harrassment: The Social Experience of 600+ Regular Virtual Reality (VR) Users' (*THE EXTENDED MIND*, 2018) <<https://www.extendedmind.io/the-extended-mind-blog/2018/04/04/2018-4-4-virtual-harrassment-the-social-experience-of-600-regular-virtual-reality-vrusers>> accessed 28 May 2024.

²⁷ Rebecca Camber, 'Police Launch the First Investigation into "Virtual Rape"' *Daily Mail Online* (1 January 2024) <<https://www.dailymail.co.uk/news/article-12917329/Police-launch-investigation-kind-virtual-rape-metaverse.html>> accessed 28 May 2024.

²⁸ Julian Dibbel, 'A Rape in Cyberspace. How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database Into a Society' (*The Village Voice*, 23 December 1993) <http://www.juliandibbell.com/texts/bungle_vv.html> accessed 27 May 2024.



physical rape. When it comes to metaverses, abuse is unfortunately frequent and already several sexual assaults have been reported on Horizon Worlds²⁹.

Defining safety, a core concept for success of metaverses, is challenging due to the nature of metaverses. Indeed, safety is a compound term used to refer to a multitude of considerations.

A key challenge for safety assessment is that **safety risks in metaverses can be wide-ranging**. Hine et al. in their paper "Safety and Privacy in Immersive Extended Reality: An Analysis and Policy" have explored immersive extended reality (IXR) safety threats and use a three-part definition of "safety" encompassing physical, mental, and social elements³⁰.

They categorized threats based on literature review including physical threats as either incidental (such as cybersickness) or intentional (for instance through the hack and manipulation of devices or virtual environment³¹)³².

Mental health threats can arise from interactions with other users (e.g. harassment, cyberstalking) or from the platforms and technologies used that can contribute or exacerbate psychological disorders based on unhealthy engagement and addiction³³. This raises critical questions about how to address situations where threats or offenses in metaverses put users at real-life risk. Such risks include manipulation, incitement to suicide, and the development of mental disorders³⁴.

Threats to social stability were further divided into threats to the social order (such as normalization of harassment or abusive behaviors), to security (metaverse used for extremist recruiting) and to democracy (Metaverse used as tool for spreading disinformation)³⁵. As demonstrated by this categorization, safety risks are numerous in metaverses. The European Union Agency for Law Enforcement Cooperation (Europol) also identifies the metaverse as a new playground for criminals, highlighting risks of identity theft, deepfakes, scams, money laundering, child abuse and exploitation,...³⁶

Another aspect directly connected to the wide range of safety threats is the wide range of Metaverse users: from children, gamers, businesses and professionals, to content creators, educators and so forth. All these different users require safety measures tailored to their needs and safety risks.

In addition to the wide range of safety threats and users, another component influencing safety is the **type of experience offered in metaverses**. For instance, safety risks will differ whether extended reality (XR) is experienced through virtual reality (VR),

²⁹ Harriet Marsden, 'Rape in the Metaverse: A Case for the Real-Life Police?' *The Week* (2 January 2024) <<https://theweek.com/crime/rape-metaverse-real-life-police-crime>> accessed 28 May 2024.

³⁰ Emmie Hine and others, 'Safety and Privacy in Immersive Extended Reality: An Analysis and Policy Recommendations' (27 September 2023) <<https://papers.ssrn.com/abstract=4585963>> accessed 22 May 2024.

³¹ Europol mentions the Chaperon Attack which alters the boundaries of a user's virtual world but also the overlay Attack where the attacker takes complete control over the user's virtual environment and provides their own overlay. Europol, 'Policing in the Metaverse: What Law Enforcement Needs to Know. An Observatory Report from the Europol Innovation Lab', (European Union Agency for Law Enforcement Cooperation 2022) <<https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know>> accessed 28 May 2024.

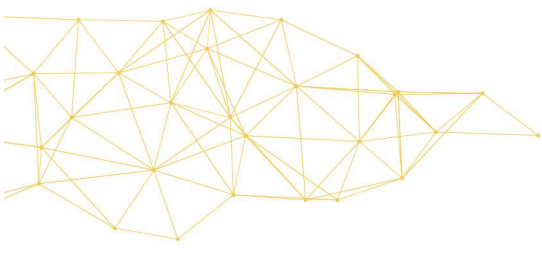
³² Hine and others (n 30).

³³ *ibid.*

³⁴ Europol (n 31).

³⁵ Hine and others (n 30).

³⁶ Europol (n 31).



augmented reality (AR), mixed reality (MR), or simply if non-immersive social metaverse platforms (desktop experience) is used. Safety risks linked to products used in a metaverse context (glasses, helmets, haptic suit,...) are also a core part of the safety layered landscape.

Immersion is a crucial element to consider when assessing safety in metaverses as it has the potential to make abuses more intrusive and harmful. Europol also highlighted the significant impact metaverses can have on the physical world. While some may dismiss or minimize the offences committed in the metaverse as not being real, the whole point of virtual realities is their immersive nature³⁷. It is precisely the immersion which is blurring the lines between physical and virtual worlds which can make experiences in VR far more traumatic than in other digital environments.³⁸

Immersion also triggers the same physiological and psychological responses as in the physical world.³⁹ In addition, with some equipment, users can even feel actions in virtual reality when wearing haptic suits⁴⁰. Nina Jane Patel, a psychotherapist who has highlighted the issue of sexual assault on avatars in virtual reality and the resulting physiological and psychological trauma, commented on her assault in the metaverse. She mentioned that “while she logically knew her attack happened to a digital avatar, hearing the voices of her attackers in her ear made it feel like it was happening to her body”⁴¹.

In addition to the immersive aspect of metaverses, **avatars and digital identity** perception play a crucial role in the virtual worlds⁴². Research analyzing how people would perceive their avatars in social virtual reality concluded that giving avatars personality and unique traits helps users see those as a second self, leading to attachment and concern, especially if the avatar is under threat or harm⁴³. Compared to traditional virtual worlds and online games, participants found their interactions with avatars in social VR to be more engaging, intimate, and personal⁴⁴. Users tend to make their social VR avatars resemble themselves, often viewing their avatars as extensions of their own identity⁴⁵.

The question of the status of the avatar has not been legally handled. So far, avatars have not yet reached the status of legal or natural persons. Some wonder if legal persona is necessary to make avatars responsible for their actions in metaverses. Even then, discussions remain on what standards and criteria need to be in place to distinguish

³⁷ Will Taylor, ‘Police Investigate “rape” in Metaverse after Group of Men Attack Girl in Virtual Reality Room’ *LBC* (2 January 2024) <<https://www.lbc.co.uk/news/police-investigate-rape-metaverse/>> accessed 28 May 2024.

³⁸ Mary Anne Franks, ‘The Desert of the Unreal: Inequality in Virtual and Augmented Reality’ (2017) 51 *U.C.D. L. Rev.* 499.

³⁹ Hine, « Content Moderation in the Metaverse Could Be a New Frontier to Attack Freedom of Expression »; commenting on the findings of Parsons et al., « Assessment of Psychophysiological Differences of West Point Cadets and Civilian Controls Immersed within a Virtual Environment ».

⁴⁰ Marsden (n 29).

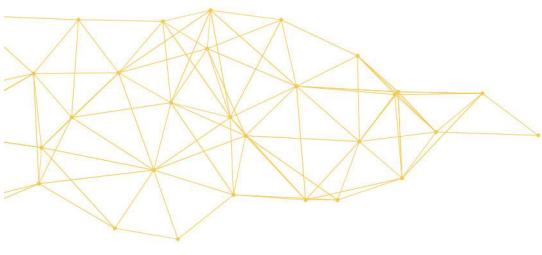
⁴¹ Naomi Nix, ‘Attacks in the Metaverse Are Booming. Police Are Starting to Pay Attention.’ *Washington Post* (8 February 2024) <<https://www.washingtonpost.com/technology/2024/02/04/metaverse-sexual-assault-prosecution/>> accessed 28 May 2024.

⁴² Hong Wu and Wenxiang Zhang, ‘Digital Identity, Privacy Security, and Their Legal Safeguards in the Metaverse’ (2023) 2 *Security and Safety* 2023011.

⁴³ Guo Freeman and others, ‘My Body, My Avatar: How People Perceive Their Avatars in Social Virtual Reality’, *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (Association for Computing Machinery 2020) <<https://dl.acm.org/doi/10.1145/3334480.3382923>> accessed 16 May 2024.

⁴⁴ *ibid.*

⁴⁵ *ibid.*



between a “legal” avatar and the true legal person who operates that avatar⁴⁶. Some also wonder if the strong relationship a real person has with their avatar, compared to cases where there is no such bond, influences the assessment of the offense. If so, how could such a distinction be made⁴⁷?

Another factor influencing safety consideration is the **anonymity**, as in metaverses, there is no way of knowing whether the other person is real or not⁴⁸. It complexifies accountabilities and creates enforcement challenges. Discussions regarding the risk and benefits of online anonymity already exist when it comes to digital regulation, with proposals to restrict online anonymity arising regularly. The nature of metaverses and the additional risks posed by increased immersiveness amplify the importance of the question.

Safety in metaverses is intricately linked to **jurisdiction and enforcement**. Some report that “virtual reality is still a legal vacuum”, leading Interpol to call for police forces around the world to develop protocols for dealing with VR crime, including sexual assault⁴⁹. Interpol even opened a Police station within its own metaverse⁵⁰. Legal uncertainties persist regarding whether the criminal elements of offenses committed in virtual reality meet the definitions stipulated by current laws. Police officer report warn about the emotional and psychological impact for victim that virtual offences can have⁵¹. These offences committed on avatars may not meet the legal criteria for (sexual) abuse, as existing legislation typically requires physical acts and other material conditions to be fulfilled⁵². A solution would be to rely on lesser charges such as harassment which could apply since physical contact is not a constitutive element of the offence. In addition, lesser charges could be used such as harassment in case of rape as the physical contact is not necessary. However, this often requires multiple offenses over time, and the ephemeral nature of interactions in metaverses complicates the application of such provisions⁵³. This “misalignment between technological advancements and the limited jurisdiction of regulations, law enforcement, and consumer protection presents considerable challenges”⁵⁴.

