IMPROBABLE

Regulating the Metaverse

A Review of Potential EU Policy Issues in Immersive Environments

Executive Summary

The EU continues to be a global frontrunner in the field of tech regulation, particularly in the emerging tech sector. In the letter of intent accompanying her annual State of the European Union address, European Commission President, Ursula von der Leyen, announced that the EU will seek to influence the regulation of global tech markets by evaluating "new digital opportunities and trends, such as the metaverse." A non-legislative "initiative on virtual worlds, such as the metaverse" is also included in the Commission's new Work Programme for 2023. This initiative will likely be the stepping-stone through which the Commission will showcase its current approach and future intent for this ecosystem. It will also mark the EU globally as one of the preeminent leaders in the regulation of the emerging tech sector, and its eventual laws may have repercussions across the virtual and physical worlds.

This paper assesses how the EU's existing tech regulations may be challenged or complemented by the emergence of the Metaverse in several key policy areas, including content moderation, platform liability, fundamental freedoms, user privacy, cybersecurity and child safety. Notably, this paper does not attempt to provide an exhaustive overview of every regulatory gap, particularly with respect to issues that are the prerogative of EU Member States. Nor does it focus on infrastructural elements of the Metaverse, including its potential economies or practical feasibility. Rather, it focuses on a few key legislative pillars with the aim to provide an initial review of the current state of play, general trends and suggest possible pathways for future development.

Ultimately, the paper concludes that a new regulatory approach will likely be needed to address the challenges and make the most of the opportunities posed by the Metaverse.

- **Content Moderation**: Moderating content in the Metaverse will be a challenge as users shift to more real-time behavioural interactions. Expecting Metaverse platforms to moderate behaviour using the same tools with which they have moderated content may be technically infeasible without risking users' fundamental freedoms.
- **Platform Liability**: Transactions conducted via decentralised blockchain infrastructure may make it difficult for Metaverse platforms to identify cybercriminals and respond to user complaints according to the current liability model. Liability may also be difficult to assign to users that participate in illegal behaviour in virtual spaces that may be leased/developed by a third-party or owned collectively.
- **Fundamental Freedoms**: Balancing users' fundamental freedoms of expression and information against the desire to protect consumers from illegal activity or harm will be increasingly complex in a hyper-real Metaverse in which users interact in real time.
- **User Privacy**: As the Metaverse is expected to encompass all aspects of our lives, the opportunities for data collection will extend beyond simple web browsing or social media engagement to include a multitude of personal activities, whether social, professional or recreational. Metaverse-enabling devices will also require a large amount of personal data to deliver immersive experiences. Helping users obtain more visibility on these data transfers so that they may give informed consent without compromising their privacy will likely remain an ongoing political and educational challenge.
- **Cybersecurity**: The Metaverse will give cybercriminals access to advanced, hyper-real technologies that could create new avenues for cybercrime. Increasing the resilience of digital infrastructures and educating users of their online risks will be essential to mitigate this risk.
- **Child safety**: Children will be able to experience new educational experiences through the Metaverse but may also encounter risks to their safety including bullying, harassment,

grooming, violence and exposure to sexually explicit material. Safeguarding children's right to privacy while keeping them safe from harm has already proven to be a contentious issue – and will likely continue to be so.

No matter the challenges, it is important to recall that the Metaverse also has the potential for substantial good, creating an entirely new economic space and introducing new forms of digital ownership and content creation, as well as considerable advancements in health, education, sustainability, productivity and entertainment. Policymakers have an opportunity to utilise the full strength of the EU regulatory toolkit to facilitate the growth of the Metaverse in a way that encourages these multiple benefits while mitigating its potential risks. Working with industry partners and external experts may also help EU regulators develop laws with consumer and child safety at their heart, following the principles of privacy and safety by design. New working groups may also consider how compliance and enforcement may be challenged by the Metaverse and already start to develop solutions. Through a combination of co-regulation, self-regulation, performance-based regulation and regulatory sandboxes, the EU may start to define the policy norms that will govern the Metaverse around the world.

I: Introduction

"We will not witness a new Wild West or new private monopolies. We intend to shape from the outset the development of truly safe and thriving metaverses."

Thierry Breton, Commissioner for Internal Market, European Commission[1]

The EU's approach to tech regulation has and continues to set global norms. The 2016 General Data Protection Regulation (GDPR) has become a global standard for data protection and privacy, and the recently-adopted Digital Markets Act (DMA) and Digital Services Act (DSA) are likely to follow suit. At time of writing, the EU has also become a leader in the regulation of virtual assets, as it finalises negotiations on the Markets in Crypto-Assets (MiCA) Regulation and develops a raft of other regulatory frameworks for crypto markets. In the letter of intent accompanying her annual State of the European Union address, European Commission President, Ursula von der Leyen, announced that the EU will continue to influence the regulation of global tech markets by evaluating "new digital opportunities and trends, such as the metaverse."[2] An "initiative on virtual worlds, such as the metaverse" is also included in the Commission's Work Programme for 2023.[3] The EU will therefore likely be among the first regions to regulate the emerging sector known as the Metaverse, and its laws may have repercussions across the virtual and physical worlds.

Already, the Metaverse has generated significant interest and excitement around the world, with numerous analysts predicting it will be anywhere from a multi-billion to multi-trillion dollar opportunity within the decade.[i] The Metaverse is considered by many to be a key feature of the next iteration of the Internet, creating new social, educational and professional communities as well as new forms of digital ownership, micro-economies and content creation. However, there is risk associated with this substantial and expansive growth, particularly if the problems of the Internet today persist in the Metaverse.

[i] Bloomberg calculated that the global Metaverse revenue opportunity could approach USD 800 billion by 2024; Global Market Insights expects the Metaverse market to surpass USD 500 billion by 2028; P&S Intelligence forecasts that the revenue of the Metaverse market will be over USD 1500 billion by 2030; McKinsey estimates that the value of the Metaverse could reach USD 5 trillion by 2030; Citi predicts the Metaverse economy could be worth USD 13 trillion by 2030.

EU regulators have spent the past few decades creating laws to govern digital services. The laws have varied from the "light-touch" approach that largely characterised the era of techno-democratic optimism to more recently interventionist laws aimed at limiting a rising number of online inequities and societal harms. Although the EU's existing regulatory framework will apply to the Metaverse as it exists now,[ii] regulators around the world are starting to question whether new laws may be needed to govern it as it matures. In the US, for example, the Congressional Research Service recently prepared a report assessing key policy issues relating to the Metaverse[4] and earlier this year the UK's Competition and Markets Authority organised a symposium to evaluate its regulatory implications.[5] In the EU, policymakers have already advanced to the stage of integrating mention of the Metaverse into legislative drafts[iii] and are exploring its various opportunities and risks in a range of regulatory fields.[6] The question, therefore, is not if regulation will come, but when and in what form.

This paper will assess how the EU's existing tech regulations may be challenged or complemented by the emergence of the Metaverse. It will review some of the key themes that have motivated Internet regulation to date (including consumer and child protection, data privacy and cybersecurity) and consider what impact the Metaverse may have on them. This paper does not attempt to provide an exhaustive overview of every regulatory threat the Metaverse may pose or every regulatory solution the EU may employ. Rather, it focuses on a few key legislative pillars with the aim to provide an initial review of the current state of play and possible pathways for future development. In the succeeding sections, we review some of the policy areas where we expect regulation on the Metaverse to be introduced and consider what lessons EU policymakers have learned from the regulation of the Internet to date that they may bring forward with them into the Metaverse.

Defining the Metaverse

Before proceeding, it is necessary to first define what we mean when we write about the Metaverse. Although popularised by Facebook's name-change to Meta last year, the concept of an immersive, hyperreal, virtual reality space dates to the early twentieth century, while the term itself was coined thirty years ago by author Neal Stephenson in his 1992 novel, *Snow Crash*. Since then, definitions of the Metaverse have varied widely and occasionally contradicted each other. More often than not, this variation has been at least partly attributable to the fact that people interchangeably refer to the Metaverse both as it exists now (in a very limited form) and as what it might become in the next 10-15 years (at a considerably more advanced stage).

As the technology enabling the Metaverse is still nascent, and corporations are only just beginning to discuss the standards that may underlie it,[iv] it is not yet certain how the Metaverse may eventually develop. However, there is general agreement that the Metaverse will eventually give users a new sense of being physically present in virtual worlds by enabling new forms of interaction built on three key features: (1) an immersive, three-dimensional user experience, (2) real-time, persistent network access and (3) cross-platform interoperability.[7] While it may be possible to develop some of these features in isolation, combining them will still take years to achieve,[8] and even longer before the Metaverse may facilitate meaningful experiences in virtual worlds that are imbued with meaning by

[ii] Initially confirmed by the answer to a written question given by European Commissioner Thierry Breton to a Parliamentary question about the Metaverse.

[iii] Amendment 902 of the Artificial Intelligence Act, for example, introduces a new Article on "Metaverse environments"

[iv] In June 2022, a group of standards organisations and companies announced the launch of the Metaverse Standards Forum, whose stated goal is to develop interoperability standards needed to build the open metaverse. In July 2022, a group of Web 3.0 companies launched OMA3 (Open Metaverse Alliance) with the aim to build a community-run, decentralized, indexable and interoperable Metaverse.

society.[9] This paper therefore takes a theoretical stance toward the Metaverse, positing how current EU laws may apply to it as it develops, and suggesting where it may create new regulatory challenges.

