BRIEFING

European Parliament

Metaverse

Opportunities, risks and policy implications

SUMMARY

One of the most talked about concepts in modern technology, the metaverse can be described as an immersive and constant virtual 3D world where people interact by means of an avatar to carry out a wide range of activities. Such activities can range from leisure and gaming to professional and commercial interactions, financial transactions or even health interventions such as surgery. While the exact scope and impact of the metaverse on society and on the economy is still unknown, it can already be seen that the metaverse will open up a range of opportunities but also a number of risks in a variety of policy areas.

Major tech companies are scaling up their metaverse activities, including through mergers and acquisitions. This has given impetus to a debate on how merger regulations and antitrust law should apply. Business in the metaverse is expected to be underpinned largely by cryptocurrencies and non-fungible tokens, raising issues of ownership, misuse, interoperability and portability. Furthermore, the huge volume of data used in the metaverse raises a number of data protection and cybersecurity issues (e.g. how to collect user consent or protect avatars against identity theft).

There is considerable scope for a wide range of illegal and harmful behaviours and practices in the metaverse environment. This makes it essential to consider how to attribute responsibility, inter alia, for fighting illegal and harmful practices and misleading advertising practices, and for protecting intellectual property rights. Moreover, digital immersion in the metaverse can have severe negative impacts on health, especially for vulnerable groups, such as minors, who may require special protection. Finally, the accessibility and inclusiveness of the metaverse remain areas where progress has still to be made in order to create an environment of equal opportunities.

IN THIS BRIEFING

EPRS | European Parliamentary Research Service

Authors: Tambiama Madiega, Polona Car and Maria Niestadt with Louise Van de Pol
Members' Research Service

PE 733.557 – June 2022

EN

Background

Although the notion of the metaverse, the literal meaning of which is 'beyond universe', does not have a uniform definition, it has been described as an immersive and constant virtual 3D world where people interact through an avatar to enjoy entertainment, make purchases and carry out transactions with crypto-assets, or work without leaving their seat.[1]

Technology

From a technology standpoint, the metaverse is commonly considered to be an evolution of the internet towards 'Web3' (Web1 being the worldwide web and Web2 meaning the rise of social media) in which individuals are empowered and actively involved in the creation of virtual worlds. Starting with video games, fantasy realities have already evolved over time into 3D virtual environments (e.g. the multimedia platform Second Life or the gaming platform World of Warcraft) that now combine numerous technologies to create an immersive experience. The metaverse will constitute the next and much more encompassing step in that development.

Experts stress that the metaverse would ideally exhibit four specific technical features:

- 'realism', which enables people to become emotionally immersed in the virtual world;
- 'ubiquity', meaning that the virtual spaces are accessible through all digital devices while using one virtual identity;
- 'interoperability', allowing distinct systems or platforms to exchange information or interact with each other seamlessly;
- 'scalability', namely having the network architecture deliver sufficient power to enable massive numbers of users to occupy the metaverse without compromising the efficiency of the system and the experience of the users.

The immersive experience is generated by using a range of technologies including virtual reality (VR), which is a three-dimensional online environment that can be entered by using a dedicated headset connected to a computer or game console, and augmented reality (AR), which shows the real world enhanced by computer-generated items, such as graphics. Users can create a virtual avatar in the metaverse, to represent them in any desired shape or form. The quality of illustration of the virtual avatar increases the immersive experience. Furthermore, connectivity is paramount to the metaverse; artificial intelligence (AI) and internet of things (IoT) technologies are also used to ensure seamless communications.