⁴⁶ Pin Lean Lau, ‘3 Issues to Address before We Dive into the Metaverse’ (*World Economic Forum*, 7 February 2022) <<https://www.weforum.org/agenda/2022/02/metaverse-legal-issues/>> accessed 28 May 2024.

⁴⁷ Matthias Kettemann, Martin Müller and Caroline Böck, ‘Regulatory Approaches to Immersive Worlds: An Introduction to Metaverse Regulation’ (*Project Immersive Democracy*, 25 September 2023) <<https://www.metaverse-forschung.de/en/2023/09/25/963/>> accessed 28 May 2024.

⁴⁸ Wu and Zhang (n 42).

⁴⁹ Andrew Potter, ‘A Rape in Cyberspace, Revisited’ (*nevermind*, 12 February 2024) <https://nevermindgenx.substack.com/p/a-rape-in-cyberspace-revisited?utm_medium=reader2> accessed 27 May 2024.

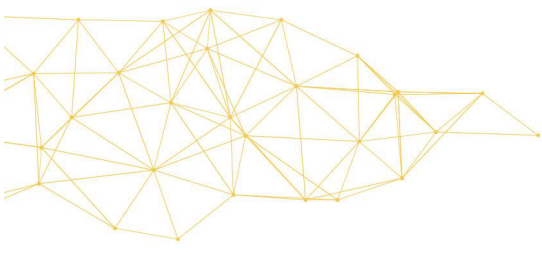
⁵⁰ Michal Gromek, ‘Are We Ready For Avatars Reporting Sexual Harassment In The Metaverse Police Stations?’ (*Forbes*) <<https://www.forbes.com/sites/digital-assets/2023/05/08/are-we-ready-for-avatars-reporting-sexual-harassment-in-the-metaverse-police-stations/>> accessed 28 May 2024.

⁵¹ Nancy Jo Sales, ‘A Girl Was Allegedly Raped in the Metaverse. Is This the Beginning of a Dark New Future?’ *The Guardian* (5 January 2024) <<https://www.theguardian.com/commentisfree/2024/jan/05/metaverse-sexual-assault-vr-game-online-safety-meta>> accessed 27 May 2024.

⁵² Europol (n 31).

⁵³ Nix (n 41).

⁵⁴ Gromek (n 50).



2.5. Safety in EU policy and regulatory instruments on metaverses

Safety is also a key consideration in EU policy documents. On a horizontal level, safety is included in the European Declaration on Digital Rights and Principles for the Digital Decade⁵⁵. The declaration mentions commitments to protect individuals, businesses, and public institutions from cybercrime, including data breaches and cyberattacks, and safeguarding digital identities from theft or manipulation. But also to hold accountable those who undermine online security, compromise the integrity of the European digital environment, or promote violence and hatred online.

On policy instruments specific the metaverse, the EC citizens panel on virtual worlds, resulted in a report of 23 citizen recommendations which included safety as one the 8 citizen's values & principles for desirable and fair European Worlds⁵⁶. European citizens asked to be kept safe and secure, including through the protection of data and prevention of manipulation and theft. These values and principles were the foundations of a set of recommendations elaborated by the citizen's panel. Recommendation 21 called for legal frameworks for transparency and protection of everyone in the metaverse - prioritizing vulnerable groups. The recommendation emphasizes how safety must be the priority and how citizens, their identities, the vulnerable ones should be kept safe. They called for rules minimizing the risks or criminal or harmful activities in virtual worlds and the Metaverse.

The European Commission adopted during summer 2023, its communication entitled An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition.⁵⁷ The text highlights the development of virtual works would likely pose challenges to fundamental rights, cybercrime, cyberviolence including gender-based but consumer protection and safety. The Commission initiative for a Web 4.0 aims for a virtual world which reflects the EU values, principles and where fundamental rights are respected and where people can be safe, confident and empowered. The initiative also highlights the potential of the EU robust legislative framework to safeguard and protect EU values, principles and fundamental rights. It further specifies that "in relation to the protection and enforcement of the rights of individuals and companies operating in virtual worlds, the Digital Services Act (DSA) and the Digital Markets Act (DMA) introduce a comprehensive system of accountability and obligations for online platforms"⁵⁸.

Since the release of the initiative, the European Parliament has had active Committee which delivered two reports of their own initiatives in December 2023 : the report on virtual worlds – opportunities, risks and policy implications for the single market from the Internal Market and Consumer Protection Committee⁵⁹ and the report on policy

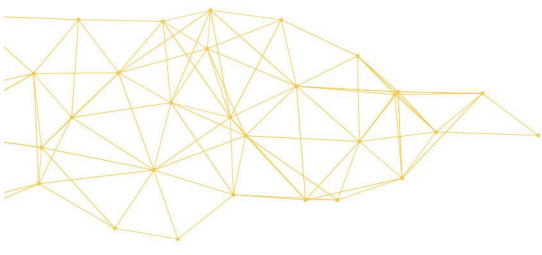
⁵⁵ European Commission, European Declaration on Digital Rights and Principles for the Digital Decade 2022 [COM/2022/28 final].

⁵⁶ European Commission, Staff Working Document Accompanying the document Communication from the Commission to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition 2023 [SWD(2023) 250 final].

⁵⁷ European Commission COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS An EU initiative on Web 4.0 and virtual worlds (n 14).

⁵⁸ *ibid.*

⁵⁹ European Parliament and Pablo Arias Echeverría, 'REPORT on Virtual Worlds – Opportunities, Risks and Policy Implications for the Single Market' (2023) A9-0397/2023 <https://www.europarl.europa.eu/doceo/document/A-9-2023-0397_EN.html> accessed 22 May 2024.



implications of the development of virtual worlds – civil, company, commercial and intellectual property law issues from the Legal Affairs Committee⁶⁰. One report considers that virtual worlds should be regulated to prevent harmful behaviors such as harassment, bullying, discrimination, and surveillance, ensuring a safe environment with robust cybersecurity, privacy, transparency, user rights protection through existing European legislation and strategies like the Digital Services Act⁶¹.

While all these policy documents mention safety, none is providing a common definition. Safety in the metaverse seems to be “loosely defined”⁶² and constitutes a compound term covering a wide range of aspects including cybercrime (digital identity thefts, hacks, fraud, scam,...), content moderation (violence online, hate speech, spread of illegal content, disinformation), data protection, manipulation risks, consumer protection, respect to fundamental rights, principles & values, and the protection of vulnerable groups. The EC expressly identified the DSA, a new content moderation legislation, as part of the applicable framework for regulating metaverses and ensuring a safer digital environment. Therefore, the question of whether safety considerations and safety risks reduction in metaverses could actually be handled under the EU content moderation landscape arise.

2.6. Content moderation in the metaverse: challenges and considerations

Content moderation, broadly defined as the “governance mechanisms that structure participation in a community to facilitate cooperation and prevent abuse”⁶³, faces unique and complex challenges within the metaverse. E. Hine succinctly frames the fundamental question of metaverse content moderation as “what to remove, where, for whom, and how.”⁶⁴ While these questions may seem straightforward, they raise numerous intricate issues.

The metaverse hosts **multitude content forms** including posts, chats, behaviors, avatars, outlook, world elements, user-generated content and so forth. Virtual reality (VR) adds layers of complexity by incorporating “both verbal and non-verbal interaction such as voice, gestures, proxemics, gaze, and facial expression.”⁶⁵ These diverse forms of content complicate the definition and execution of content moderation.

Furthermore, content and behaviors in the metaverse can be both ephemeral and highly context-dependent, unlike the content we are currently accustomed to⁶⁶. This ephemerality means no traces are left behind, complicating evidence gathering and reporting⁶⁷. Effective content moderation in the metaverse would require providers to

⁶⁰ European Parliament, Axel Voss and Iban Garcia Del Blanco, ‘Report on Policy Implications of the Development of Virtual Worlds – Civil, Company, Commercial and Intellectual Property Law Issues’ (European Parliament 2023) A9-0442/2023 <https://www.europarl.europa.eu/doceo/document/A-9-2023-0442_EN.html> accessed 22 May 2024.

⁶¹ European Parliament and Arias Echeverría (n 59).

⁶² Louise Donovan, “A Wake-up Call”: After Alleged Metaverse Rape, Calls to Protect Women and Girls Grow’ (*The Fuller Project*, 22 January 2024) <<https://fullerproject.org/story/a-wake-up-call-after-alleged-metaverse-rape-calls-to-protect-women-and-girls-grow/>> accessed 28 May 2024.

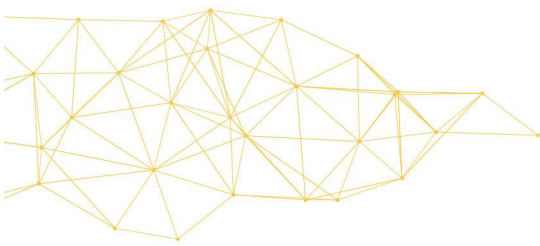
⁶³ James Grimmelman, ‘The Virtues of Moderation’ [2015] Cornell Law Faculty Publications <<https://scholarship.law.cornell.edu/facpub/1486>>.

⁶⁴ Hine (n 7).

⁶⁵ Freeman and others (n 43).

⁶⁶ Europol (n 31).

⁶⁷ *ibid.*



monitor and analyze every second of every interaction, a daunting and impractical task⁶⁸. However, over-removal and aggressive moderation creates freedom of expression concerns including risks for chilling effects⁶⁹.

Metaverse providers, like traditional social media platforms, offer both **private and public spaces on their services**, adding another complexity layer to content moderation. Legislation applicable to information communicated in public spaces might only apply to a portion of the metaverse's offerings, complicating enforcement and compliance⁷⁰.