There are two aspects in the above definition that we would like to highlight for the purposes of this report. First, when we write about the Metaverse, we are writing about three-dimensional virtual worlds. This means that instead of visiting separate webpages to find information, play games, consume entertainment or participate in digital communities, we will enter into more encompassing virtual spaces that may include sports[10] and entertainment[11] facilities, workplaces[12], retail centres[13], health[14], education[15] and any number of additional real-world services. This aspect is particularly significant when considering the adaptability of legislation that may apply to the Metaverse since we may anticipate a continued blurring of the traditional division between laws that are applicable in the physical world and those that apply to the digital space.

Second, data is expected to be interoperable across virtual worlds persistently and in real time. While this definition does not presume that the Metaverse will be built on top of decentralised platforms or the blockchain (both of which we will define further in the following section), it does anticipate the development of industry standards that will facilitate seamless and instantaneous interoperability, similar to the way that the voluntary and global adoption of the Internet Protocol Suite (TCP/IP) helped to enable the interoperable internet we use today.[16] It also presumes that we will be able to overcome considerable technological and infrastructural obstacles in order to facilitate the exchange of data at such high speeds that users experience the virtual world in real time (the computational requirements alone are estimated to demand an efficiency improvement of over 1000x today's levels).[17] The significant quantities of data involved in this process and the environmental risks of transferring such data persistently may itself create new regulatory challenges.

The remainder of this paper will proceed as follows. In **Section II** we offer a brief explanation of the infrastructure that may underlie the Metaverse and the possible challenges it may present, particularly if built upon decentralised models. **Section III** begins with a **Spotlight** on the unique challenge of content moderation in the Metaverse. It continues with a review of other specific regulatory issues, based on a survey of key legislative files that we have selected to represent how the Internet has been regulated to date in the EU. We conclude with **Section IV**, in which we summarise our key considerations and outline the policy milestones that may lead to future regulation of the Metaverse.

II: The transition from Web 2.0 to Web 3.0

One of the reasons the Metaverse has attracted so much attention recently is due to technological advances that have started to realise the possibility of Web 3.0. Web 3.0, or simply Web3, is so named because it is considered the next iteration of the Internet, coming after Web1, in which users consumed content on read-only, static, browser-based web pages and Web2, considered the participatory web characterised by the rise of social media. Unlike Web1, Web2 is read-write, utilising more interactive elements, notably user-generated content, that may be accessed through both web pages and mobile applications ("apps").

Although the user-generated content of Web2 has given people unprecedented opportunities for self-expression and free speech, it has also led to the proliferation of online harms, such as mis- or disinformation, online harassment and hate speech. In response to these harms, online platforms have deployed terms of service, community guidelines and content moderation tools. EU regulatory efforts have also obliged online platforms to develop new solutions. However, diverging standards and splintered laws have created legal uncertainty on how platforms should respond to easily identifiable unlawful content.[v] In addition, other forms of content may be more difficult to define or identify accurately. In such cases, platforms have pursued industry-led initiatives[18] to help them judge whether such content violates platform rules (rather than related laws) and what the consequences for sharing such content may be. The centralised nature of most of these Web2 platforms allows them to manage content by removing it, barring access to the users who share it or by making other unilateral changes to the digital spaces they control.[vi]

Despite the safeguards they may offer in terms of security, centralised platforms have come under criticism in recent years for the uneven way that content moderation and user account disbarment decisions have been applied. In the EU especially, these companies have come under additional scrutiny for the way they handle and monetise user data.[19] While Web2 therefore facilitated the explosive growth of creator content, it also indirectly created the ad-driven data economy, driving a flood of free entertainment to consumers, while also creating data privacy risks.

Web3 and Blockchain

Conversely, Web3 philosophers and architects envisage a new model of data ownership online that lets creators retain intellectual property (IP) rights to their own artistic creations, while consumers maintain and have the option to conceal their identities, financial information, browsing history, social connections and other demographic data from third parties. This is because the substrate of Web3 is built on decentralised blockchains, rather than centralised platforms that are financed and controlled by private, corporate entities. Unlike online platforms, blockchains generally function as immutable, transparent and distributed ledgers that enable peer-to-peer interactions, without the need for oversight by a central authority.[20] Transactions recorded on a blockchain are both open and secure; once written they cannot be deleted, and any attempt to tamper with them will likely fail. In contradiction to the Web2 model where users may not always fully or inherently be aware of what personal information they are sharing, the Web3 model gives users the ability to track, control and profit off their own data using a well-guarded private key across the blockchain, restricting or permitting access at their personal discretion.[21]

Web3 also has the potential to create new governance communities for online platforms, including in the Metaverse. These communities are notably known as decentralised autonomous organisations (DAOs), so named because they are built on smart contracts embedded on the blockchain that are designed to execute autonomously.[22] DAOs offer users an ownership stake in Web3 platforms, giving them the chance to participate in governance decisions and receive a share of revenues in return for their engagement.

Web3 also creates new possibilities when it comes to the ownership and monetisation of virtual assets in the Metaverse. Non-fungible tokens or "NFTs", for example, are essentially units of data that are represented by a token on an encrypted blockchain. Unlike other digital assets, such as a .jpg image, each NFT represents an entitlement of ownership, embodied by a unique blockchain address that cannot be replicated through traditional "copy and paste" functions. The representative token of an NFT may moreover appear to be anything from a piece of digital artwork to accessories or clothing for user's avatars to an access pass for unique digital experiences to other virtual goods. As NFTs may be minted by anyone, they offer new possibilities for self-employed artists and other content creators to

[v] The Digital Services Act, for example, includes an obligation to put in place notice and action mechanisms, which allow users to flag potentially illegal content hosted on an online platform.
[vi] Including fact-check labels or violent content warnings.

design and monetise digital assets while also bringing more peace to mind to the users spending real money to purchase those digital goods.[23]

Blockchain use in this type of Web3 construct therefore offers the potential for users to exercise ownership over digital assets. However, the decentralised nature of Web3 also means that users may have fewer corrective actions available to them if something goes wrong.[24] As we will detail further in the following section, the lack of a central authority has already created new challenges when it comes to maintaining user safety and retrieving stolen (virtual) property on Metaverse platforms today. Meaningful digital ownership may therefore be considered to come at the cost of regulatory oversight and consumer protections.

Web3 and financial services

Web3 not only creates new ownership possibilities, but does so by introducing new financial models that replicate those in the physical world. The economies of the Metaverse are built around token exchanges and cryptocurrencies, which are bought and sold on blockchain. This decentralisation of financial services, e.g., payments, exchange, lending, is intrinsically linked to the rise of Web3, bringing new disintermediation possibilities. In this new digital space, cryptocurrencies are most often used for payments, peer-to-peer transactions, and the execution of governance rights through utility tokens and stablecoins.

Utility tokens serve a particular purpose, for example to redeem a special service (i.e. to purchase unique digital assets) or receive preferential treatment for services (i.e. governance rights on a DAO). On the other hand, stablecoins generate price stability as they are backed by real-world assets. To get stablecoins, users need to lock collateral in decentralised protocols, in a process akin to borrowing. The issuance and transfer of stablecoins are, at present, dominated by private entities, but central banks globally are advancing in the development of so-called Central Bank Digital Currencies (CBDCs). Privately-issued stablecoins and CBDCs are similar in that their value is pegged to a fiat currency. While industry debates on this are ongoing, economists broadly agree that only stablecoins can be a credible store of value and means of exchange i.e. the “money” of the Metaverse.

There are a wide variety of design and risk-management choices being made in the way a currency peg is maintained, for example in the reserves held against the stablecoins issued, the technology used for issuance and transfer and the interoperability between them. In the exchange and transfer of tokens, be they stable or not, fungible or not, there is also money laundering risk. Thus, these new types of financial services are being increasingly regulated for the purposes of financial stability, consumer protection and anti-money laundering. The payments use case, from Beijing to Brussels, has been highest on the regulatory agenda; lending has been less comprehensively addressed, though it faces rising regulatory concerns.

Will the Metaverse be centralised or decentralised?

It is likely that some of the most attractive aspects of Web3, such as the possibility of real data ownership/control across different virtual spaces, independence from the unilateral decisions of Web2 platform owners, and the opportunities it offers to reinforce trust in governance may encourage industry to pursue a decentralised Metaverse.[vii] However, there is nothing that explicitly ties the Metaverse as we conceptualise it in this paper with Web3, blockchain or decentralisation.

[vii] The EPRS briefing, “Metaverse: Opportunities, risks and policy implications,” recommends exploring the decentralised Metaverse model further in order to better address data protection issues that are difficult to resolved in centralised models (p. 6).

Currently, there are a number of self-styled Metaverse platforms, some of which are centralised, such as Horizon Worlds and Roblox, and some of which pursue a more decentralised approach. Whether there is eventually one decentralised Metaverse, one centralised Metaverse or several platforms belonging to a Metaverse, some of which are centralised and some of which are decentralised, will impact which policy issues are likely to have the greatest impact on businesses and consumers. For example, if one or only a couple centralised Metaverse platforms emerge that fail to interoperate with each other or that utilise conglomerate strategies, they may give rise to the same competition and antitrust concerns that recently inspired EU policymakers to define new rules about digital "gatekeepers" in the DMA.