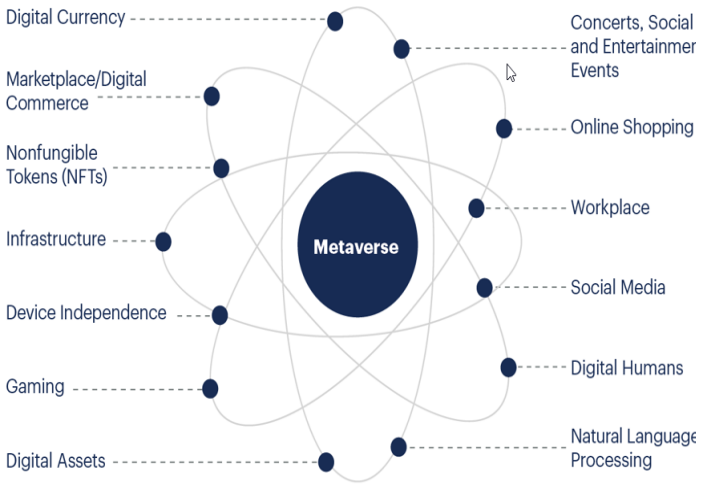
There are, however, competing visions as to the shape the metaverse will take. In a 'privatised form', big companies would determine how people could live in the metaverse, whereas in a 'community form', communities would build and govern their own worlds. Whatever form the metaverse takes, it is expected to become a world where people can buy and sell virtual goods (e.g. real estate, manufacturing and textiles) by means of digital currencies. The economic metaverse ecosystem will then rely on blockchains and cryptocurrency technologies, such as 'non-fungible tokens' (NFTs), to monetise transactions in the digital environment.

Usage

Virtual worlds are becoming increasingly popular. Technological research and consulting firm Gartner predicts that, by 2026, 25 % of people will spend at least an hour daily in the metaverse for work, shopping, education, social activities and/or entertainment (see Figure 1). Commercial companies have begun to develop their own platforms in the metaverse. In March 2022, the Metaverse Fashion Week event occurred in Decentraland, one of the most popular existing virtual worlds. The metaverse can be used also for entertainment purposes. For instance, a livestreamed online concert held on gaming platform Fortnite gathered an audience of 12 million. Furthermore, the metaverse is already used to advertise local tourism and banks.

In addition to commercial uses, organisations are exploring the use of virtual worlds for other purposes. For instance, the metaverse is useful in the healthcare sector to perform virtual therapy and remote surgeries. It will surely also expand the possibilities of online education. The US army is exploring using the metaverse to establish a virtual environment for soldiers' training. Virtual worlds can also be set up by public administrations (e.g. the city of Seoul is planning to open a 'Metaverse 120 Center' in 2023, with officials providing consultations and civil service as avatars) or for political purposes (e.g. in Turkey, the AK Party hosted a party meeting within a metaverse platform).

Figure 1 – Metaverse elements



Source: Gartner, 2022.

Economics

Economic studies have predicted that the global metaverse market will reach €597.3 billion by 2030. Many companies have invested in the creation of the metaverse. Meta (formerly known as Facebook) has announced annual investment of €8.8 billion in the metaverse. Microsoft has bought Activision Blizzard (a company owning online games such as Call of Duty and World of Warcraft) for nearly €61.6 billion, with the perspective that gaming will be a big part of the development of the metaverse. Qualcomm has established a €88 million metaverse fund to further develop VR and AR technologies.

The metaverse is a big trend in China too. More than 1 500 Chinese companies have already applied for trademarks related to the metaverse and many Chinese companies have invested in this business area. For example, Alibaba has invested €52.8 million in Nreal, an augmented reality glasses maker, and TikTok's parent company, ByteDance, has spent €1.2 billion on VR headset maker Pico.

Not only are companies investing in the metaverse, but users are also starting to invest. Recently, one user bought a piece of land in virtual world Sandbox for €3.7 million (i.e. the biggest purchase in the Metaverse so far) and another individual purchased a virtual plot for €396 000, just to be the virtual neighbour of Snoop Dogg, a famous singer.

Selected policy issues

Competition

Building the metaverse environment requires the interconnection and interoperability of many devices and platforms across the digital ecosystem. Major tech companies are rapidly scaling up including through mergers and acquisitions to shape the metaverse environment building blocks. For instance, Meta has been making large acquisitions in the area of video games and social media sectors. This new landscape, which might be dominated by a few big companies, raises many competition concerns.

Issues

Standardisation and interoperability. Big tech companies will likely drive the metaverse architecture in defining technical standards and protocols. The risk is that some tech companies will attempt to shape the emerging metaverse standards so as to foster (or at least not adversely affect) their business practices. Some stress the importance of the technical solutions, protocols and

services that enable interoperability to build the metaverse ecosystem, but warn that this may lock in developers and limit consumer choice and the creation of competing innovations.