The scale, speed, and live nature of interactions in the metaverse present further difficulties. Relying solely on human moderators is unrealistic, but automated moderation systems also have significant limitations, including risks of over-removal, under-removal, lack of contextual understanding, and insufficient linguistic diversity in datasets⁷¹.

Cross-border content moderation introduces additional complications. Metaverse community guidelines or terms of service might conflict with local laws of the users' respective locations.⁷² This could create a situation where metaverse platforms may need to restrict content based on local laws, leading to scenarios where users from different countries see different online worlds, undermining a shared reality⁷³. Shared reality which is a goal of metaverses (and later the general metaverse). Alternatively, removing content globally could infringe on users' autonomy and freedom of expression. Determining enforcement structures, jurisdiction, and applicable laws is further complicated by the potential loss of user location data⁷⁴.

In the case of unacceptable behaviors in metaverses, one can wonder what moderation decision would be effective. Europol underlines that "suspending an account may just lead to someone opening another, while finding a perpetrator in the physical world and enforcing the law where they live may be a big challenge as well."⁷⁵ Especially if platforms are decentralized and based on anonymization. In 2022, Meta added a personal boundary system to stop harassment in VR which stops other people from getting too close⁷⁶. It is only a reactive measure adopted after abuse was reported. While this measure has shown imperfect results, it underscores the importance of designing technology, products, and services with safety in mind from the outset. Embedding safety by design and incorporating interdisciplinary consultations, including input from vulnerable groups, is crucial for developing effective and inclusive moderation practices⁷⁷.

⁶⁸ Ryan Hsu, 'Meet the New 'verse, Same as the Old 'verse: Moderating the "Metaverse"' (*Georgetown Law Technology Review*, 2 May 2022) <<https://georgetownlawtechreview.org/meet-the-new-verse-same-as-the-old-verse-moderating-the-metaverse/GLTR-05-2022/>> accessed 26 January 2023.

⁶⁹ *ibid.*

⁷⁰ For more on the question of public and private communication of the metaverse, see below 'Dissemination to the Public'

⁷¹ Noémie Krack, Lidia Dutkiewicz and Emine Ozge Yildirim, 'AI4Media Report on Policy for Content Moderation (D6.2) (2023) <<https://www.ai4media.eu/reports/report-on-policy-for-content-moderation-d6-2/>> accessed 29 September 2023.

⁷² Hine (n 7).

⁷³ *ibid.*

⁷⁴ Europol (n 31).

⁷⁵ *ibid.*

⁷⁶ Adi Robertson, 'Meta Is Adding a "Personal Boundary" to VR Avatars to Stop Harassment' (*The Verge*, 4 February 2022) <<https://www.theverge.com/2022/2/4/22917722/meta-horizon-worlds-venues-metaverse-harassment-groping-personal-boundary-feature>> accessed 28 May 2024.

⁷⁷ Donovan (n 62).

In conclusion, content moderation in the metaverse is fraught with challenges that extend beyond those faced by traditional online platforms. The diverse and immersive nature of the metaverse requires nuanced and innovative approaches to ensure user safety while respecting freedom of expression. The European Commission points to the Digital Services Act (DSA) as one of the appropriate tools for framing the regulatory landscape of the metaverse.

3. The Digital Services Act : regulating metaverses?

3.1. *Lex generalis* for content moderation and user safety

The DSA is part of the EU content moderation legislative arsenal. Content moderation decisions are for some required by the law through content moderation legislations and others performed voluntarily by platforms based on their terms and conditions or community guidelines⁷⁸.

The EU content moderation landscape has been increasingly complex over the years by the adoption of different regulatory instruments making distinctions based on the category of online platforms, the type of content, and the nature of the legal instrument, whether it is hard law, soft law, or self-regulation⁷⁹. The EU regulatory content moderation framework include first horizontal rules applicable to all categories of online platforms and all types of content (*lex generalis*) including the DSA focusing on content moderation and then a set of *lex specialis* addressing specific types of content that require particular attention, regulations, and procedures. "Given the various sensitivity or degrees of the illegality of this content, a one size fits all approach would be detrimental to freedom of expression; therefore, specific rules have been adopted".⁸⁰ These include content related to terrorism, child sexual abuse material, copyright infringement and hate speech.

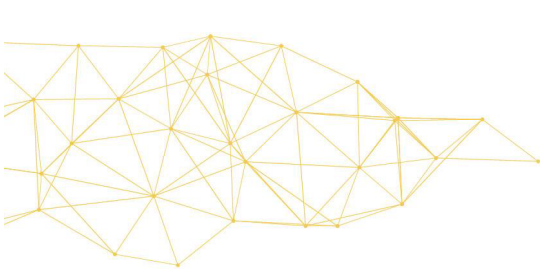
The DSA provides the first legal definition of content moderation. According to Article 3(t), content moderation is defined as "the activities, whether automated or not, undertaken by providers of intermediary services, that are aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetization, disabling of access to, or removal thereof, or that affect the ability of the recipients of the service to provide that information, such as the termination or suspension of a recipient's account".

The scope of content moderation primarily depends on the definition of illegal content and information that is incompatible with the intermediary service's terms and conditions. 'Illegal content' is defined as "any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law" (Article 3 h DSA). Recital 12 DSA completes the definition indicating that illegal content should be defined broadly to cover information relating to illegal content, products, services, irrespective of its form (DSA art. 3, h) completed by recital 12). However, "information", which is a key component,

⁷⁸ Krack, Dutkiewicz and Yildirim (n 71).

⁷⁹ *ibid.*

⁸⁰ *ibid.*



is not further defined in the DSA. This triggers numerous questions when it comes to metaverses and virtual reality. Can user behavior be considered information? What about the design of their avatars or the objects, environments, and elements in the virtual world? These questions remain legally unsettled.

3.2. Provider of metaverses and the scope of the DSA

The scope of the DSA covers all intermediary services offered to recipients in the European Union irrespective of the place of establishment of the intermediary service provider. The DSA categorizes digital service providers into several tiers, such as technical services⁸¹, hosting services⁸², and online platforms⁸³, with a special category for very large online platforms (VLOPs) and very large online search engines (VLOSEs)⁸⁴.

The first layer of obligations applies to all intermediary services. The DSA distinguishes three types of intermediary services:

- Mere conduit services⁸⁵
- Caching services⁸⁶
- Hosting services⁸⁷

This categorization aligns with the eCommerce Directive. Metaverse platforms fall under the third category, hosting services. While mere conduit and caching services provide purely technical functions, hosting services "store information provided by, and at the request of, a recipient of the service⁸⁸." The second layer of DSA obligation applies to hosting services providers. When a metaverse platform allows a user to upload their avatar or create content using tools on the platform, it is storing information at the user's request. This should apply to all types of metaverse platforms, except those that operate purely offline, which would not qualify as a metaverse.

The third layer of DSA obligation applies to online platforms. The DSA defines them as a subset of hosting services. An online platform is "a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public"⁸⁹

To qualify as an online platform, several conditions must be met:

- It must be a hosting service.
- It must not only store information but also disseminate it to the public at the user's request.
- The service must not be auxiliary.

⁸¹ DSA, article 4 and 5

⁸² DSA, article 6

⁸³ DSA, article 2(i)

⁸⁴ DSA, article 33

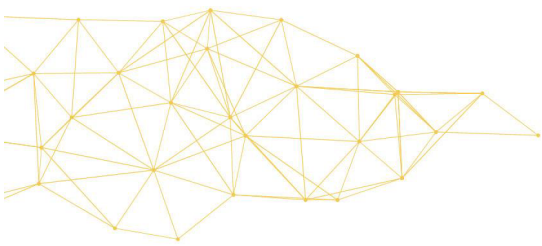
⁸⁵ DSA, article 4

⁸⁶ DSA, article 5

⁸⁷ DSA, article 6

⁸⁸ Ibid.

⁸⁹ DSA, article 2, (i)



3.2.1. Dissemination to the public

The concept of dissemination to the public raises several questions. Is there a threshold of users a service must have to be considered large enough to qualify as a platform? Are websites that only allow users after a careful vetting procedure excluded? Recital 14 of the DSA clarifies that information is considered disseminated to the public when it is made “easily accessible to recipients of the service in general without further action by the recipient of the service providing the information being required, irrespective of whether those persons actually access the information in question.” The information must be available to a “potentially unlimited number of persons.”

This brings us to an important point regarding the classification of metaverses as online platforms: the difference between a publicly open and a private structure of a metaverse. In a public metaverse, similar to an online platform like Facebook, virtually anyone can sign up. Platforms like Second Life currently work in this similar manner.

In the opposite situation, a private metaverse restricts access to specific individuals. An example could be a virtual classroom, where only a certain number of people are allowed, typically selected by the teacher. In such cases, Recital 14 seems to exclude these from the definition of an online platform. It specifies that “where access to information requires registration or admittance to a group of recipients of the service, that information should be considered to be disseminated to the public only where recipients of the service seeking to access the information are automatically registered or admitted without a human decision or selection of whom to grant access.”

Meta Horizons Quest offers its users to create “Members-Only” Worlds, where users have to be manually approved to join. The terms and conditions of the platform highlight what can and cannot be allowed on those private metaverses⁹⁰. Developers of those worlds have to adhere to the Code of Conduct for Virtual Experiences⁹¹ and Meta highlight in their terms and conditions that they will remain in charge of applying their community guidelines in those private virtual spaces⁹².