As we presume that a future Metaverse will be at least partially built in Web3, the remainder of this report focuses primarily on the regulatory challenges the Metaverse may pose if it is decentralised.

III: Review of regulatory challenges

In this section, we review some of the specific regulatory challenges the EU has faced as the Internet has developed, beginning with a Spotlight on the unique challenge of moderating content in the Metaverse.

Spotlight: The unique challenge of moderating content in the Metaverse

As touched on briefly in the preceding section, content moderation in Web2 is complex. Even purely illegal content may be difficult for online platforms to expeditiously identify and remove. Negotiating additional considerations around harmful content that is not necessarily illegal but opposed to a platform's terms of service adds an additional layer of complexity to this process. And all of this is increasingly challenged by the advent of new forms of content, including real-time audio/video communications and synthetic media.

Already, Web2 platforms struggle to take down illegal content produced in real time. Illegal streams of live sports, for example, have become so problematic that last year, the European Parliament proposed new rules to tackle the online piracy of live sporting events.[25] As opposed to text-based interactions, where a literal text trail persists after the engagement takes place that may be followed by moderators, or recorded audio/video footage that may be scanned by AI technologies,[26] the ephemeral nature of real-time content makes its identification and take-down substantially more onerous.

The Metaverse will not only multiply the frequency of real-time content generation, but shift communication that is currently text-based – on social media platforms, web forums or chat rooms, for example – into behavioural interactions (with both verbal and non-verbal elements). Protecting users without infringing on their fundamental rights in such situations will be a significant technical challenge. According to Andrew Bosworth, Chief Technology Officer at Meta, such moderation "at any meaningful scale is practically impossible."[27] In addition, new forms of interaction in the Metaverse may require platforms to develop new standards for what is and is not socially acceptable behaviour in virtual environments.

Today, self-styled Metaverse platforms are addressing this content moderation challenge. Consider, for example, the experience Aaron Mak describes as a virtual bouncer on Microsoft's social platform, AltSpaceVR. Mak talks about seeing a male avatar "repeatedly bouncing back and forth, right into a woman's face" – an action that may either be a greeting in VR or a form of sexual harassment.[28] Although Mak and his fellow moderators ultimately tell the male avatar to stop his behaviour, Mak comments that a lot of Metaverse moderating involves "a delicate dance of guessing at motivations and making quick judgement calls."[29] As the Metaverse evolves, the relative speed and frequency of these interactions will likely increase, demanding increasingly sophisticated behaviour moderation tools, including perhaps advanced automated filter technologies and other AI solutions, in addition to new community standards and other user controls. As we explore further in this section, all of these solutions may continue to create new challenges when it comes to balancing user safety with free speech and privacy objectives.

The remainder of this section identifies several other policy issues that may prove especially challenging in the Metaverse, including platform liability, fundamental freedoms, user privacy, cybersecurity and child safety. For each issue, we highlight the lessons policymakers appear to have learned from regulating Web2 and suggest how these lessons might be applied to the Metaverse.

As discussed in the Introduction, it is important to note that this list of regulatory issues is not exhaustive. Notably, it focuses purely on policies relating to Metaverse content, rather than those that may relate to the economic infrastructure underlying the Metaverse. Apart from other topics that may be dealt with at EU level, there are also a range of issues that are the prerogative of EU Member States such as health and security. In such circumstances, the EU can provide a degree of guidance to Member States, but may not intervene directly in national laws. For example, new use-cases around national defence, such as immersive training drills or the possibility for new forms of political espionage or voter manipulation may emerge that would benefit from EU level coordination but be the prerogative of local regulators to legislate. The taxation of crypto-assets is also an ongoing policy concern. Although the EU plays an important role in coordinating tax policies between EU Member States, it does not currently have the authority to set those policies. The Metaverse may also prompt non-regulatory reactions at both EU and national level, including changes to competition and antitrust models. The EU and its Member States' eventual response to these issues may have both economic and geopolitical consequences, a subject worth exploring separately from this paper.

We follow the same general format for each of the following regulatory challenges: we start with a brief description of the issue in the Web2 space and the EU's response to date. We then suggest how the Metaverse may create new concerns and what some possible regulatory responses may be.

Liability

The Metaverse will introduce several new legal challenges, including who or what should be held responsible if something goes wrong. Establishing liability is not only essential when it comes to the payment of damages but is important to ensure consumers feel secure and safe in their online interactions.

Liability in Web2

For the majority of Web2, regulators avoided making centralised operators responsible for illegal content hosted on their platforms. One of the earliest pieces of tech regulation in the EU, for example, was the 2000 eCommerce Directive (ECD), which established the "liability exemption," setting the standard that information society service providers may not be held liable for third party illegal content hosted on or passing through their servers unless they have actual knowledge of illegal activity /information or they have modified illegal information during its transmission.[30]

As the Internet developed, EU regulators started to demand that online platforms take more responsibility for identifying and removing illegal user-generated content more rapidly. The EU's Code of Conduct on Countering Illegal Hate Speech online, for example, recommends that IT companies aim to review the majority of valid notifications for the removal of illegal hate speech in less than 24 hours.[31] The DSA, successor to the ECD, echoes this benchmark, and additionally stresses that other types of content may require even shorter timelines, depending on the "facts, circumstances and types of illegal content at hand."[32] Not only have Web2 laws in the EU therefore gradually made private entities increasingly responsible for the identification and rapid removal of illegal content, but for judging what types of content may threaten users with more immediate harm.

Crucially, both the ECD and the DSA presume that an online platform will have the capacity to remove third-party content if it is found to be in conflict with the law. A scenario in which an online platform may be incapable of responding to user concerns about content it hosts is inconceivable in a Web2 space. Therefore, failure to remove illegal content that has been flagged or that the platform may reasonably know to exist exposes a platform to potential fines and legal repercussions under EU law.

Liability in the Metaverse

As mentioned in the previous section, the Web3 model on which the Metaverse may be at least partially built creates new problems when it comes to ascribing responsibility and liability to online intermediation services. Although blockchain creates new ownership possibilities over digital assets, data and self-sovereign identities, it also weakens the protections that centralised platforms may otherwise offer to users. This is particularly evident when users become victims of cybercrime, especially malicious attempts to steal data stored on a blockchain.

There have already been numerous cases of users falling prey to scams that have stolen millions of euros worth of virtual assets. So far, most of these have happened in a Web2 context, i.e. users go to websites they believe to be legitimate that prompt them to enter the login credentials for their crypto wallets, which are then stolen (and potentially sold) by cybercriminals. This problem may only intensify in a Web3 space, especially if a decentralised ecosystem makes it more difficult to track down lost funds. The Metaverse may therefore challenge the Web2 model of liability in which centralised platforms may be held legally responsible for failing to respond to illegal user activity if the infrastructure itself prevents them from doing so.

The existing liability model may also be challenged by the virtual real estate possibilities of the Metaverse. Currently, self-styled Metaverse platforms like the Sandbox offer users and commercial entities the opportunity to purchase virtual plots of land on which they may develop Metaverse experiences. Plots of land may also be purchased by one company and rented out to others.[33] If illegal activity transpires in such spaces, it is unclear whether the platforms, landowners, experience developers or others should be held responsible for that behaviour.

Lessons learned

One response to a potential decrease or reassessment of platform responsibility is an increase in user responsibility, which will require more advanced digital skills from EU consumers. The EU has already launched several initiatives to increase consumers' digital literacy. The EU's Digital Education Action Plan (2021-2027), for example, aims to ensure that 70% of those aged 16-74 have at least basic digital skills by 2025.[34] Enhancing user awareness of cybersecurity threats may make them less likely to fall victim to scams and better equipped to be liable for their own actions in the Metaverse.

Another alternative may be to make those individuals or platforms who profit most from a particular activity in the Metaverse subject to regulation that imposes a certain degree of accountability as a mediator. Standards that have already been introduced in the Web2 space, such as Know-Your-Business-Customer will also likely persist, or new identification services may be required for commercial entities to operate in the Metaverse.

EU policymakers are also in the process of reassessing how they have ascribed liability more generally. Recently, the Commission adopted two new proposals to revise the EU's Product Liability Directive and introduce new laws around Artificial Intelligence (AI) liability to better address the challenges that arise when liability rules are applied to emerging technologies and connected devices.[35] Negotiations on these files may prompt policymakers to consider whether existing liability structures continue to be technically feasible in a Web3 reality.

Jurisdiction in the decentralised Metaverse

Jurisdiction is an additional challenge when it comes to ascribing liability in the Metaverse. Apart from the liability exemption, the ECD developed the country-of-origin principle, which essentially requires companies to follow the rules of the country in which they are established, rather than the varying laws of each individual Member State.[36] If a company is established outside of the EU, the DSA and other recent pieces of legislation have clarified that it must follow the laws of the country in which its EU-based legal representative is registered.[37] These laws are crucial for the issue of content moderation as they determine what behaviour is illegal in each Member State and is therefore subject to removal under the parameters of the DSA and related laws.[viii] However, determining jurisdiction in a decentralised Metaverse may be particularly challenging as it could apply, for example, to the location of a user, avatar, or relevant servers.[38] Judging whether a Metaverse platform should be held liable for user-generated content and responsible for its removal may therefore have this additional level of complexity in decentralised realities.