Killer acquisitions and merger control. The case of 'killer acquisitions' – acquisitions by large companies of innovative, nascent competitors solely (or primarily) to halt their innovation and pre-empt future competition – has become a concern in the metaverse environment. More generally, the ability of the EU regulators to use current merger and acquisitions tools to tackle monopolisation in the high-tech sector has come under increasing scrutiny. In this regard, the European Commission's clearance of Google's takeover of wearable fitness device company Fitbit (authorised with remedies) met with some criticism.

Antitrust. Building the metaverse environment will give some companies unparalleled opportunities to monopolise digital markets. Some warn that the same powerful tech firms that currently dominate digital markets may also control the metaverse environment, with every incentive to perpetuate current anticompetitive practices, such as self-preferencing (i.e. favouring their own products) and dark patterns (i.e. designing websites and mobile application interfaces in order to influence users' behaviour and decision-making).[2] Some regulators, such as the German Bundeskartellamt, are already trying to tackle dominant positions in the emerging virtual reality market (e.g. the Oculus case). The fact that the metaverse environment requires competitors to communicate, collaborate and ensure that platforms are interoperable could also potentially lead to a series of anti-trust challenges, for instance concerning the sharing of sensitive information, such as pricing, or agreements between competitors subject to competition law scrutiny.

Possible policy implications

Merger regulation. A debate has started in the EU on the need to amend merger regulation. Some changes in merger enforcement tools and standards have been implemented or are being considered in order to tackle mergers and killer acquisitions in digital markets. In the US, there are calls to reform merger control to address market power stemming from data collected by devices but also increasingly from targeted advertisements, dark patterns, and other forms of coercive choice architecture, upon which the metaverse environment is being built.[3]

Antitrust tool. The Parliament has called on the Commission to ensure that companies in the metaverse abide by the relevant digital legislation and competition framework. To some extent, existing competition law, including the recently agreed digital markets act (DMA), arguably addresses antitrust issues such as the self-preferencing by metaverse platforms of their own content or refusals to grant a competitor access to a metaverse space.[4] However, some experts argue that antitrust law should be adapted to identify competitive issues arising in the metaverse world[5] and others propose, more broadly, to promote consumer autonomy, prohibit the use of dark patterns and implement data silos to block cross-market data flows.[6]

Regulate standards setting and interoperability. Some experts call for efforts to foster the development of open metaverse standards – rather than proprietary ones – in order to foster a community metaverse.

Data protection

People will participate in the metaverse through avatars, using special equipment, such as VR headsets or similar devices, enabling an immersive experience. This entails the collection of massive amounts of data, including biometric data and data on the emotional and physiological responses of users, representing sensitive personal data under the General Data Protection Regulation (GDPR) and thus requiring special attention and explicit user consent for each purpose for which data is used. Nevertheless, researchers are trying to find ways to make the use of enabling devices privacy safe and GDPR compliant without compromising the use of such devices too much.

Issues

Blurred roles. The multitude of entities present in the metaverse will create a web of relationships, making it very difficult to determine responsibilities and liabilities. Defining the distinction between data controller and data processor in the metaverse might become a big challenge as the entities present in a particular universe will be highly intermingled. Defining who does what on behalf of whom will not be easy. This raises the issue of the collection of user consent and the obligation to display privacy notices, i.e. should this be done for a particular metaverse in its entirety or for each entity in a metaverse separately? Under the GDPR, users must give explicit consent for each specific purpose. This would for example differ if you were in the metaverse to attend a concert or to go to an auction. Moreover, users' data will be gathered more widely during their experience in the metaverse. There are claims that data collection will be involuntary and continuous, therefore making the collection of consent almost impossible.

Furthermore, the immersion experience in the metaverse entails the integration of access points with content of services and thus reduces considerably users' capacity to avoid collection of personal data. This raises the question of the confidentiality of personal correspondence that happens in the metaverse and the redefinition of private virtual space to protect it from commercial and state interests. As the metaverse will likely present access points to digital content in the future, opt-out would not be a practical solution. Therefore, government and industry regulatory solutions will need to be sought. The storage, handling and safeguarding of data used in the metaverse will also have to be addressed, as well as responsibility for data theft or misuse.