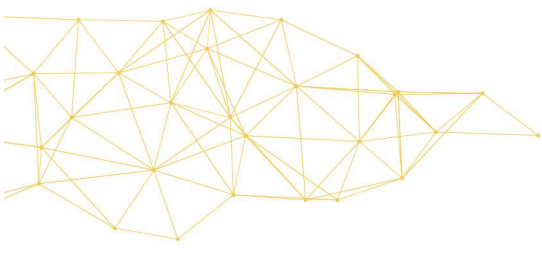
The coexistence of public and private virtual worlds on platforms gives rise to the following question: What part of the DSA applies to a private classroom hosted in an open metaverse? Recital 15 of the DSA states that “where some of the services provided by a provider are covered by this Regulation whilst others are not, or where the services provided by a provider are covered by different sections of this Regulation, the relevant provisions of this Regulation should apply only in respect of those services that fall within their scope.” Should a private forum, such as a member-only world on horizon quest be considered a different service from the general service of providing the metaverse platform? The same question arises regarding regular private groups on online platforms and the application of DSA obligations to them.

Based on the above definition of virtual worlds, we could argue that such private virtual worlds do not qualify as virtual worlds at all: indeed, users on such private groups

⁹⁰Meta Horizon Worlds Mature and Prohibited Worlds Policy | Meta Store' <<https://www.meta.com/help/quest/articles/horizon/create-in-horizon-worlds/restrictions-to-worlds-in-horizon/>> accessed 3 June 2024.

⁹¹Code of Conduct for Virtual Experiences | Meta Store' <<https://www.meta.com/help/quest/articles/accounts/privacy-information-and-settings/code-of-conduct-for-virtual-experiences/>> accessed 3 June 2024.

⁹² 'How the Code of Conduct for Virtual Experiences (CCVE) Applies to Members-Only Worlds | Meta Store' <<https://www.meta.com/help/quest/articles/horizon/safety-and-privacy-in-horizon-worlds/code-of-conduct-members-only-worlds/>> accessed 3 June 2024.



lack the capability to interact in real-time with the community as a whole. While the interaction between public and private virtual worlds on metaverse providers raise questions regarding the applicability of the DSA, we will keep the focus on this article on situations where a metaverse provider allows for such communication and therefore clearly falls under the DSA classification of online platforms.

3.2.2. Online platforms allowing contracts

The DSA also defines another category of online platforms: those allowing consumers to conclude distance contracts with traders⁹³. The DSA defines traders as “any natural person, or any legal person irrespective of whether it is privately or publicly owned, who is acting, including through any person acting in his or her name or on his or her behalf, for purposes relating to his or her trade, business, craft, or profession.”⁹⁴ Thus, if a metaverse platform allows professional traders to sell goods to customers, it falls under this category of DSA obligations. However, those particular obligations fall beyond the scope of this paper, as we previously stated that we would not focus on the exchange of goods and services in metaverses.

3.2.3. Very Large Online Platforms and general metaverse

The fourth and last layer of DSA obligations applies to very large online platforms and very large online search engines (VLOPs and VLOSEs)⁹⁵. Earlier, we mentioned the difference between specific metaverses and a potential future general metaverse. While we are far from achieving the latter, several existing platforms can be classified as metaverses. However, none of these platforms meet the DSA's threshold for very large online platforms, defined as those with over 45 million average monthly users in the EU.

3.2.4. The DSA and metaverse(s): potential, yet many questions remain

The DSA does not provide a specific definition for the metaverse or virtual worlds. Therefore, metaverses under the DSA must be categorized based on their specific characteristics. Some platforms defined as metaverses could be considered online platforms, while others may not. This paper primarily focuses on the risks associated with metaverses accessible to a large number of people—essentially, metaverses that are also online platforms.

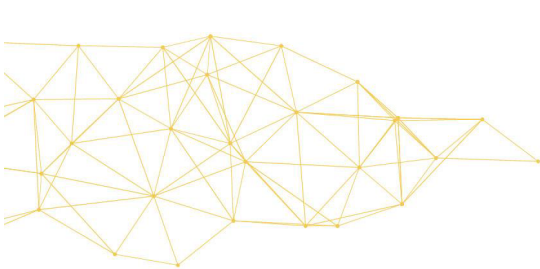
3.3. Liability of metaverse providers in EU law

First, it is important to clarify that we are discussing the intermediary liability regime applied in a metaverse context. We focus on the provider of the metaverse platform, not the users responsible for infractions within the metaverse. In many cases, it will be

⁹³ DSA, Section 4

⁹⁴ DSA, article 2, (f)

⁹⁵ DSA, Section 5



challenging for victims to bring these individuals to justice due to issues such as geographical differences, lack of proof, and online anonymity⁹⁶. Consequently, victims are often more likely to seek redress directly from the platforms.

The Digital Services Act (DSA) does not radically change the EU liability regime for online intermediaries. It reaffirms the rules established in the eCommerce Directive and clarifies them in line with European Court of Justice rulings, such as in the L'Oréal and Google France cases. Article 6 of the DSA outlines the liability exemption for hosting services, under which metaverse providers fall:

The service provider shall not be liable for the information stored at the request of a recipient of the service, on condition that the provider: (a) Does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or (b) Upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content.

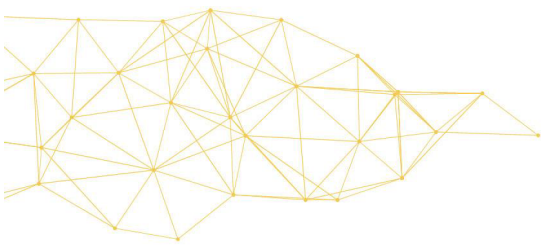
The DSA introduces additional requirements known as due diligence obligations to this liability exemption. These obligations mark a transition from a horizontal liability exception regime for intermediary services providers to a new horizontal moderation legal framework composed of horizontal liability and accountability rules. The DSA harmonizes the notice and action procedures, which were previously uncovered by the e-commerce Directive. Article 16 DSA now mandates that hosting services implement “mechanisms to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content.” Such notices “shall be considered to give rise to actual knowledge or awareness for the purposes of Article 6 in respect of the specific item of information concerned where they allow a diligent provider of hosting services to identify the illegality of the relevant activity or information without a detailed legal examination.”

It is unclear whether (proto) metaverses could benefit from the liability exemption contained in the DSA. For example, in the case of Second Life, authors argue that as the platform mostly relies on user-created content, it plays an active role in the storage of content and therefore cannot profit from the exemption offered by the e-Commerce directive nor the DSA⁹⁷. Indeed, if the service provider “plays an active role of such a kind as to give it knowledge of, or control over, that information”⁹⁸, then it should not enjoy the liability exemption. In any case, the application of the liability exemption will need to be assessed on a case-by-case basis and might depend on the architecture and services offered by a particular metaverse platform. Furthermore, while lifting the liability exemption might offer recourse against platforms in some situations, the full establishment of civil liability will need to be established, which might not always be an easy task when it comes to a virtual action.

⁹⁶ See supra

⁹⁷ Batu Kinikoglu, ‘Liabilities of Virtual World Developers as Intermediary Service Providers: The Case of Second Life’ (2023) 13 Queen Mary Journal of Intellectual Property 121.

⁹⁸ DSA, recital 18



3.4. Metaverses as online platforms: obligations in the DSA

The DSA is an asymmetric regulation as it imposes different levels of obligations and responsibilities based on the type of intermediary services. Each category has distinct obligations tailored to the specific needs and risks associated with different types of digital service providers. In this section, we will focus on the obligations of the DSA that are applicable to intermediary services as a whole, hosting services and online platforms. We will not provide a full overview of these obligations but will pinpoint those who we deem of interest for regulating metaverses.

3.4.1. Obligations applicable to all intermediary services.

While Meta, Microsoft, and Roblox are companies with registered offices, Decentraland operates as a "foundation" with no disclosed registered office or publicly known identities of the individuals in its Decentralized Autonomous Organization (DAO) Committee, who are only known by their usernames⁹⁹. In addition, the use of "Ethereum blockchain means that the shares in the "foundation" cannot easily be legally assigned to a person"¹⁰⁰ complexifying enforcement. However, articles 11 to 13 of the DSA impose intermediary services to put in place a single point of contact across the European Union, or to designate a legal representative if they are outside the Union. While our article does not focus on the issues related to the extra-territorial nature of the DSA, the fact that users can join across different countries raises different challenges.¹⁰¹ Such challenges would be even higher with no point of contact at EU level – thankfully these articles take care of that.

The DSA also improves transparency in the intermediary services terms and conditions. Article 14 of the DSA states that: "Providers of intermediary services shall include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions. That information shall include information on any policies, procedures, measures and tools used for the purpose of content moderation, (...), as well as the rules of procedure of their internal complaint handling system. (...)". The article further specifies that intermediary services "shall act in a diligent, objective and proportionate manner in applying and enforcing the restrictions (...), with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service".

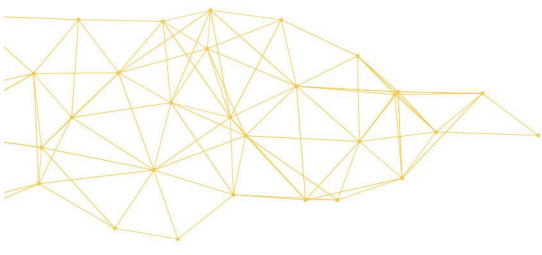
By providing their users with a clear framework on what type of content should or should not be allowed on their services and by making sure that providers adhere to due process at some level, this provision reinforces the rights of users. When it comes to metaverses, this clarification protects the freedom of expression of users towards the moderation of the content they produce. Furthermore, the obligation to apply those restrictions offers recourses towards users who estimate they are confronted with content that does not follow the rules of the online environment.

It was not possible for us to access the experience of creating and using a Meta Horizons Quest account, as the service is currently not available in our home country of

⁹⁹ Sara Nesler and Antonia Herfurth, 'The Metaverse in the Legal Framework (1)' (*Alliuris*, 16 January 2024) <<https://www.alliuris.org/the-metaverse-in-the-legal-framework-1/>> accessed 28 May 2024.

¹⁰⁰ *ibid.*

¹⁰¹ Hine (n 7).