Fundamental rights

Although there are several fundamental rights at issue when it comes to tech regulation, our central concern in this section is the interaction between laws that aim to protect consumers or businesses from either illegal content or IP theft and Article 11 of the Charter of Fundamental Rights of the EU, which grants freedom of expression and information to all peoples of Europe.[39]

Fundamental rights in Web2

The tension between protecting consumers while preserving their fundamental right to express themselves freely is a key theme that has characterised the regulation of Web2 in the EU. The central issue is the risk of over-censorship through efforts to either keep consumers safe from illegal or harmful content or to preserve the integrity of IP. One of the most contentious debates on the EU's Copyright Directive, for example, concerned the potential impact of automated filter technology on

[viii] Consider, for example, that at time of writing Holocaust denial is illegal in Germany but not in Spain or that same-sex marriage is illegal in Poland but not in France.

fundamental rights.[ix] On the one hand, automated filters make it possible to swiftly take down content that defies national laws or copyright protections. On the other hand, stakeholders claim that the current lack of sophistication in filter technology means that filters often remove content that does not infringe on copyright protections, such as reports, reviews or parodies; in other words, content that should be protected under the EU's Charter of Fundamental Rights.[40]

This same argument has resurfaced in numerous legislative proposals, including the proposal for a regulation on Terrorist Content Online (TCO), where the desire to protect consumers from radicalisation and the celebration of terrorist acts had to be balanced against the concern that automatic filters could limit the freedoms EU citizens should otherwise be able to enjoy.[41] It was also a key debate in negotiations around the DSA, particularly when it came to the question of whether the DSA should strengthen the obligation for platforms to respond to illegal content only or both illegal and "harmful" content.[42]

Fundamental rights in the Metaverse

Information that may harm consumers in Web2 will have greater potential to damage consumers in the Metaverse. Instead of an advertisement sponsored by a terrorist agency or a message sent through a social networking site, terrorist recruiters may, for example, represent themselves as relatable avatars in any number of virtual contexts. Moreover, the increasing sophistication of deepfake technology may give harmful actors the opportunity to represent themselves as trusted or respected individuals in increasingly immersive and realistic ways. These technologies may proliferate the quantity of misinformation and disinformation that users are exposed to, in addition to illegal content. Maintaining users' freedoms to represent themselves and interact with who or what they choose without fear of constant surveillance in the Metaverse will likely be increasingly difficult to balance against the desire to keep them safe from harm.

IP may also be difficult to safeguard as automated filter technologies will need to become sophisticated enough to correctly decipher the context of behaviours happening in real time across diverse Metaverse realities. As explored in the Spotlight section above, even human moderators struggle to interpret context and intent in such spaces.

Lessons learned

EU policymakers are currently trying to navigate the balance between freedom and protection in an array of legislative texts, most recently through ongoing negotiations on the AI Act. Among other issues, the proposal for an AI Act prompts policymakers to consider which uses of AI should be prohibited in all circumstances due to the fundamental risks they pose to EU citizens. Despite its potential dangers, experts insist that deepfake and other synthetic media technologies should not be prohibited outright as their common function is banal. Henry Ajder, a researcher specialising on the malicious use of deepfakes, has already pointed out the difficulty in banning such technology:

> "If you ban synthetic media you ban all Instagram filters, you ban the computational photography on your camera and your smartphone, you ban the dinosaurs in Jurassic Park. It's not going away – the future will be synthesised and there's no sugarcoating the challenges ahead."[43]

[ix] In May 2019, Poland brought a legal challenge against the Copyright Directive to the Court of Justice of the European Union, claiming that it infringed upon the right to freedom of expression and information guaranteed in Article 11 of the Charter (see paragraph 23 of the Court Judgment).

If outright bans are inappropriate, EU policymakers will likely task Metaverse platforms with finding a way to moderate both content and behaviour perpetuated by users, without compromising their fundamental rights. This may demand a revision to such texts as the Copyright Directive, TCO or DSA to adapt them to new technological realities, or it may require entirely new laws to ensure that users who behave inappropriately in the Metaverse suffer the same consequences for those behaviours as they would in the real world.

User Privacy

Article 8 of the European Convention of Human Rights enshrines the right to respect for private and family life, home and correspondence.[44] It is essentially a right to privacy, and the arbitrary or unjust interference in one's private life by public authorities. Article 8 of the EU Charter of Fundamental Rights simultaneously grants EU citizens protection over their personal data from both public and private entities.[45] Despite the importance of privacy in the EU, Web2 technologies have already challenged public guarantees of it, and the Metaverse has the potential to introduce new surveillance threats.

User Privacy in Web2

In addition to the liability exemption and country-of-origin principle, the ECD also developed a prohibition on general monitoring.[46] This principle aimed to prohibit platforms from monitoring all communication between users (without due cause) in order to preserve their fundamental right to privacy.

Over time, AI technologies, such as automated filters, gave centralised Web2 platforms the ability to monitor user-generated content for illegal phrases without reading each private message passing through their servers. Though not always efficient, these technologies were developed to protect consumers *en masse* without restricting their rights.

However, other surveillance technologies developed during Web2 served different commercial or, at times, criminal purposes. Tracking a user's activity through single sign-in methods, for example, gave Web2 platforms and their commercial partners the ability to tailor advertisements based on a user's interests. This has been particularly beneficial for several actors within the digital economy, including advertisers[47], news media[48], retailers[49] and SMEs[50]. However, this practice has recently come under criticism from consumer and digital rights groups, as well as centre-left politicians in the European Parliament. Motions to ban targeted advertising have emerged in several recent legislative proposals, including the DSA, DMA, AI Act and the regulation on political advertising. Tracking a user's clicks and keystrokes have also been used by criminal actors seeking to record and steal passcodes and other sensitive data.[51] Despite legal guarantees, the Web2 space has therefore already challenged users' right to privacy.

User Privacy in the Metaverse

> *What are the five most important aspects of VR technology? The punch line: Tracking. Tracking. Tracking. Tracking. Tracking.*
>
> *Jeremy Bailsenson, Virtual Human Interaction Lab, Stanford University*[52]

The Metaverse presents at least two additional challenges to the Web2 model of user privacy. First, content moderation will become increasingly difficult with the shift from text-based to behavioural interactions. Moderation tools capable of registering and evaluating these Metaversal interactions may demand enhanced surveillance over all of an individual's interactions online or offline in connected spaces. Given that the Metaverse is expected to extend to all corners of our lives, this means not only enhanced surveillance over social media correspondence, but in Metaverse workplaces, retail or entertainment experiences and in connected homes.

This last aspect points to the second significant challenge to user privacy posed by the Metaverse. To deliver immersive experiences, Metaverse-enabling devices require a large amount of information about individuals and their surroundings.[53] According to one report, twenty minutes of VR use can generate approximately two million data points, in addition to recordings of body language.[54] This information may be collected through different applications and tools that derive biometric data through motion sensors or facial scans and may include data linked to posture, gait, gestures, eye gaze and facial expressions.[55] Some of the technologies capable of processing this data are already in circulation, while others are still in development; Meta, for example, has already patented technology to build eye and facial expression tracking into the headsets it is developing for use in the Metaverse.[56]

The sheer quantity of personal information involved in delivering, moderating and engaging in immersive experiences creates new cybersecurity risks (which we detail further in the following section) and may involve sharing and exposing more data with commercial entities, especially in a centralised Metaverse.

Lessons learned

EU policymakers have recognised the importance and value of data, referring to it as "the new oil" on several occasions.[57] As such, regulatory attention continues to focus on the question of securing user data, ensuring users are aware when data is being collected about them and how they may give or withdraw consent to have their movements and interests tracked online.[x] Recently, the European Parliament Research Service also started to explore the opportunities the Web3 Metaverse may be able to offer to consumers when it comes to safeguarding their data.[58] Yet, it remains to be seen whether existing regulatory solutions are still relevant or effective in the Metaverse. The e-Privacy Directive (EPD), for example, obliges companies to obtain user consent before processing any data collected through cookies.[xi] However, cookie use, as well as the method for collecting user consent around it, may need to be rethought for the Metaverse. User experience may be considerably impaired if users are expected to read a wall of text each time they try to enter a new virtual world; inevitably, new standards will need to be developed for common motions to indicate acceptance or rejection of terms in immersive digital spaces.[xii]

Cybersecurity

Research shows that cybersecurity threats and cybercrimes are rapidly and dramatically increasing, rising by 50% or more year on year.[59] These cybercrimes are not restricted to commercial targets or financial institutions, but impact key industries and ordinary consumers. Despite progress, cybersecurity has remained a challenge throughout the Web2 era. The Metaverse will likely increase the potential damage cybercriminals may cause to users due to its extensive breadth and the significant data collection generated through the provision of immersive experiences.

[x] Already back in 2016, the GDPR's Article 5 strengthened the Transparency Principle, giving a data subject the right to know how his or her personal data is processed and for what purpose.

[xi] For more information on cookies, please visit https://gdpr.eu/cookies/.

[xii] Such standards already exist in the Web2 space. For example, consider on touch devices that it is standard to "pinch to zoom" or "slide up to scroll down." 3D spaces will require similar new standards.