Data sharing and portability. The notion of interoperability and the movement of users inside and between different metaverses, together with their data and assets, raises the question of data sharing and data portability. Companies, which tend to prefer proprietary rights over users' data, will need to establish data sharing agreements, which will need to fulfil data protection requirements such as user consent and the privacy notification obligation. This may be challenging in decentralised metaverse models. Moreover, international transfers of data will need to be clarified, to enable free movement in the metaverse. Determining jurisdiction in the metaverse will be a challenge as it could for example apply either to the location of the user, the location of the avatar, or the location of the relevant servers.

The issue of direct marketing based on geolocalisation and emotional response[7] will arise in the metaverse, as users will be offered product selection based on their behaviours and reactions. Sharing (selling) of data with third parties under GDPR requires the active and freely given consent of users. The question is how to maintain this requirement in the metaverse environment in which users may be increasingly subject to subliminal advertisement. Furthermore, researchers have established that eye-trackers could give companies data, which could be used for targeted advertising at a very granular level. Special attention in this regard will have to be made for the protection of vulnerable groups, in particular of children's personal data, which under the GDPR requires special protection. Effective age verification and measures to deter children from providing their personal data will therefore be required.

Intrusive profiling. Access to sensitive data, such as emotional reactions, could lead to intrusive ways of profiling, which could have harmful consequences, such as loss of control over one's life and decisions or voter manipulation, in particular for vulnerable groups. However, it is in the interest of big tech to encourage people to spend more time online so that they can collect more data. Consequently, also state surveillance could increase given governments' access to data shared in the metaverse.

Metaverse workplace. Metaverse-enabling devices generate a range of physiological data about employees based on their participation in VR simulations. This could enable employers to perform intrusive surveillance of their employees. Moreover, perceptual experiences could replace reflexive decision-making and could consequently lead to biased automated decision-making and to inequalities in processes such as hiring, performance evaluation and training.[8]

Possible policy implications

Revision of data protection framework. The European Parliament has emphasised that the privacy and data protection framework does apply to the metaverse and has called on the Commission to ensure the compliance of companies and entities working in the metaverse with the existing legal framework. There are also calls to revise and update the GDPR, as it was not designed to address some of the challenges and complexities now presented by the metaverse, such as the need to regulate data gathered during unconscious behaviour, or for interaction with AI.

Data intermediaries could serve as links between people and entities collecting their data. Nevertheless, special attention should be made to AI-enabled data agents, which would decide on users' data permissions. The EU has opted for a human-centric approach to AI in the draft AI act, which could limit unwelcome developments. Moreover, the EU has established a framework for data sharing management and consent controls for people via data intermediation services, such as personal data spaces (or data wallets), in the draft data governance act.

Open and decentralised metaverse. To enable universal operation and interoperability, a metaverse model, based on blockchain and open standards is starting to emerge, controlled by the users themselves in form of decentralised autonomous organisations (DAOs). The decentralised metaverse model could be explored to do more to address data protection issues that are difficult to resolve in more centralised business models (i.e. the users themselves would control their data and decide how it could be shared. There are tensions however between blockchain and the data protection regulation. Some researchers recommend the adoption of regulatory guidance, and of codes of conduct and certification mechanisms, to contribute to legal certainty.

Liabilities

There is considerable scope for a wide range of illegal and harmful behaviours and practices in the metaverse environment. The question is how to prevent or control those phenomena in the metaverse space, the boundaries of which are still largely unknown. The nature of the metaverse poses many challenges when it comes to addressing liabilities, combating illegal and harmful practices and misleading advertising practices, and protecting intellectual property rights.