Belgium.¹⁰² However, the terms and conditions for using Meta Platform Technology (MPT) products are available online.¹⁰³ However, the terms and conditions for using Meta Platform Technology (MPT) products are available online. We did, however, not find it easy to navigate through policies which are contained in different sections of the website presenting the terms and conditions. For example, navigating towards the “Meta Terms of Service” redirects the user towards the Facebook terms and conditions¹⁰⁴, making it unclear to understand whether those would also apply on the virtual worlds offered through the Horizon Quest app.

Further research and examination would be necessary to provide a clear view of which policies apply (or not) in virtual worlds – however, such complexity clearly seems in conflict with the requirements of article 14 which mandates that terms and conditions shall be provided in “clear, plain, intelligible, user-friendly and unambiguous language, and shall be publicly available in an easily accessible and machine-readable format”.¹⁰⁵ Second Life offers a slightly better approach to this question: their terms of services¹⁰⁶ directly refer to their content guidelines¹⁰⁷ (for the creation of content) and their community standards¹⁰⁸ (for acceptable behaviors on the platform).

Article 15 of the DSA request intermediary services providers to deliver at least once a year transparency reports providing the following information related to their moderation practices:

- Orders to remove content as provided by article 8 of the DSA
- Information on their moderation practices, should they engage in such activities
- The number of complaints they received through their internal complaint-system; and
- Any use of AI for content moderation

We were not able to find any publicly available report for (proto)-metaverses platforms such as Meta Horizon Quest or Second Life.

3.4.2. Obligations applicable to providers of hosting services and online platforms

Article 16 of the DSA request online platforms and hosting services to put in place notice and action mechanisms to allow “any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content.” This only applies to illegal content and not content that merely violates the platform’s terms and conditions.

When it comes to metaverses, such an obligation would make sure mechanisms are in place for users to report unlawful content and/or behavior that they are witness to. However, even if such reporting systems would be legally compliant with the DSA, in terms

¹⁰²Supported Countries for Meta Horizon Worlds | Meta Store’ <<https://www.meta.com/help/quest/articles/horizon/explore-horizon-worlds/horizon-supported-countries/>> accessed 3 June 2024.

¹⁰³ ‘Meta Store’ <<https://www.meta.com/be/fr/legal/supplemental-terms-of-service/>> accessed 28 June 2024.

¹⁰⁴ ‘Meta Platforms e.a. (Conditions générales d’utilisation d’un réseau social).

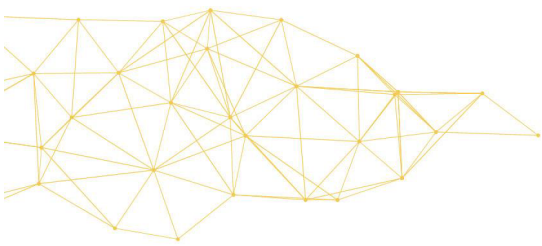
¹⁰⁵

DSA, article 14

¹⁰⁶ ‘Terms of Service’ <<https://lindenlab.com/tos>> accessed 3 June 2024.

¹⁰⁷ ‘Content Guidelines’ <<https://lindenlab.com/legal/content-guidelines>> accessed 3 June 2024.

¹⁰⁸ ‘Community Standards’ <<https://lindenlab.com/legal/community-standards>> accessed 3 June 2024.



of safety it is a post-hoc mechanisms, meaning users would still be harmed¹⁰⁹. In addition, article 16 lists the mandatory information to provide in the notice to constitute a sufficiently precise and adequately substantiated notices.

The DSA has not been adopted with metaverses in mind as the notice requires a clear indication of the exact electronic location of that information, such as the exact URL or URLs. Nevertheless, the provision still points out that where necessary, additional information enabling the identification of the illegal content adapted to the type of content and to the specific type of hosting service can be included. For metaverses, given the ephemerality of interactions and various content forms, this part seems complex to comply with, complicating the reporting of illegal content for metaverse users.

Article 17 of the DSA forces online platforms and hosting services to “provide a clear and specific statement of reasons to any affected recipients of the service for any of the following restrictions imposed”. Those statements of reasons will allow users whose content is restricted on the metaverse to better understand why such restriction occurred and how to seek recourse after such a decision.

Article 18 of the DSA obliges hosting services and online platforms to report “any information giving rise to a suspicion that a criminal offense involving a threat to the life or safety of a person(s)” to relevant Member States authorities when becoming aware of the presence of such information on their services. This forces metaverse platforms to better take into account potential illegal misuses of their services.

3.4.3. Obligations applicable to online platforms, to the exception of MSE

Article 20 and article 21 focus on the redresses offered to users regarding decisions taken by online platforms. Article 20 governs how platforms put in place internal complaint-handling systems while article 21 allows users to resort to out-of-court dispute mechanisms. This enhances users’ right to a fair redress regarding decisions taken by the metaverse platform. We were not able to find clear recourse policies for users when it comes to content moderation on platforms such as Horizon Worlds and Second Life.

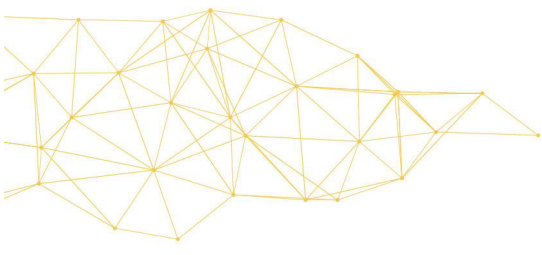
Article 22 introduces the notion of trusted flaggers, a status awarded by Digital Services Coordinator (DSC)¹¹⁰. Trusted flaggers are “entities, and not individuals, that have demonstrated, among other things, that they have particular expertise and competence in tackling illegal content and that they work in a diligent, accurate and objective manner.”¹¹¹ Online platforms must ensure that notices sent under article 16 of the DSA by a trusted flagger are given priority. While civil society organizations are the obvious choice for this role, law enforcement agencies could also be awarded such status if they meet the conditions. For instance, the Interpol Metaverse police station could potentially be awarded this status as an additional tool to fasten the Metaverse provider actions.

Article 23 requires online platforms to suspend from their services users that “frequently provide manifestly illegal content.” This incentives platform to take actions against users whose online behavior is repeatedly found in breach of the law. However, a risk to user safety is that these users could simply create new accounts after each

¹⁰⁹ Hsu (n 68).

¹¹⁰ Digital Services Coordinator are entities responsible for the enforcement of the DSA for intermediaries at Member State level – see DSA, art. 49

¹¹¹ DSA, recital 61



suspension under different identities or anonymity, if the latter is provided. Safety by design would require metaverse providers to address these considerations thoughtfully.

Article 24 imposes transparency and reporting for online platforms about the following information:

- The number of out-of-court dispute settlements under article 21 DSA,
- The number of accounts suspended under article 23 DSA,
- The number of their average monthly active recipients
- Their statement of reasons under article 17 needs to be provided to the European Commission to be stored in a publicly available database¹¹².

Article 25 prohibits platforms to “design, organize or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions.” It is a prohibition of dark patterns. It is important to note that practices covered under consumer protection¹¹³ and privacy¹¹⁴ are excluded from this provision¹¹⁵. However, article 25 only concerns online platforms, not other actors relying on the service to create virtual worlds – in that situation, users might have to solely resort on consumer protection or privacy regulation to avoid dark patterns.

3.5. DSA, online platforms & virtual risks

One of the primary objectives of the DSA is to ensure a safe, predictable and trusted online environment (Art. 1 § 1, recital 9 DSA) and this goes by establishing a clear, effective, predictable and balanced set of harmonized due diligence obligations for providers of intermediary services (Art. 1 §2 recital 40 DSA). The above section shows that while platform operating metaverses will be able to rely on the liability exception regime, they will still be bound by the provisions of the DSA pertinent to online platforms.

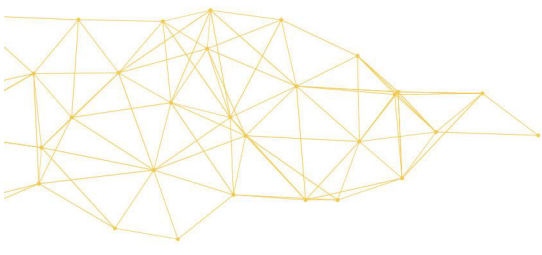
Those obligations exist to provide a safer online environment to the user and are therefore even more important when such an online environment allows a fully-immersive users experience, creating stronger risks for the user. However, the DSA merely provides metaverses’ platforms operators with due diligence obligation mainly focused on transparency requirements through a detailed procedural framework on content moderation but it does not impose stronger, holistic obligations ensuring user safety in the Metaverse. Therefore, merely imposing online platforms to put in place efficient, robust and fair content moderation mechanisms is probably not the most adequate response given the deep immersiveness offered by information exchanged on the metaverse.

¹¹² This database is active and available at the following address : <https://transparency.dsa.ec.europa.eu/>. On 22 May 2024, it only contained statements of reason for the 16 of the 17 VLOPs originally designed by the Commission (with Wikipedia being excluded from the database).

¹¹³ Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (‘Unfair Commercial Practices Directive’) (Text with EEA relevance) 2005.

¹¹⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)(Text with EEA relevance) 2016 (OJ L).

¹¹⁵ DSA, article 25, 2.



A pivotal question still lies in what should be considered as content or information under the DSA. Can the conducts, behaviors, outlook of a digital avatar be considered as information, content that has to be moderated under platforms' terms and conditions? In the case of virtual rape for example, could we consider the actions of the incriminated players as merely an information that should be moderated just like any other sort of text, video or audio content? The DSA does not further define the definition of information but its goal of protecting users online would justify a broad interpretation of the notion of information. This broad interpretation would allow Metaverse users' behaviors to be considered as information and also fall in the scope of the DSA obligations.