Cybersecurity in Web2

Cybercrime is defined in the EU as the output of criminal acts perpetrated online through the use of electronic communications networks and information systems.[60] It may be generally broken down into three separate categories: (1) crimes that are unique to the Internet (e.g. attacks against information systems or phishing), (2) online fraud or forgery and (3) illegal online content (including child sexual abuse material, hate speech, racism, xenophobia, terrorism or glorification of violence).[61]

Web2 solutions to cybercrime targeting individuals have centred around the development of tools to inform users when they may have been exposed to malicious activity and to remove malicious content, such as virus scanner software. Other online tools, such as automatic prompts to generate stronger passwords or the obligation to engage in multi-factor or passwordless authentication to access certain online services, have also helped protect consumers from Web2 cybersecurity risks. Enhancing the digital education of users has also been key to furthering cybersecurity goals, with some corporations incorporating basic cybersecurity training into their onboarding processes.

The EU has also developed some frameworks to help companies better prevent and respond to cybersecurity breaches, such as the Directive on the Security of Network and Information Systems (NIS),[xiii] which aims to improve cybersecurity incident reporting, the Digital Operational Resilience Act (DORA)[xiv], which harmonises digital resilience in the EU for financial services firms, and the non-legislative EU Cybersecurity Strategy, which aims to build collective capacity to respond to major cyberattacks.[62]

In spite of these developments, securing Web2 spaces has remained a constant challenge for both enterprises and individuals – and the Metaverse only intensifies these risks.

Cybersecurity in the Metaverse

In addition to creating new risks for user privacy, Web3 technologies may also create new avenues for cybersecurity threats. Connected devices, for example, could be targeted by malicious actors. Stolen information could then be used by cybercriminals to steal a person's online or offline identity. Moreover, identity theft in the Metaverse may not only result in stolen property, goods or assets. Rather, it may lead to avatar impersonations that may not only usher in a new era of fake news but could ruin a user's offline relationships or reputation.[63] Last year, MIT Technology Review reported that between 90% and 95% of all online deepfake videos are nonconsensual pornography, in which deepfake technology is used to swap uploaded faces onto the bodies of pornography actors.[64] Currently, these face-swaps are usually crude and obviously fake, but as the technology develops, online identity theft could have increasingly disastrous results.

Apart from pornography, cybercriminals may also impersonate avatars for other crimes. They may, for instance, represent themselves as the avatar of a virtual bank teller asking for users' personal information[65] or they might impersonate someone from the HR department in a users' Metaversal workplace. Trying to determine in which contexts such deceptions are more or less harmful for users and may require more rapid or thoughtful reactions will become increasingly challenging for commercial entities.

[xiii] A legislative proposal for a revised NIS Directive, known as the NIS2, was presented in December 2020. A political agreement was reached on the file in May 2022.

[xiv] A legislative proposal for DORA was presented in September 2021. A political agreement was reached on the file in May 2022.

There are also hardware cybersecurity risks associated with the Metaverse as haptic suits, gloves and other devices could be manipulated to cause users' physical harm.

Lessons learned

No matter how sophisticated the protections may be, it is widely accepted that new security threats will always develop. The EU's regulatory focus will therefore likely remain on prevention and response, while encouraging the development of new protective measures from industry.

One of the most notable pieces of recent legislation dealing with cybersecurity is the Cyber Resilience Act, a new proposal which aims to introduce common cybersecurity standards for connected devices and other digital products.[66] It is likely that these standards will apply to connected devices that are already in circulation, as well as those in development. The EU's General Product Safety Directive is also in the process of being revised into a Regulation (the "GPSR") to better address the challenges brought on by the advent of AI-powered products and connected devices.[67]

The EU may also develop new tools, such as enhanced European Digital Identity Wallets, to help consumers better protect their identities. Currently, the European Commission is in the process of reviewing the regulation on electronic identification and trust services (the eIDAS Regulation).[68] One of the policy options being considered in this review is the creation of a user-centric Personal Digital Identity Wallet (EUeID) that will give EU citizens the possibility to maintain their own self-sovereign identities, potentially through decentralised solutions.[69]

However, none of these tools is aimed to address specific cybersecurity challenges within the Metaverse itself, such as protecting avatar integrity, managing the relationship between the Metaverse and the dark web or evaluating the real-world impact of crimes committed in the Metaverse (including their emotional impact). There is therefore a gap that will likely need to be filled by either policymakers, industry or the full Metaverse community when it comes to protecting users from cybersecurity threats.

Anonymity, identity and financial crime

A core feature of crypto assets and Web 3.0 is the perceived anonymity and privacy offered by these new technologies. Although they offer some benefits, the anonymity and nebulous identities linked to crypto-currencies are also used by criminals for broad money laundering purposes, including the trade of illicit goods and services, fraud and a growing number of for-profit schemes relating to child sexual abuse material (CSAM).[70]

European regulators have taken a keen interest in updating their frameworks to introduce specific regulations to ensure the identification of transactions and individuals, such as the creation of European Digital Identity Wallets. The recent changes to the Transfer of Funds Regulation (TOFR), part of the Commission's 2021 Anti-Money Laundering Package, aim to bring the current information transfer regime in line with technological developments. All crypto transactions in the bloc will be required to carry identifying data, with no minimum transaction threshold. Exemptions will be carved out for transfers between un-hosted wallets – that is, wallets kept outside of an exchange.[71]

The European Commission has also been exploring the use of Self-Sustaining Identities (SSI) for the past few years, promoting it as a "new identity model, that has the potential to enhance the way citizens manage their digital identity, as well as the ability to offer public administrations new ways of authenticate citizens and offer better public services" – aiming to ensure transparency through a one stop shop for digital identity– notably in the crypto sphere.[72]

Child safety

The Metaverse creates exciting new opportunities for children, not only for gaming and entertainment, but for immersive education. Through the Metaverse, children may take a virtual field trip to walk through ancient cities as though they were newly built or fly around planets in a virtual spaceship. Research has already demonstrated that such experiences may improve a student's level of attention, retention of information and enjoyment of course material.[73] However, though some possibilities are thrilling, the Metaverse may also pose more risks for children, especially if Metaverse platforms fail to create safeguards to ensure that children are protected from immersive, age-inappropriate, harmful or illegal content.

Child safety in Web2

Guaranteeing children's safety online has already proven challenging in Web2. Both policymakers and industry have recommended that Web2 platforms employ some form of age verification in order to protect children from content that is inappropriate; however, the method of age verification has not been clearly established. The GDPR, for example, mandates a higher level of protection for children's personal data than for that of adults, without clarifying how a data controller should be able to distinguish between them.[74] The GDPR thus implicitly assumes that some form of age verification takes place, but does not specify the process. Similarly, the EU's Audio Visual Media Services Directive (AVMSD) suggests that age verification may be used in order to protect the physical, mental and moral development of minors, but considers it only one of several possible tools.[75]

Choosing the correct method for age verification has been the subject of debate since reliable online age verification is difficult to impose without risking a child's right to data privacy. Although there are some methods that are more privacy-preserving than others, Web2 platforms have sometimes found themselves in a "Catch-22" situation in which they are only allowed to process biometrics for age verification if the user has given explicit consent, but they need to first verify a user's age to determine if the user is old enough to give consent.[76] The question of method is also the key debate in negotiations around the proposal for a regulation laying down rules to prevent and combat CSAM. Since the CSAM proposal was first adopted in May 2022, numerous stakeholders from multiple Member States have criticised it, particularly in Germany.[77] These criticisms centre around the possibility for authorities to issue "detection orders" to providers of hosting and interpersonal communications services that may oblige them to scan users' private conversations, including encrypted conversations, for explicit content or evidence of child grooming.[78] Choosing the correct method for age verification will likely continue to feature strongly in negotiations about this proposal.

Child safety in the Metaverse

Despite the opportunities to explore new forms of learning in the Metaverse, it is also possible that increasingly immersive experiences may expose children to new harms. Research conducted by the Centre for Countering Digital Hate (CCDH), for example, found that users, including minors, are exposed to abusive behaviour every seven minutes on VR Chat, a social networking Metaverse app.[79] This abusive behaviour includes sexual content, bullying, harassment, grooming and violence. The National Society for the Prevention of Cruelty to Children (NSPCC) has also suggested that children are currently being exposed to "entirely inappropriate, really incredibly harmful experiences" in the Metaverse and that safeguards for children's safety must become a central consideration in the development of future Metaverse technologies.[80]

Where the Metaverse presents a particular threat to children is in its delivery of embodied experiences, potentially permitting strangers to not only speak to and share content with children but interact using their bodies, represented by avatars. Currently, the opportunities for parents or guardians to supervise such interactions are limited.[81]

Apart from the potential exposure to harmful or illegal content, children may experience developmental dangers by entering the Metaverse[82], such as increased risk of screen addiction,[83] or confusion between the boundaries of real and imaginary worlds.[84] They may also experience physical risks as some haptic suits are currently being manufactured that allow users to feel simulated pain through electric shocks.[85] These and other threats that will need to be accounted for when it comes to preserving the safety of children in the Metaverse.

Lessons learned

As described above, EU policymakers are currently in the early stages of debating the first substantial regulation dedicated exclusively to child safety. However, the road to get to this point has not been easy; EU policymakers have been debating the best legislation to tackle CSAM since at least 2020. In summer 2020, the Commission proposed a derogation to the EPD that was designed to give online platforms an explicit legal basis to continue to voluntarily check their services for CSAM content and evidence of child grooming. Despite the intended design of this derogation as a quick, temporary legislative fix, it launched a year-long battle over its scope and privacy implications. The CSAM proposal faced similar issues and was ultimately delayed by more than a year.