Issues

Illegal and harmful content online. Augmented and virtual reality will create new content moderation challenges, including for tackling verbal harassment or hate speech in a virtual space, inappropriate actions from avatars that simulate sexual harassment or assault, pornographic content modelled on avatars, or misinformation or defamatory content generated using augmented reality.[9] When users interact through their avatars, there may then be situations that would equate to breaking civil or even criminal laws. Cases of women being sexually harassed on Meta's VR social media platform have already been documented. Although these incidents happen in a virtual world, they can feel very 'real' and 'violating' to the person involved. Some studies also point to the fact that metaverse platforms could become fertile ground for disinformation to spread and even for the expansion of extremist ideologies (e.g. the resurrection of Osama Bin Laden in a virtual world). Furthermore, artificial intelligence (AI) including machine-learning algorithms and deep-learning architectures, will likely be central to the metaverse. Those technologies could increase the ability of companies active in the metaverse environment to track and monitor their users and customers in real time and expand the negative impacts that some social media have shown in recent years.

Advertising practices. Advertising strategies are taking off in immersive contexts. Whereas one study warns of the risk of consumer manipulation, given the psychological effects of immersive technology,[10] the impact on consumers of advertising practices in the metaverse are still unclear.

Intellectual property rights protection. Experts warn that intellectual property (IP) enforcement is a challenge in the metaverse environment. This is because it is more difficult to identify the provider that can take down infringing content, since metaverse content is distributed and replicated across decentralised networks running on Web 3.0 and blockchain-based platforms. There may therefore be issues around applicable law and jurisdiction and how to identify infringers. Popular brands are also facing issues of unauthorised use of registered trademarks in the metaverse.

Possible policy implications

Content moderation. The question as to whether the EU content moderation rules currently being amended would apply to illegal or harmful metaverse content is unsettled. Some argue that it is likely that the digital services act (DSA) will apply to numerous developers and businesses operating in a metaverse and that the draft artificial intelligence act (AI act) may regulate the use of biometrics as well as the implementation of subliminal, manipulative or exploitative techniques in a metaverse environment. The need to further amend EU law to keep users safe online cannot be ruled out, while the topic of virtual reality is not specifically addressed in the DSA, in the draft AI act, or under the forthcoming liability framework for emerging digital technologies. The decision of companies such as Facebook to develop a self-regulation approach to metaverse content moderation has been met with some scepticism. Policymakers could take further initiatives so that online platforms and law enforcement authorities are better able to identify and respond to dangerous or illicit content in the immersive environment (e.g. strengthening protection against non-consensual pornography and defamatory content) and ensure that liability laws applicable to online intermediaries consider the potential impacts on AR/VR communications platforms and their users.[11] Whether it is necessary to grant legal personality to avatars to make them responsible for their actions in the metaverse or, at least, to identify criteria to distinguish between an avatar and the true legal person who operates that avatar is another question that has been raised.

Revising advertising and rules on intellectual property. There is a debate on the need to revise legislation on advertising in order to address its metaverse implications. Some experts believe that the current rules applicable to video games will inform the regulation framework for advertising in the metaverse. The French advertising authority recently updated its guidelines to clarify the rules applicable to virtual universes. While it seems that, generally speaking, the current trademark laws are applicable to the metaverse, some experts stress that it might be useful to include specific references to the metaverse in the law. Other experts argue that regulations should be crafted to limit the scope of emotion-responsive advertising to restrict virtual product placement within the metaverse and improve transparency.[12]

Financial transactions

Commercial transactions in the metaverse are expected to be largely under-pinned by cryptocurrencies (e.g. bitcoin or ethereum) and non-fungible tokens (NFTs) will be used to track and validate the sale and ownership of digital goods. NFTs are blockchain-enabled cryptographic assets that represent proof of ownership for digital objects. When someone buys a digital item in the metaverse world (e.g. an avatar, avatar clothing or a virtual decoration), the purchase is recorded on a blockchain (i.e. a decentralised digital platform used to store information and record transactions securely) in which transaction records cannot be deleted or altered. Major worldwide brands have started to forge new business models in which when customers buy a physical item in the real world, they also get ownership of a linked NFT in the metaverse world. However, a range of legal issues has been highlighted, including those outlined below.

Issues

Ownership of digital assets in the metaverse. The legal and regulatory framework surrounding NFTs is under development and the extent to which NFTs create an ownership right is still very much disputed. Some legal commentators stress that current ownership of metaverse assets is governed

by contract law rather than by property law and warn that private metaverse platforms may therefore be contractually given a great deal of control over some key aspects of digital assets in the metaverse environment. Legal issues may arise regarding proper verification of ownership.