An interesting view on this can be observed in the terms and conditions of Second Life¹¹⁶ : their Community Guidelines includes inappropriate content as a subset of the prohibited behaviors on the platform, alongside for example assault, harassment and intolerance. The content guideline defines content as "anything that you create, share, post or otherwise transmit that another person could see, hear or otherwise experience in the Second Life Marketplace", while the Community Guidelines do not offer a general definition of what might be considered as "behavior". Regarding content, Second Life states that they might remove any content not respecting the guidelines and that users in violation of the content policy might see their accounts banned. The general Community Guidelines refers to account suspension or termination solely.

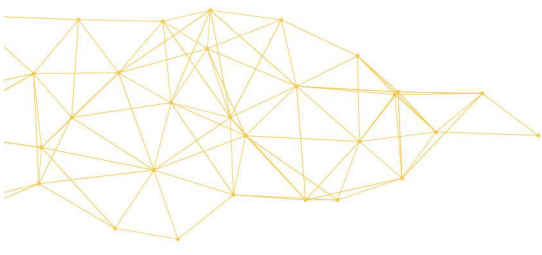
In that sense, we propose the following way to differentiate between content and behavior on the metaverse: content is any type of information generated by the user that is present on the platform in a permanent manner, while behavior is temporary. For example, a user that creates a virtual painting and that displays it in his virtual home has created content, while the user that comes and chats through a live temporary audio conversation engages in a virtual behavior.

From the point of view of the DSA however and given the objective of the regulation in terms of user safety, it would not make much sense to differentiate the application of the regulation for those two kinds of online information. Therefore, we argue that the DSA should apply broadly to information provided by users on the metaverse. However, the current obligations applicable to online platforms do not fully address the specific challenges created by virtual worlds and the metaverse. The DSA foresees a specific layer or rules for the VLOPs and VLOSEs. User's safety might be better covered under this set of rules.

3.6. Metaverse & DSA VLOPS regime

Given the significant influence of very large online platforms and search engines in facilitating public debate, economic transactions, and information dissemination, the DSA imposes additional obligations on these providers (Recital 75). As outlined in the previous sections of this contribution, current metaverse platforms are only bound by the obligations up to the level of online platforms. At present, no metaverse platform is large enough to qualify as a Very Large Online Platform (VLOP). However, looking ahead, it is worth investigating whether the additional layer of obligations under the DSA could effectively address user safety if these metaverse providers would meet the threshold one day.

¹¹⁶ 'Terms of Service' (n 106).



One of the DSA cornerstones is the systemic risks assessment (Art. 34 DSA) and mitigation obligations (Art. 35 DSA). The regulation underlines in its recital 79 that “very large online platforms and very large online search engines can be used in a way that strongly influences **safety online**”. These actors therefore need to be bound to an additional layer of obligations.

3.6.1. Systemic risks

Art. 34 DSA obliges VLOPS & VLOSES to “diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services.” They should assess the systemic risks stemming from the design, functioning and use of their services, as well as from potential misuses by the recipients of the service (individual or institutional actors), and should take appropriate mitigating measures in observance of fundamental rights.

The article defines what constitutes systemic risks. The following ones are relevant for metaverse safety risks.

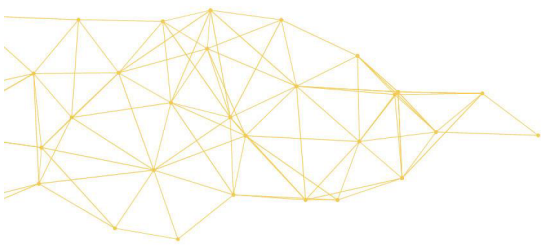
a) the dissemination of illegal content including also types of misuse of their services for criminal offences, and the conduct of illegal activities (rec 80)

b) any actual foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights which could stem design of the algorithmic systems

d). any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and **serious negative consequences to the person’s physical and mental well-being**. This one is of interest for the risks identified earlier on in this contribution. Recital 83 illustrates that online interface design could create such a risk.

Art. 35 requires VLOPs to put in place reasonable, proportionate, and effective mitigation measures, tailored to the specific systemic risks identified. The article lists various measures which could be adopted to mitigate the risks. These include adapting the design, features or functioning of their services including their online interfaces (Art. 35§1, a), or adapting their terms and conditions and their enforcement (Art. 35§1, b). Adapting content moderation processes is also mentioned. Interestingly for mitigating Metaverse safety risks, the provision mentions cyber violence in addition to illegal content (Art. 35§1, c). It also specifies that deep fakes should be identifiable as such and that a simple tool should be provided for users to report them (Article 35(1)(d)). This is particularly relevant in a metaverse context, as research has shown that deepfakes pose a rising threat to users, being used for cybercrime, manipulation, and impersonation¹¹⁷.

¹¹⁷Julia Stavola and Kyung-Shick Choi, ‘Victimization by Deepfake in the Metaverse: Building a Practical Management Framework’ (2023) 6 International Journal of Cybersecurity Intelligence & Cybercrime <<https://vc.bridgew.edu/ijcic/vol6/iss2/2>>; Shahroz Tariq, Alsharif Abuadba and Kristen Moore, ‘Deepfake in the Metaverse: Security Implications for Virtual Gaming, Meetings, and Offices’, *The 2nd Workshop on the security implications of Deepfakes and Cheapfakes* (2023) <<http://arxiv.org/abs/2303.14612>> accessed 30 May 2024.



3.6.2. Shortcomings

While the systemic risks assessment and mitigation obligations hold great promises and appear to be a relevant and useful regime to address the metaverse's risks explored earlier in this contribution, they also come with some shortcomings.

Those are self-assessment mechanisms. The DSA articles do not set up a risks assessment methodology. Recital 79 provides some hints such as the fact that severity and probability of the systemic risks should be considered when assessing the systemic nature of the risks. The same recital explains that providers "could assess whether the potential negative impact can affect a large number of persons, its potential irreversibility, or how difficult it is to remedy and restore the situation prevailing prior to the potential impact." This lack of guidance has prompted civil society to step up and produce insights such as methodologies for a meaningful implementation of this obligation¹¹⁸. Close interdisciplinary collaboration between relevant stakeholders will be key to ensure well thought risks assessment and mitigation procedure and methodology¹¹⁹.

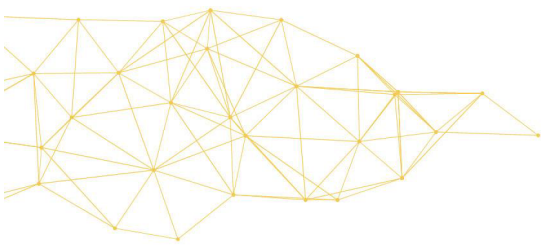
The mitigation obligation is only activated once the systemic risks stemming from the VLOPS and VLOSE have been identified as such. Risks and harms must therefore have occurred and build up into a systemic risk before such the obligation of assessment and mitigation is triggered. This ex-ante approach is diverging from other tech regulatory instruments such as the General Data Protection Regulation (GDPR) which foresees the obligation to conduct a data protection impact assessment (DPIA) if some conditions are met. The recently adopted AI Act is also adopting an ex-ante approach to avoid causing harms through strict market requirements to be met before releasing the product or service on the market. The AI Act also offers an environment where technology can be tested through regulatory sandboxes before entering the market which enables to also identify risks beforehand.

Another question about the risks assessment system in the DSA is the interpretation of systemic compared to individual-based risks. The notion of scale and target group impact are playing a role in the DSA systemic risks identification. It seems that the potential harm is not just to individual users, but to systems in society. "A risk is therefore systemic when it can lead to harm to individuals at a large scale or to systems essential to the governance and good functioning of society".¹²⁰ Investigating the roots of the systemic risk's concept, CERRE identifies 3 measures to include in assessment. First, how much of the overall system will be affected by a shock in one player; second, how much any individual player contributes to the systemic risk embedded in the whole system; and third, the ability of any given player to resist shocks and mitigate the associated risk. These

¹¹⁸ ECNL and Access Now, 'How Tech Corporations Should Assess Impacts on Our Rights' (*European Digital Rights (EDRI)*, 11 October 2023) <<https://edri.org/our-work/how-tech-corporations-like-google-meta-and-amazon-should-assess-impacts-on-our-rights/>> accessed 24 May 2024; Algorithm Watch and Michele Loi, 'How to Define Platforms' Systemic Risks to Democracy' (2023) <<https://algorithmwatch.org/en/making-sense-of-the-digital-services-act/>> accessed 24 May 2024; Directorate-General for Communications Networks, Content and Technology (European Commission), *Digital Services Act: Application of the Risk Management Framework to Russian Disinformation Campaigns* (Publications Office of the European Union 2023) <<https://data.europa.eu/doi/10.2759/764631>> accessed 24 May 2024.

¹¹⁹ Noémie Krack, 'Algorithmic Systems: How Should DSA Risk Assessments Be Conducted?' (*AI4media*, 21 November 2023) <<https://www.ai4media.eu/algorithmic-systems-how-should-dsa-risk-assessments-be-conducted/>> accessed 24 May 2024.

¹²⁰ Centre on Regulation in Europe (CERRE), Sally Broughton Micova and Andrea Calef, 'Elements for Effective Systemic Risk Assessment under the DSA' (2023).



elements are of particular interest when you think of threats to safety. Much will be clarified while DSA methodologies are developed, and guidance is released.

3.7. Towards a general metaverse and potential impact based on DSA' Scope

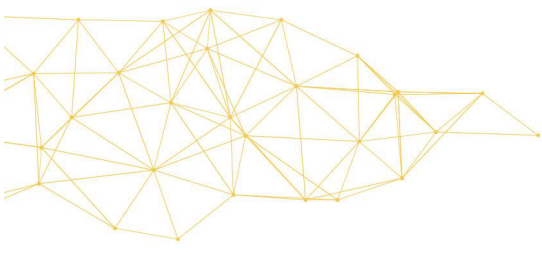
As a reminder, when we discuss the general metaverse, we think of a metaverse allowing users to travel through virtual worlds hosted by different service providers. This interconnected metaverse raises several significant questions, particularly concerning content moderation. For instance, if a user transitions from one metaverse platform to another and commits an offense against another user, it becomes crucial to determine which platform is responsible for handling, moderating, and taking action against such behavior. This situation is further complicated if the different metaverse platforms have varying terms and conditions, and community guidelines. Users would need to be clearly notified of the specific rules and regulations applicable in each new environment they enter to ensure they are aware of the differing standards of conduct. Another layer of complexity arises from the differing standards for account and avatar creation across metaverse providers. If some platforms promote anonymity while others require verified identities, the disparity can lead to significant challenges in maintaining consistent user accountability and safety.