Forthcoming negotiations are expected to be similarly drawn out and difficult, as the CSAM proposal provides an ongoing flashpoint for both general concerns over the invasion of privacy and demands for online companies to take greater responsibility to safeguard children from online threats.[86]

Policymakers will likely continue to struggle with this issue throughout the negotiations on CSAM and as future regulation is developed. They may additionally seek to encourage industry to better consider child safety when developing new hardware and software, following previous recommendations by experts. During a public policy conference on the Metaverse last year, several VR experts pointed to the need to bake child protection into product design. Michael Preston, Executive Director of the Joan Ganz Cooney Center, notes that, "Often the necessary protections for kids are applied only to products designed for kids, rather than products designed for adults that kids happen to adopt."[87] As the Metaverse is likely to be used by everyone, and children are already some of the earliest adopters of Metaverse technology, policymakers will likely use all means at their disposal to make the Metaverse as safe as possible for all users, especially children.

Immersive technologies and child safety

The increased severity of harm in the Metaverse as compared to the Web2 Internet has to do with the potential for both immersive and sensory experiences. Earlier this year, a reporter named Yinka Bokinni posed as a 22-year-old woman and 13-year-old girl on two Metaverse social networking apps. She experienced sexual harassment within minutes of using both apps, along with racial slurs.[88] Other VR studies have shown the possibility for children to experience age-inappropriate content, such as gambling and sexually explicit material, including avatar nudity.

Bokinni's experience also highlights the difficulty of monitoring or reporting such behaviour. In her words, "You need names, IDs, some sort of evidence. But when you're witnessing something that upsets you, your first thought isn't necessarily: 'Let me record this conversation so I can report it and they can take action'."[89] When children are involved, the likelihood of reporting such behaviour further decreases; in many cases, unless users specifically "cast" their headset view to an external screen, it is impossible to monitor what a child is seeing or doing in the Metaverse.[90] When it comes to child safety then, technology creators may explore settings such as safe search, profanity filters and parental monitoring and include them in their products and platforms by design.

IV: Summary and Conclusion

The Metaverse marks a milestone in the way innovators are developing and deploying new technologies. Such a milestone will soon need to be reflected by a corresponding regulatory approach towards this emerging ecosystem. Although non-exhaustive, this papers' review of select policy areas already demonstrates that a multitude of policy challenges lie ahead:

- **Content Moderation:** Moderating content in the Metaverse will be a challenge as users shift to more real-time behavioural interactions. Expecting Metaverse platforms to moderate behaviour using the same tools with which they have moderated content may be technically infeasible without risking users' fundamental freedoms.
- **Liability:** Transactions conducted via decentralised blockchain infrastructure may make it difficult for Metaverse platforms to identify cybercriminals and respond to user complaints according to the current liability model. Liability may also be difficult to assign to users that participate in illegal behaviour in virtual spaces that may be leased/developed by a third-party or owned collectively.
- **Fundamental Freedoms:** Balancing users' fundamental freedoms of expression and information against the desire to protect consumers from illegal activity or harm will be increasingly complex in a hyper-real Metaverse in which users interact in real time.
- **User Privacy:** As the Metaverse is expected to encompass all aspects of our lives, the opportunities for data collection will extend beyond simple web browsing or social media engagement to a more comprehensive overview of individual activities, whether social, professional or recreational. Metaverse-enabling devices will also require a large amount of personal data in order to deliver immersive experiences. Helping users obtain more visibility on these data transfers so that they may give informed consent without compromising their privacy will likely remain an ongoing political and educational challenge.
- **Cybersecurity:** The Metaverse will give cybercriminals access to advanced, hyper-real technologies that could create new avenues for cybercrime. Increasing the resilience of digital infrastructures and educating users of their online risks will be essential to mitigate this risk.
- **Child Safety:** Children will be able to experience new educational experiences through the Metaverse but may also encounter risks to their safety including bullying, harassment, grooming, violence and exposure to sexually explicit material. Safeguarding children's right to privacy while keeping them safe from harm has already proven to be a contentious issue.

While expanding the scope of EU laws tailored for a Web2 environment may help to address some of these concerns, it is likely that the new structure and technologies of the Metaverse will require new rules tailored to immersive and potentially decentralised virtual spaces. In addition, other challenges, such as health, security, defence, competition and antitrust may need to be addressed separately, depending on where EU competency lies. They may therefore demand new forms of coordination, cooperation and/or enforcement with national and international institutions or even amongst industry stakeholders themselves.

No matter the challenges, it is important to recall that the Metaverse also has the potential for substantial good, creating an entirely new economic space and introducing new forms of digital ownership and content creation, as well as considerable advancements in health, education, sustainability, productivity and entertainment. Policymakers have an opportunity to utilise the full strength of the EU regulatory toolkit to facilitate the growth of the Metaverse in a way that encourages these multiple benefits while mitigating its potential risks. Working with industry partners and external experts may also help EU regulators develop laws with consumer and child safety at their heart, following the principles of privacy and safety by design. New working groups may also consider how compliance and enforcement may be challenged by the Metaverse and already start to develop solutions. Through a combination of co-regulation, self-regulation, performance-based regulation and regulatory sandboxes, the EU has the opportunity to establish the standards that will govern the Metaverse around the world.

This research paper was commissioned by Improbable and M2. Drafting support was provided by the Head of FTI Consulting EU’s Metaverse Taskforce, Alexandra Shoichet, with additional support from FTI Consulting’s Strategic Communications and Technology segments.

Appendix

In the short-term, EU policymakers may define new rules to regulate the different parts of the Metaverse that have not yet come together. Although it is doubtful that they will do so in entirely new legislation, they may seek to at least partially regulate the Metaverse in both upcoming texts and, at a later stage, during the regular review of existing laws. The following table highlights the majority of laws mentioned in this paper, noting when they are due for adoption or review and suggesting how they may lead to initial regulation of the Metaverse:

Name of Legislation	Date of Adoption/Review	Relevance to the Metaverse
DSA	Entered into force in November 2022 and shall apply from February 2024. Its first evaluation is expected to take place three years after it enters into force	The DSA clarifies and harmonises the liability regime for online intermediaries, laying down obligations to tackle illegal activity online while protecting users' fundamental rights. Its review may be one opportunity to reassess the liability framework in decentralised Metaverse environments.
AI Liability Directive	The proposal was presented by the European Commission on 28 September 2022. It will now be reviewed by the European Parliament and the Council. Negotiations are expected to take +/- 18 months	The AI Liability Directive aims to provide legal certainty to industry developing emerging digital technologies, including VR and AR devices that may be used for a more immersive Metaverse experience.
Copyright Directive – Directive (EU) 2019/790	The Directive is scheduled for review in June 2026	The Copyright Directive tasks online providers that host user-generated content to employ measures that prevent users from violating copyright. Its review may be an opportunity to assess the use of automated filters in the Metaverse.
TCO - Regulation (EU) 2021/784	A Commission evaluation on the effectiveness of the safeguard mechanisms and impact of the law on fundamental rights is expected by June 2024	Similar to the Copyright Directive above, the evaluation of the TCO may assess the use of automated filters, as well as new risks for terrorism recruitment in the Metaverse.
AI Act	Interinstitutional negotiations are expected to start in Q4 2022/Q1 2023. Following the current Commission proposal, the AI Act will start applying two years after its entry into force	The European Parliament has already submitted amendments to the Draft Report on the AI Act that refer directly to the Metaverse.[91] Such amendments may, for example, widen the scope of the AI Act to include Metaverse services.
GDPR – Regulation (EU) 2016/679	The Commission is expected to publish a report on the evaluation and review of the GDPR in May 2024	The GDPR sets out the legal framework for the collection and processing of personal information, which may need to be adapted if personal information is managed, collected or transferred in new way in the Metaverse that may threaten user privacy.
e-Privacy Regulation (EPR)	Over the past five years, policymakers have been negotiating the draft e-Privacy Regulation, intended to eventually replace the 2002 e-Privacy Directive. According to the original Commission proposal, it will be evaluated	The EPD outlines rules on cookies that will likely need to be re-assessed for the Metaverse. The EPR or its review may also be an opportunity to develop or respond to emerging Metaverse standards.

	three years after it enters into force	
NIS 2	Expected to enter into force in Q4 2022. After it enters into force, Member States will have 21 months to transpose it into national law	The NIS 2 aims to update and expand the scope of the 2016 NIS Directive, while harmonising the rules on cybersecurity risk management and incident reporting across the EU. Its transposition may be an opportunity to specify cybersecurity standards for Metaverse platforms and related technologies.
Cyber Resilience Act	The proposal was presented on 15 September 2022. It will now be reviewed by the European Parliament and the Council. Negotiations are expected to take +/- 18 months	The Cyber Resilience Act aims to introduce common cybersecurity standards for connected devices and other digital products, which will likely impact hardware that may be used to enter the Metaverse.
GPSR	Interinstitutional negotiations are expected to start in Q4 2022	The GPSR aims to revise and modernise EU rules for general product safety to ensure that products of the digital age meet European safety standards. This will likely impact hardware that may be used to enter the Metaverse.
eIDAS - Regulation (EU) 910/2014	Interinstitutional negotiations are expected to begin in Q4 2022/Q1 2023	The re-vamped eIDAS may create Personal Digital Identity Wallets, which could be instrumentalised across a decentralised Metaverse.
CSAM	The interim derogation to the EPD expires in August 2024. Ideally, negotiations on the CSAM proposal will have concluded by that date	As the potential risks of the Metaverse to children are already being explored, the Metaverse may be considered during interinstitutional negotiations on the proposal.