Misuse of NFTs. NFTs can be misused in various ways. Fraudulent acts include scams, malware and hacking to gain unlawful access to digital wallets storing NFTs and other crypto-assets. With no clear regulatory framework concerning NFT ownership, criminals can create and sell NFTs without owners' knowledge or permission.[13] Other legal issues regarding digital currency use concern virtual money transfers (between avatars), money laundering and gambling in a virtual world.[14]

Interoperability and portability. There is as yet no interoperability or portability between the various metaverse environments, and as it stands, each platform needs to link NFTs to its own proprietary digital assets. This calls into question customers' ability to carry their virtual avatars and properties from one virtual world to another.

Possible policy implications

Fintech regulation. While NFTs are currently not subject to specific regulation in the EU, they must comply with some existing legislation, including the Anti-Money-Laundering Directive, which for instance imposes anti-money-laundering requirements on virtual currency exchanges. Although some authors believe some EU laws, such as the directive on digital content, could apply to digital assets purchased in the metaverse, it is essential for policymakers to assess whether the EU fintech and consumer protection frameworks need to be revised in order to fit the new virtual environment better. One example of a regulation that could influence the economic governance of the metaverse is the draft proposal for a regulation on markets in crypto-assets. The European Commission's view is that unregulated crypto assets expose consumers and investors to substantial risks.

Cybersecurity

The sheer volumes of data circulating in the metaverse and the ways in which this data will be used constitute a growing risk for users. Current cybersecurity challenges such as phishing, malware and hacking will persist[15] and will extend to devices enabling a metaverse experience and to avatars. Protecting the integrity of avatars will therefore be a particular issue of concern, as will new forms of cyber-crime, such as selling fake NFTs, illicit use of crypto-currencies and malicious smart contracts. Researchers also raise the question of how virtual crimes will be considered in comparison to offline ones. A further hurdle in terms of fighting hackers, organised criminals, terrorist groups and sex offenders, will be the multi-layered structure of the virtual environment. The metaverse may allow them to hide behind encryption and untraceable NFTs, making it difficult to identify them and pursue a legal recourse. There are also concerns about the possible connections between the dark web and the metaverse, and consequently the need to create a metaverse criminal justice system to prevent and limit illegal activity. Therefore, security considerations and possible solutions need to be built into the development of the metaverse from its inception.

Issues

Security of metaverse enabling devices. Recent research has revealed that the characteristics of such devices could lead to serious data breaches, as the sensitive data needed for such devices to function, such as voice control or facial movement, could be reproduced. VR technology enables emotions and consciousness to be manipulated and gives hackers access not only to the victim's psyche,[16] but also to their body. Furthermore, hackers gaining access to such a device would be able to control what the victim was seeing and hearing, and would be able to see inside their office or home, with serious security consequences.

Security of protocols. A particular technical challenge will be building protocols able to mitigate the risk of transfer of harmful code between platforms to enable seamless movement of users between virtual spaces. Entities in the metaverse will therefore need to look beyond their particular

security measures, as they will depend on the cybersecurity of other entities. Implementing interoperability will entail allocation of responsibilities. Supply chain due diligence will be essential to preserve the security of the platforms.

Avatar integrity. Risk of identity theft, avatar duplication and misuse creates an issue for interoperability. Identity authentication built on blockchain will be crucial in this respect, as it is more resistant to cyber-attacks than a centralised system. Nevertheless, this cannot address criminal activity such as social engineering, which targets human behaviour. A decentralised identification network, enabling an account verification system built on international standards, to enhance user confidence to use avatars across platforms, could be one way to overcome this problem. However, this would simultaneously generate bigger concentrations of data, making the accounts more vulnerable and potential damage in the event of a cyber-attack even bigger.