Moreover, the challenges are amplified if some providers fall outside the scope of EU regulations, the access for EU users would need to be limited. It would be of crucial importance to avoid inconsistencies in enforcement and protection, potentially undermining user safety and trust. DSA's scope, implementation and interpretation would need careful consideration to accommodate the unique complexities of a general metaverse.

4. Recommendations for policymakers to address user safety challenges in the metaverse

While the Digital Services Act (DSA) represents a significant step towards enhancing user safety and ensuring accountability for online platforms, its applicability to the unique challenges of the metaverse is not entirely adequate. The DSA introduces essential obligations for digital platforms, fostering transparency and accountability, and exempts small and medium-sized enterprises (SMEs) from several burdensome requirements (DSA, Art. 19). Clarification on the core DSA concepts of content and information in the Metaverse context should be brought. Provisions should be adapted or interpreted to reflect the metaverse features. When it comes to safety the relevant DSA provisions for systemic risks assessment and mitigation do not apply to any metaverse platforms, as none meet the monthly user threshold for being designated as VLOPS. One can wonder whether the immersive nature of the metaverse may warrant a lower threshold for risk assessments compared to traditional online platforms.

However, the current risk assessment framework under the DSA might not be fully appropriate for the metaverse. The DSA's focus on societal-level risks does not adequately address the individual-level risks prevalent in the metaverse. Alternative solutions, such as the risk framework proposed in the AI Act, could be more suitable for the metaverse. For instance, accessing the metaverse via non-immersive means, such as using Horizon



Quests through a smartphone, presents different risk profiles compared to fully immersive experiences.

Although some trends indicate a reduced interest in the metaverse, recent developments contradict this slowdown, suggesting a continued need for robust regulatory considerations. Treating the metaverse purely as content under the DSA's perspective may be insufficient. There is a growing argument for a specific regulatory framework tailored to the metaverse to address its unique challenges¹²¹. This new framework would need to balance fostering technological development within the EU and managing the risks that the metaverse presents.

In summary, while the DSA provides a foundational regulatory approach for online platforms, its application to the metaverse reveals gaps that need addressing. A tailored framework, possibly integrating elements from the AI Act, may better serve the dynamic and immersive nature of the metaverse, ensuring both innovation and user safety are adequately balanced.

However, the relevance of yet another piece of EU digital regulation needs to be carefully assessed. Firstly, the current lack of enthusiasm of the general public for metaverses platforms attenuates the danger it poses to society¹²². Secondly, regulators at Member State level are already tasked with implementing and enforcing a variety of new regulations: the DSA, the Digital Market Act, the AI Act and adding yet another legislation might reduce the efficacy of regulatory enforcement – especially for smaller countries in the Union.

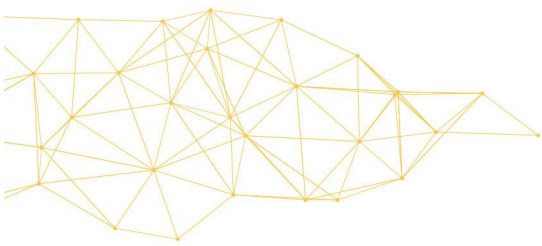
While regulatory instruments might come in the future, companies have a vested interest in not waiting for regulation and already developing safety-by-design practices to mitigate abuse and harassment, which are significant deterrents for Metaverse users. Interdisciplinarity by design would also ensure well thought Metaverse development.

A co-regulatory approach, such as the one taken in the DSA, where platforms can be punished by the regulators for breaching the rules they set themselves in accordance with the regulation also offers solutions that can improve safety while reducing the legislative burden on both companies and regulators. Such an approach is not void of criticisms either and more research is necessary to see whether it would fit the particular framework of the metaverse.

In conclusion, this article reflects on the broader issue of regulating virtual worlds and the Metaverse. Although the technology is still in its developmental stages and has faced recent commercial setbacks, the Metaverse holds significant potential to revolutionize communication and societal evolution. Its influence on individual well-being and society at large could be profound. Historically, the development of virtual technologies, such as online platforms and artificial intelligence, has largely proceeded without stringent regulation, under the assumption that technological progress inherently benefits humanity. However, recent challenges across various domains have amplified calls for a more measured approach to technological development, one that considers the actual impact on society. Facebook's former motto, "Move fast and break things," epitomized a philosophy that left regulators and civil society with no other choice than

¹²¹ European Parliament Research Service, 'Metaverse: Opportunities, Risks and Policy Implications' (24 June 2022) <[https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2022\)733557](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733557)> accessed 23 February 2024.

¹²² Meta Horizon Worlds only reported 200 000 active monthly users worldwide in 2022, see Jonathan Vanian, 'Meta Is Rebooting Horizon Worlds as the VR Platform Struggles to Grow' (CNBC, 28 July 2023) <<https://www.cnbc.com/2023/07/28/meta-horizon-worlds-metaverse-is-getting-an-update-with-more-games.html>> accessed 28 June 2024.



“Wait and repair”. We propose a shift in this paradigm: technological advancements should prioritize ensuring the safety and the protection of fundamental rights of all individuals, rather than pursuing progress for its own sake. Ex ante interdisciplinary risks assessment of the impact of metaverse on users safety should be pursued.

While the DSA was drafted as a technology-neutral regulation, metaverses are already shaking this up. Therefore, we strongly believe that it is now time to reflect on the notions contained in the DSA that will impact content moderation of the metaverse. There is no clear certainty on whether behavior and content are regulated similarly in the metaverse. Therefore, clarification of what the DSA (and more generally, EU Digital Regulation) defines as information and content appears primordial.



Bibliography

Abilkaiyrkyzy A and others, 'Metaverse Key Requirements and Platforms Survey' (2023) 11 IEEE Access 117765

Algorithm Watch and Loi M, 'How to Define Platforms' Systemic Risks to Democracy' (2023) <<https://algorithmwatch.org/en/making-sense-of-the-digital-services-act/>> accessed 24 May 2024

Camber R, 'Police Launch the First Investigation into "Virtual Rape"' Daily Mail Online (1 January 2024) <<https://www.dailymail.co.uk/news/article-12917329/Police-launch-investigation-kind-virtual-rape-metaverse.html>> accessed 28 May 2024

Cappannari L and Vitillo A, 'XR and Metaverse Software Platforms' 135

Centre on Regulation in Europe (CERRE), Broughton Micova S and Calef A, 'Elements for Effective Systemic Risk Assessment under the DSA' (2023)

'Code of Conduct for Virtual Experiences | Meta Store' <<https://www.meta.com/help/quest/articles/accounts/privacy-information-and-settings/code-of-conduct-for-virtual-experiences/>> accessed 3 June 2024

'Community Standards' <<https://lindenlab.com/legal/community-standards>> accessed 3 June 2024

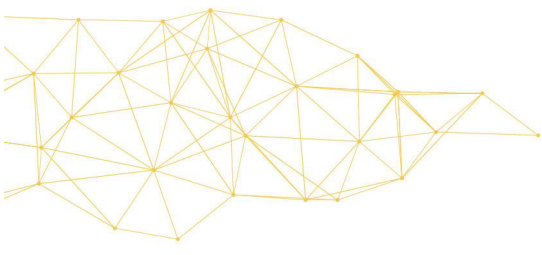
'Content Guidelines' <<https://lindenlab.com/legal/content-guidelines>> accessed 3 June 2024

Dibbel J, 'A Rape in Cyberspace. How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database Into a Society' (The Village Voice, 23 December 1993) <http://www.juliandibbell.com/texts/bungle_vv.html> accessed 27 May 2024

Dionisio JDN, Iii WGB and Gilbert R, '3D Virtual Worlds and the Metaverse: Current Status and Future Possibilities' (2013) 45 ACM Computing Surveys 1

Directorate-General for Communications Networks, Content and Technology (European Commission), Digital Services Act: Application of the Risk Management Framework to Russian Disinformation Campaigns (Publications Office of the European Union 2023) <<https://data.europa.eu/doi/10.2759/764631>> accessed 24 May 2024

Donovan L, "A Wake-up Call": After Alleged Metaverse Rape, Calls to Protect Women and Girls Grow' (The Fuller Project, 22 January 2024) <<https://fullerproject.org/story/a-wake-up-call-after-alleged-metaverse-rape-calls-to-protect-women-and-girls-grow/>> accessed 28 May 2024



ECNL and Access Now, 'How Tech Corporations Should Assess Impacts on Our Rights' (European Digital Rights (EDRi), 11 October 2023) <<https://edri.org/our-work/how-tech-corporations-like-google-meta-and-amazon-should-assess-impacts-on-our-rights/>> accessed 24 May 2024

European Parliament and Arias Echeverría P, 'REPORT on Virtual Worlds – Opportunities, Risks and Policy Implications for the Single Market' (2023) A9-0397/2023 <https://www.europarl.europa.eu/doceo/document/A-9-2023-0397_EN.html> accessed 22 May 2024

European Parliament, Voss A and García Del Blanco I, 'Report on Policy Implications of the Development of Virtual Worlds – Civil, Company, Commercial and Intellectual Property Law Issues' (European Parliament 2023) A9-0442/2023 <https://www.europarl.europa.eu/doceo/document/A-9-2023-0442_EN.html> accessed 22 May 2024

European Parliament Research Service, 'Metaverse: Opportunities, Risks and Policy Implications' (24 June 2022) <[https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2022\)733557](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733557)> accessed 23 February 2024