Works Cited

[1] Breton, T. (14 September 2022), “People, technologies & infrastructure – Europe’s plan to thrive in the metaverse”. LinkedIn: https://www.linkedin.com/pulse/people-technologies-infrastructure-europes-plan-thrive-thierry-breton/

[2] Von der Leyen, U., & Šefčovič, M. (14 September 2022), “State of the Union – Letter of intent”. European Commission: https://state-of-the-union.ec.europa.eu/system/files/2022-09/SOTEU_2022_Letter_of_Intent_EN_0.pdf

[3] European Commission (18 October 2022), “Commission work programme 2023: A Union standing firm and united”, Publications Office of the European Commission: https://ec.europa.eu/info/publications/2023-commission-work-programme-key-documents_en

[4] Zhou, L. (2022), *The Metaverse: Concepts and Issues for Congress*, Congressional Research Service: https://crsreports.congress.gov/product/pdf/R/R47224

[5] Howe, J. (22 June 2022), “The Metaverse and immersive technologies – A regulatory perspective”. Competition and Markets Authority: https://competitionandmarkets.blog.gov.uk/2022/06/22/the-metaverse-and-immersive-technologies-a-regulatory-perspective/

[6] Madiega, P., Polona, C., & Niestadt, M. (24 June 2022), “Metaverse: Opportunities, risks and policy implications”. European Parliamentary Research Service: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733557

[7] Zhou, L. (2022), *The Metaverse: Concepts and Issues for Congress*. Congressional Research Service: https://crsreports.congress.gov/product/pdf/R/R47224

[8] See, for example: Nguyen, T., Lee, A., & Verma, A. (08 April 2022). “Metaverse Evolution Will Be Phased; Here’s What It Means for Tech Product Strategy”. Gartner: https://www.gartner.com/en/articles/metaverse-evolution-will-be-phased-here-s-what-it-means-for-tech-product-strategy

[9] Narula, H. (2022), *Virtual Society: The Metaverse and the New Frontiers of Human Experience*. Currency, New York.

[10] See, for example: IRL Studios Inc. (2022), “Gym Class – Basketball VR”. MetaQuest: https://www.oculus.com/experiences/quest/3661420607275144/

[11] See, for example: Chan, J. C. (24 August 2022), “iHeartMedia Plans to Host Metaverse Concerts In ‘Fortnite’ Virtual World”. The Hollywood Reporter: https://www.hollywoodreporter.com/business/digital/iheartmedia-iheartland-fortnite-1235204209/

[12] See, for example: Purdy, M. (05 April 2022), “How the Metaverse Could Change Work”. Harvard Business Review: https://hbr.org/2022/04/how-the-metaverse-could-change-work

[13] See, for example: MetaVRse (23 March 2022), “Introducing TheMall”. TheMall: https://themall.io/

[14] See, for example: OliveX (2022), “Building the fitness metaverse”. OliveX: https://www.olivex.ai/

[15] See, for example: Ragav, A., Noen, K., Lindahl, M., Dohler, M. (17 August 2022), “Metaverse education: from university to metaversity”. Ericsson: https://www.ericsson.com/en/blog/2022/8/metaverse-education-from-university-to-metaversity

[16] Patel, N. (19 July 2022), “Is the metaverse going to suck? A conversation with Matthew Ball”. The Verge: https://www.theverge.com/23269170/what-is-the-metaverse-matthew-ball-interview-decoder-podcast

[17] Citi GPS. (30 May 2022), “Metaverse and Money: Decrypting the Future”. Citigroup: https://icg.citi.com/icghome/what-we-think/citigps/insights/metaverse-and-money_20220330

[18] See, for example: European Commission (16 June 2022), “The Strengthened Code of Practice on Disinformation 2022”. European Commission: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

[19] See, for example, the concerns listed in: Gawer, A., & Srnicek, N. (March 2021), “Online platforms: Economic and societal effects”. European Parliamentary Research Service: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656336/EPRS_STU(2021)656336_EN.pdf (p. 29)

[20] For further information, see, e.g.: IBM, “What is blockchain technology?”. IBM: https://www.ibm.com/topics/what-is-blockchain

[21] See, for example: Gorman, K. (12 March 2022), “Open or closed? A key battle over the metaverse is underway that will decide the buzzy technology’s future”. Fortune: https://fortune.com/2022/03/12/metaverse-open-closed-source-nft/

[22] The Economist (26 January 2022), “What are DAOs, or decentralised autonomous organisations?”. The Economist: https://www.economist.com/the-economist-explains/2022/01/26/what-are-daos-or-decentralised-autonomous-organisations

[23] Miranda, L. (15 August 2022), “Avatars need their nails done, too. Enter the metaverse side hustle”. NBC News: https://www.nbcnews.com/business/business-news/metaverse-make-money-avatars-decentraland-rcna41336

[24] Van Roey, M. (28 May 2022), “Why Web3 represents a new frontier for personal data ownership”. VentureBeat: https://venturebeat.com/datadecisionmakers/why-web3-represents-a-new-frontier-for-personal-data-ownership/

[25] European Parliament (19 May 2021), “Tackling online piracy of live sporting events”. EP Press Releases: https://www.europarl.europa.eu/news/en/press-room/20210517IPR04117/tackling-online-piracy-of-live-sporting-events.

[26] See, for example: YouTube Help (2022), “How Content ID works”. YouTube: https://support.google.com/youtube/answer/2797370?hl=en

[27] As quoted in Murphy, H. (12 November 2021), “*How will Facebook keep its metaverse safe for users?*”. Financial Times: https://www.ft.com/content/d72145b7-5e44-446a-819c-51d67c5471cf

[28] Mak, A. (09 May 2022), "I Was a Bouncer in the Metaverse". Slate: https://slate.com/technology/2022/05/metaverse-content-moderation-virtual-reality-bouncers.html

[29] *ibid*

[30] See "Section 4: Liability of intermediary service providers" in Directive 2000/31/EC, "Directive on electronic commerce" OJ (L178) 17.7.2000, p. 1-16: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32000L0031

[31] European Commission (2019), "The EU Code of conduct on countering illegal hate speech online". European Commission: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

[32] See *Recital 58a* in Regulation (EU) 2022/2065, "A Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)" OJ (L277) 27.10.2022: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32022R2065

[33] Berg, N. (05 September 2022), "Inside the lucrative business of a metaverse landlord, where monthly rent can hit $60,000 per property". Fast Company: https://www.fastcompany.com/90749937/inside-the-lucrative-business-of-a-metaverse-landlord-where-monthly-rent-can-hit-60000-per-property

[34] European Commission, "Digital Education Action Plan (2021-2027)". European Commission: https://education.ec.europa.eu/focus-topics/digital-education/action-plan

[35] These proposals may be found at *Product Liability Directive* (2022), 2022/0302 (COD): https://single-market-economy.ec.europa.eu/document/3193da9a-cecb-44ad-9a9c-7b6b23220bcd_en & *AI Liability Directive* (2022), 2022/0303(COD): https://ec.europa.eu/info/files/proposal-directive-adapting-non-contractual-civil-liability-rules-artificial-intelligence_en

[36] See, for example, *Recital 22* in Directive 2000/31/EC, "Directive on electronic commerce" OJ (L178) 17.7.2000, p. 1-16: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32000L0031

[37] See, for example, Article 11 of Regulation (EU) 2022/2065, "A Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)" OJ (L277) 27.10.2022: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32022R2065

[38] Madiega, P., Polona, C., & Niestadt, M. (24 June 2022), "Metaverse: Opportunities, risks and policy implications". European Parliamentary Research Service: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733557, p. 5

[39] *Charter of Fundamental Rights of the European Union* (2012), C2012/326/02: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT

[40] Killween, M. (26 April 2022), "EU top court upholds Copyright Directive's "upload filter" provision with caveats". EurActiv: https://www.euractiv.com/section/digital/news/eu-top-court-upholds-copyright-directives-upload-filter-provision-with-caveats/

[41] Giglio, F. (14 September 2022), "The new Regulation on addressing the dissemination of terrorist content online: a missed opportunity to balance counter-terrorism and fundamental rights?". KU Leuven CiTiP : https://www.law.kuleuven.be/citip/blog/the-new-regulation-on-addressing-the-dissemination-of-terrorist-content-online/

[42] See, for example: European Commission (20 May 2022), "Questions and Answers: Digital Services Act*". EC Press Corner: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348

[43] As quoted in Palmer, M. (18 April 2022), "The deepfake dangers lurking in the metaverse". Sifted: https://sifted.eu/articles/deepfake-dangers-metaverse/

[44] Council of Europe (1950), *Convention for the Protection of Human Rights and Fundamental Freedoms*. In Council of Europe Treaty Series 005. Council of Europe: https://www.echr.coe.int/documents/convention_eng.pdf

[45] See *Article 8* in *Charter of Fundamental Rights of the European Union* (2012), C2012/326/02: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT

[46] See Article 15 of Directive 2000/31/EC, "Directive on electronic commerce" OJ (L178) 17.7.2000, p. 1-16: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32000L0031