Possible policy implications

Legal framework for blockchain and smart contracts. Experts suggest that blockchain and decentralised technologies could help to protect users' identities in the metaverse and prevent fraud. The advantage of blockchain is that it provides access to any digital space without interference of a centralised institution. It enables interoperability and relatively high levels of security owing to its heterogeneous architecture. By assuring security, transparency and traceability, it increases user trust. Smart contracts, used to perform transactions in virtual spaces, are embedded in the blockchain computer code and execute a contract once its terms have been fulfilled. In 2020, given the lack of legal certainty of such contracts, Parliament called on the Commission to address the issues and propose an appropriate legal framework, reiterating its 2018 resolution.

Building EU cyber-resilience capacity. The proposed NIS2 directive would further increase EU national cybersecurity capabilities and EU cyber-resilience. It does not however deal with cybersecurity requirements for consumer products. VR and AR devices, literally opening the door to the metaverse, fall within the proposal for a regulation on general product safety, which inter alia requires appropriate cybersecurity features for product protection. Protection of consumers by introducing common cybersecurity rules for digital products and ancillary services will also be addressed in the forthcoming cybersecurity resilience act. As the financial sector is particularly attractive to cyber-criminals, Parliament has called on the Commission to propose legislative changes in the area of information and communications technologies (ICT) and cybersecurity requirements for the EU financial sector, to increase its cyber-resilience. The Commission has responded to increasing threats and the proliferation of national approaches, with a proposal for a digital operational resilience act (DORA), complemented by a draft regulation on markets in crypto-assets (MiCA). An important block in building cyber-resilience in the EU may be to address the cybersecurity professionals shortage and skills gap, which are of concern, by means of the European cybersecurity skills framework (ECSF).

Education of users. Criminals, including cyber-criminals, are very innovative and tend to be a step ahead of regulators and companies in their efforts to protect data. Therefore, education of users on steps they can take to protect their identities and assets in the metaverse and preventive measures they can take will play an important role. The updated digital education action plan expects 70 % of 16 to 74 year olds in the EU to have at least basic digital skills by 2025.

Health

The metaverse has various mental and physical health implications that are especially worrying when concerning vulnerable groups such as children. At the same time, the metaverse can also help to cure people and improve patient safety. Although not metaverse-specific, the EU has already taken a number of non-legislative as well as legislative actions to protect consumers', in particular minors' health in the virtual world.

Issues

Impact on mental and physical health. If used to excess, the metaverse can cause mental health problems (such as loneliness) and reduce physical activity, leading to a rise in obesity and other physical health problems, which in turn contribute to a desire to escape the real world. Addictions to social media and online gaming as a form of escapism already exist, but the metaverse can reinforce them. Furthermore, the metaverse can create motion sickness, nausea, dizziness, eye, head and neck fatigue. In addition, if people are distracted while using the metaverse, harmful accidents can happen either to the person in the metaverse or to the persons or things (such as furniture) around them. The metaverse could however actually help people suffering from certain diseases (for example agoraphobia) or overcome dramatic experiences. It can also be used to train health professionals. Some psychologists and psychiatrists are already using virtual reality in aversion therapy, allowing patients to interact with situations that cause them anxiety. The metaverse can also facilitate telemedicine and consultation of doctors on the other side of the world. This is particularly valuable in areas where there is a shortage of medical professionals.

Impact on children. The metaverse holds the promise of offering children a unique experience. It could enable them to go back in time or visit places that they could never have explored. It also offers a form of hands-on experience that can help children to understand the world around them and how things work, potentially increasing the motivation to learn. However, the interaction of avatars in the metaverse – even if they look real – cannot replace real human interaction. It will be important to find ways to use the metaverse alongside the real world in ways that preserve real teacher-child, caregiver-child, and child-child social relationships. If the metaverse is left unregulated, it may cause children significant harm. As reported by the Center for Countering Digital Hate, in some social apps in the metaverse children are confronted with abuse, harassment, bullying, racism and pornographic content. This is not safe for children, and especially problematic, since children's sense of reality and responsibility is usually less developed. A global survey from 2021 found that 34 % of respondents had been asked to do something sexually explicit online that they were uncomfortable with during childhood. The same survey reported that the age at which this is happening seems to be getting lower.