Europol, 'Policing in the Metaverse: What Law Enforcement Needs to Know. An Observatory Report from the Europol Innovation Lab', (European Union Agency for Law Enforcement Cooperation 2022) <<https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know>> accessed 28 May 2024

'Facebook to Acquire Oculus' (Meta, 25 March 2014) <<https://about.fb.com/news/2014/03/facebook-to-acquire-oculus/>> accessed 22 May 2024

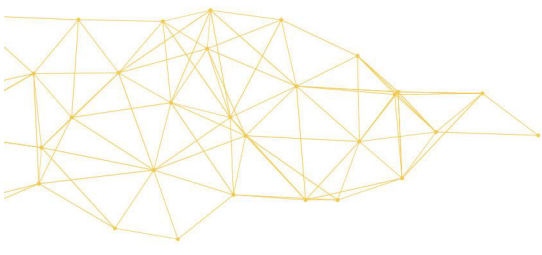
Franks MA, 'The Desert of the Unreal: Inequality in Virtual and Augmented Reality' (2017) 51 U.C.D. L. Rev. 499

Freeman G and others, 'My Body, My Avatar: How People Perceive Their Avatars in Social Virtual Reality', Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (Association for Computing Machinery 2020) <<https://dl.acm.org/doi/10.1145/3334480.3382923>> accessed 16 May 2024

—, 'Disturbing the Peace: Experiencing and Mitigating Emerging Harassment in Social Virtual Reality' (2022) 6 Proceedings of the ACM on Human-Computer Interaction 85:1

Grimmelmann J, 'The Virtues of Moderation' [2015] Cornell Law Faculty Publications <<https://scholarship.law.cornell.edu/facpub/1486>>

Gromek M, 'Are We Ready For Avatars Reporting Sexual Harassment In The Metaverse Police Stations?' (Forbes) <<https://www.forbes.com/sites/digital->



assets/2023/05/08/are-we-ready-for-avatars-reporting-sexual-harassment-in-the-metaverse-police-stations/> accessed 28 May 2024

Hine E, 'Content Moderation in the Metaverse Could Be a New Frontier to Attack Freedom of Expression' (2023) 36 Philosophy & Technology 43

—, 'Safety and Privacy in Immersive Extended Reality: An Analysis and Policy Recommendations' (27 September 2023) <<https://papers.ssrn.com/abstract=4585963>> accessed 22 May 2024

How the Code of Conduct for Virtual Experiences (CCVE) Applies to Members-Only Worlds | Meta Store' <<https://www.meta.com/help/quest/articles/horizon/safety-and-privacy-in-horizon-worlds/code-of-conduct-members-only-worlds/>> accessed 3 June 2024

Hsu R, 'Meet the New 'verse, Same as the Old 'verse: Moderating the "Metaverse"' (Georgetown Law Technology Review, 2 May 2022) <<https://georgetownlawtechreview.org/meet-the-new-verse-same-as-the-old-verse-moderating-the-metaverse/GLTR-05-2022/>> accessed 26 January 2023

'Integration of Sensing, Communication, and Computing for Metaverse: A Survey | ACM Computing Surveys' <https://dl.acm.org/doi/full/10.1145/3659946?casa_token=I03Yt1MFGf4AAAAA%3AS4BUf1FV0b2M5G_Cpls46AzKXT3CXupUEtkDiuD9hWtia2T9m2VhBDMRO0gwWQBEDQ89uIAjXev6mA> accessed 31 May 2024

Isaac M, 'Facebook Renames Itself Meta' The New York Times (28 October 2021) <<https://www.nytimes.com/2021/10/28/technology/facebook-meta-name-change.html>> accessed 22 May 2024

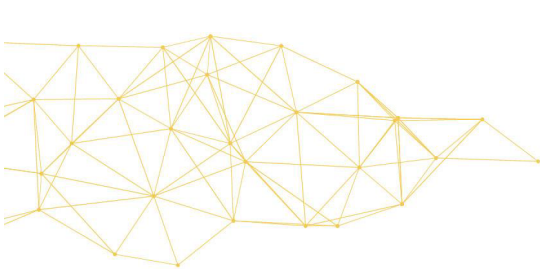
Jonniaux A, 'Horizon Worlds: Meta lance son monde en réalité virtuelle' (Journal du Geek, 13 December 2021) <<https://www.journaldugeek.com/2021/12/13/horizon-worlds-meta-lance-son-monde-en-realite-virtuelle/>> accessed 22 May 2024

Kettemann M, Müller M and Böck C, 'Regulatory Approaches to Immersive Worlds: An Introduction to Metaverse Regulation' (Project Immersive Democracy, 25 September 2023) <<https://www.metaverse-forschung.de/en/2023/09/25/963/>> accessed 28 May 2024

Kinikoglu B, 'Liabilities of Virtual World Developers as Intermediary Service Providers: The Case of Second Life' (2023) 13 Queen Mary Journal of Intellectual Property 121

Krack N, 'Algorithmic Systems: How Should DSA Risk Assessments Be Conducted?' (AI4media, 21 November 2023) <<https://www.ai4media.eu/algorithmic-systems-how-should-dsa-risk-assessments-be-conducted/>> accessed 24 May 2024

Krack N, Dutkiewicz L and Yildirim EO, 'AI4Media Report on Policy for Content Moderation (D6.2)' (2023) <<https://www.ai4media.eu/reports/report-on-policy-for-content-moderation-d6-2/>> accessed 29 September 2023



Lean Lau P, '3 Issues to Address before We Dive into the Metaverse' (World Economic Forum, 7 February 2022) <<https://www.weforum.org/agenda/2022/02/metaverse-legal-issues/>> accessed 28 May 2024

Leenes R and Lucivero F, 'Privacy in the Metaverse: Regulatory Challenges' (2018) 18 Journal of Virtual Worlds Research

Linden Research Inc v Greenzilla Kft. [2012] WL 123912, US Dist LEXIS 4569

Meta, 'Keeping People Safe in VR and Beyond' (25 February 2022) <<https://about.fb.com/news/2022/02/keeping-people-safe-in-vr-and-beyond/>> accessed 22 May 2024

Milgram P and Kishino F, 'A Taxonomy of Mixed Reality Visual Displays' (1994) IEICE Transactions on Information and Systems 1321

Mongeon M, '#MeToo in the Metaverse: Sexual Harassment in the Age of Virtual Reality' (2019) 26 Michigan Technology Law Review 253

OECD, 'Artificial Intelligence and the Digital Economy: A Roadmap for Promoting Responsible Data Sharing' (OECD Digital Economy Papers, 6 February 2023) <https://www.oecd-ilibrary.org/science-and-technology/artificial-intelligence-and-the-digital-economy_5e1d7d0c-en> accessed 24 May 2024

Papargyris M and others, 'Measuring Interactivity in Virtual Reality and Assessing the Predictive Power of Interactivity on User Engagement' (2023) 19 Journal of Virtual Worlds Research 1

Paternoster F and Dionisio JDN, 'Metaverse: A Systematic Literature Review of Current Concepts, Technologies, and Challenges' (2022) 7 IEEE Access 58364

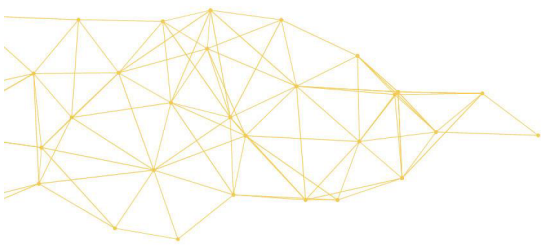
—, 'Metaverse: The Next Step in the Evolution of the Internet' (2022) 7 IEEE Access 55408

Richmond R, 'Second Life Teaches Hard Lessons as Virtual Realities Aim to Go Mainstream' The New York Times (8 January 2023) <<https://www.nytimes.com/2023/01/08/technology/second-life-metaverse-virtual-reality.html>> accessed 16 May 2024

Santos JC and others, 'A Survey on Security in Social Virtual Worlds' (2019) 40 ACM Computing Surveys 1

Schiavone S, 'The Digital Services Act's Approach to Platform Liability' (2022) 3 European Law Review 335

Singh G, Dey S and Patel A, 'The Metaverse: A Comprehensive Survey on the Virtual World' (2023) 14 IEEE Transactions on Computational Social Systems 665



Statt N, 'Facebook Is Shutting Down Its Second Life Clone' (The Verge, 25 May 2024) <<https://www.theverge.com/2024/5/25/23420208/facebook-second-life-clone-shut-down>> accessed 28 May 2024

Steiger B and Jannidis F, 'Trustworthy AI for the Metaverse' (2023) 6 Journal of Virtual Worlds Research 1

The Digital Services Act: Tackling Online Hate Speech' (Council of Europe, 18 March 2023) <<https://www.coe.int/en/web/commissioner/-/the-digital-services-act-tackling-online-hate-speech>> accessed 24 May 2024

The Information Commissioner's Office, 'Data Protection in the Metaverse: Guidance for Businesses and Individuals' (2022) <<https://ico.org.uk/for-organisations/data-protection-in-the-metaverse-guidance/>> accessed 28 May 2024

The Law Commission, 'The Metaverse: Law and Ethics in a Virtual World' (2023) <<https://www.lawcom.gov.uk/the-metaverse-law-and-ethics-in-a-virtual-world/>> accessed 28 May 2024

'Toxic Behavior in the Metaverse: Challenges and Solutions' (2023) 12 Journal of Virtual Worlds Research 1

Wauters E, 'Metaverse Moderation: Legal Challenges and Policy Responses' (2022) 14 International Journal of Law and Information Technology 98

Wong D, 'Legal Considerations for Content Moderation in the Metaverse' (2023) 24 Journal of Law and Technology 123

Xu Y, 'Metaverse Regulation: Legal Issues and Challenges' (2023) 3 Digital Law Journal 45.



MetaverseUA
Chair



Universitat d'Alacant
Universidad de Alicante