[47] See, for example: IAB Europe (27 October 2021), "IAB Europe Launches New Campaign on Targeted Advertising at crunch time for the Digital Services Act (DSA)". IAB Europe: https://iabeurope.eu/all-news/iab-europe-launches-new-campaign-on-targeted-advertising-at-crunch-time-for-the-digital-services-act-dsa/

[48] See, for example: European newspaper Publisher Association (14 December 2021), "European press urges European Parliament to protect editorial content integrity and online advertising revenues". ENPA: https://enpa.eu/press-releases/european-press-urges-european-parliament-protect-editorial-content-integrity-and

[49] See, for example: Ecommerce Europe, Independent Retail Europe, & EuroCommerce (22 October 2021), "Joint Industry Statement on Targeted Advertisement and the DSA". Ecommerce Europe: https://ecommerce-europe.eu/wp-content/uploads/2021/10/Retail-Industry-statement-on-Targeted-ads-and-DSA-22102021.pdf

[50] See, for example: SME Connect CDA (17 November 2021), "Europe's SMEs call on policymakers to reject a ban on targeted advertising" SME Connect: https://www.smeconnect.eu/europes-smes-call-on-policymakers-to-reject-a-ban-on-targeted-advertising/

[51] See, for example: Kaspersky, "What is Keystroke Logging and Keyloggers?". Kaspersky Resource Center: https://www.kaspersky.com/resource-center/definitions/keylogger

[52] Cited in Jerome, J., & Greenberg, J. (April 2021). *Augmented Reality + Virtual Reality, Privacy & Autonomy Considerations in Emerging, Immersive Digital Worlds:* https://fpf.org/wp-content/uploads/2021/04/FPF-ARVR-Report-4.16.21-Digital.pdf, p. 15

[53] Dick, E. (15 November 2021), "Public Policy for the Metaverse: Key Takeaways from the 2021 AR/VR Policy Conference". Information Technology & Innovation Foundation: https://itif.org/publications/2021/11/15/public-policy-metaverse-key-takeaways-2021-arvr-policy-conference/

[54] Jerome, J., & Greenberg, J. (April 2021). *Augmented Reality + Virtual Reality, Privacy & Autonomy Considerations in Emerging, Immersive Digital Worlds:* https://fpf.org/wp-content/uploads/2021/04/FPF-ARVR-Report-4.16.21-Digital.pdf, p. 16

[55] *Ibid.*

[56] Wheeler, T. (20 June 2022), "If the Metaverse Is Left Unregulated, Companies Will Track Your Gaze and Emotions". TIME: https://time.com/6188956/metaverse-is-left-unregulated-companies-will-track-gaze-emotions/

[57] See, for example: Szczepański, M. (January 2020), "Is data the new oil? Competition issues in the digital economy". European Parliamentary Research Service: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)646117_EN.pdf

[58] Madiega, P., Polona, C., & Niestadt, M. (24 June 2022), "Metaverse: Opportunities, risks and policy implications". European Parliamentary Research Service: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733557, p. 6

[59] Fletcher, C. (26 June 2022), "Cybersecurity and the metaverse: Identifying the weak spots". VentureBeat: https://venturebeat.com/datadecisionmakers/cybersecurity-and-the-metaverse-identifying-the-weak-spots/

[60] European Commission, "Cybercrime". EC Migration and Home Affairs: https://home-affairs.ec.europa.eu/cybercrime_en

[61] *Ibid.*

[62] European Commission. (7 June 2022), "The Cybersecurity Strategy". Shaping Europe's digital future: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

[63] Fletcher, C. (26 June 2022), "Cybersecurity and the metaverse: Identifying the weak spots". VentureBeat: https://venturebeat.com/datadecisionmakers/cybersecurity-and-the-metaverse-identifying-the-weak-spots/

[64] Hao, K. (13 September 2021), "A horrifying new AI app swaps women into porn videos with a click". MIT Technology review: https://www.technologyreview.com/2021/09/13/1035449/ai-deepfake-app-face-swaps-women-into-porn/

[65] Bell, C. (28 March 2022), "The metaverse is coming. Here are the cornerstones for securing it". Microsoft Blog: https://blogs.microsoft.com/blog/2022/03/28/the-metaverse-is-coming-here-are-the-cornerstones-for-securing-it/

[66] Proposal for a Regulation on cybersecurity requirements for products with digital elements – Cyber resilience Act (15 September 2022), 2022/0272 (COD): https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

[67] See, for example, *Art. 7(1)(h)* in *General Product Safety* (2021), 2021/0170 (COD): https://data.consilium.europa.eu/doc/document/ST-10381-2021-INIT/en/pdf

[68] Regulation (EU) No 910/2014, "Electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC" OJ (L257) 28.08.2014: https://eur-lex.europa.eu/eli/reg/2014/910

[69] *Commission Staff Working Document Impact Assessment Report accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity* (2021): https://eur-lex.europa.eu/resource.html?uri=cellar:6f30628d-c458-11eb-a925-01aa75ed71a1.0001.02/DOC_1&format=PDF

[70] Europol (2022), "Cryptocurrencies: Tracing the Evolution of Criminal Finances", Europol Spotlight Report series, Publications Office of the European Union, Luxembourg: https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances

[71] Council of the EU (29 June 2022), "Anti-money laundering: Provisional agreement reached on transparency of crypto asset transfers". Press release: https://www.consilium.europa.eu/en/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/

[72] European Commission "About SSI eIDAS Bridge". European Commission – DIGIT: https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about

[73] Makransky, G., Mayer, R.E. (2022) *Benefits of Taking a Virtual Field Trip in Immersive Virtual Reality: Evidence for the Immersion Principle in Multimedia Learning*. Educational Psychology Review, 34, 1771–1798: https://doi.org/10.1007/s10648-022-09675-4

[74] See, for example, *Article 8* in Regulation (EU) 2016/679, "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)," OJ (L119) 04.05.2016: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[75] *Audiovisual Media Services Directive* (2010), Directive 2010/13/EU: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0013&from=EN

[76] Van der Hof, S. (17 November 2021), "Age assurance and age appropriate design: what is required?". LSE blog: https://blogs.lse.ac.uk/parenting4digitalfuture/2021/11/17/age-assurance/

[77] Goujard, C., & Westendarp, L. (10 June 2022), "Germany forces EU into damage control over encryption fears". Politico: https://www.politico.eu/article/germany-eu-damage-control-encryption-abuse-online/

[78] See *Section 2: Detection Obligations* in *Child Sexual Abuse Materials* (2022), 2022/0155(COD): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472
[79] Center for Countering Digital Hate (30 December 2021), "New research shows Metaverse is not safe for kids". Press Release: https://counterhate.com/blog/new-research-shows-metaverse-is-not-safe-for-kids/
[80] Crawford, A., Smith, T. (23 February 2022), "Metaverse app allows kids into virtual strip clubs". BBC News: https://www.bbc.com/news/technology-60415317
[81] The Institution of Engineering and Technology (2022), *Safeguarding the metaverse*. IET: https://www.theiet.org/media/9836/safeguarding-the-metaverse.pdf, p. 10
[82] Boyle, J. (19 June 2022), "The battle to build a child-friendly metaverse". TechXplore: https://techxplore.com/news/2022-06-child-friendly-metaverse.html
[83] A recent survey by Pew Research Centre found that nearly half of all U.S. teenagers use the Internet "almost constantly." See Vogels, E. A., Gelles-Watnick, R., & Massarat, N. (10 August 2022), "Teens, Social Media and Technology 2022". Pew Research Center: https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/
[84] The Institution of Engineering and Technology (2022), *Safeguarding the metaverse*. IET: https://www.theiet.org/media/9836/safeguarding-the-metaverse.pdf, p. 10
[85] AFP (19 June 2022), "The battle to build a child-friendly metaverse". France 24 : https://www.france24.com/en/live-news/20220619-the-battle-to-build-a-child-friendly-metaverse
[86] See, for example: DigitalEurope (31 August 2022), "Creating an effective framework for combating child sexual abuse and exploitation online". DigitalEurope: https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2022/08/DIGITALEUROPE-Creating-an-effective-framework-for-combating-child-sexual-abuse-and-exploitation-online-FINAL.pdf
[87] Dick, E. (15 November 2021), "Public Policy for the Metaverse: Key Takeaways from the 2021 AR/VR Policy Conference". Information Technology & Innovation Foundation: https://itif.org/publications/2021/11/15/public-policy-metaverse-key-takeaways-2021-arvr-policy-conference/
[88] Bokinni, Y. (25 April 2022), "A barrage of assault, racism and rape jokes: my nightmare trip into the metaverse". The Guardian: https://www.theguardian.com/tv-and-radio/2022/apr/25/a-barrage-of-assault-racism-and-jokes-my-nightmare-trip-into-the-metaverse
[89] *Ibid.*
[90] The Institution of Engineering and Technology (2022), *Safeguarding the metaverse*. IET: https://www.theiet.org/media/9836/safeguarding-the-metaverse.pdf, p. 10
[91] See, for example: *Amendment 902*, proposing to create a new Article 2a concerning "Metaverse environments" in *Artificial Intelligence Act* (2021), 2021/0106(COD): https://www.europarl.europa.eu/doceo/document/CJ40-AM-732837_EN.pdf