Possible policy implications

To mitigate the health risks posed by the metaverse, researchers have proposed various solutions, ranging from obliging companies to issue warnings of possible harm, to setting up help centres and distress buttons.[17] Equally important is to identify the age of users effectively. Finally, parents are also responsible for monitoring their children's activity in the metaverse, although it might not be so easy in virtual reality.

Content moderation regarding minors. The European Commission has recently proposed several legislative acts to address age-inappropriate and illegal content online. The May 2022 proposal for a regulation to prevent and combat child sexual abuse online, obliges providers to detect, report, block and remove child sexual abuse material from their services. They will also have to introduce the necessary age verification measures. The European digital identity wallet, proposed by the Commission, could help to verify age. The December 2020 digital services act proposal also covers public health and minors in the virtual world. According to the provisional political agreement reached on the act, digital services must protect minors from illegal content online. Providers of digital services will have to write their terms and conditions in a way that children can understand. Furthermore, all online platforms will have to ensure the safety and security of children using their services, and will be prohibited from presenting targeted advertising based on the use of minors' personal data. Finally, in May 2022 the Commission adopted a new strategy for a better internet for kids (BIK+), which builds on the first European strategy for a better internet for children (BIK), adopted in 2012. The new strategy aims to ensure that children are protected (for example against age-inappropriate and illegal content), respected and empowered online, in line with European digital rights and principles. The strategy proposes various actions (such as an EU code on age-

appropriate design) to be undertaken by the Commission, Member States and by the industry, and takes into account Parliament's 2021 resolution on children's rights.

Accessibility and inclusiveness

Although in principle, the metaverse is open to all, in practice many might have trouble accessing it for various reasons, ranging from a lack of digital skills to not having reliable broadband or the right hardware.

Issues

The metaverse might be difficult to access in particular for people with a low level of digital literacy, or people with disabilities or living in areas with low connectivity. For other groups, the obstacle might be access to consistent reliable broadband. The high cost of equipment is another barrier in accessing the metaverse. Although a smartphone or a computer may be sufficient to experience the metaverse to some extent, navigating and engaging in it fully may require augmented reality smart glasses, a virtual reality headset and a device equipped with 5G. All this is quite expensive, although if the equipment is taken up by large numbers of people, prices are likely to drop. At the same time, the metaverse can help to make society more accessible. It may render certain physiological constraints in people with disabilities irrelevant. For example, technologies such as image recognition may help people with visual disabilities navigate the metaverse and a voice changer may help people with vocal challenges. People with autism may feel more comfortable speaking through an avatar. In the metaverse, people are also free to choose the race and gender of their avatar.

Possible policy implications

Most actions geared towards making the metaverse inclusive and accessible are voluntary. The Web Accessibility Initiative of the World Wide Web Consortium (the main international standards organisation for the internet) has, for example, published XR accessibility user requirements, which list user needs and requirements for people with disabilities when using virtual reality or immersive environments, augmented or mixed reality and other related technologies (XR). Companies developing the metaverse are also thinking about the diversity aspect, equality and inclusion. Therefore, they are trying to involve a diverse range of people not only as customers but also as developers of the metaverse. In addition, they are paying attention to the physical appearance of avatars by including a variety of types. However, there is some criticism of the voluntary nature of accessibility measures. For example, the European Disability Forum has criticised the provisional agreement on the digital services act for not ensuring accessibility for persons with disabilities. Namely, rather than making accessibility obligations mandatory for digital services, policymakers simply agreed that it was enough to give consideration to accessibility as a voluntary good practice.

Conclusion

The metaverse brings both opportunities and risks, the full scale of which are not yet clear. Some policy issues and their possible implications have been identified in various areas, including competition, data protection, liabilities, financial transactions, cybersecurity, health, accessibility and inclusiveness. The potential consequences of using immersive reality technologies have been singled out for other areas too, for instance for the environment and for people at work. It remains to be seen whether any specific EU initiatives will be necessary to address the development of the metaverse. While the Commission appears to have no immediate intention to propose legislative measures, Commission Vice-President Margrethe Vestager has stressed that the virtual reality environment poses new challenges, especially for antitrust regulators. The Council wants Europe to set conditions, so as to enable the continent to benefit fully from the opportunities opened up by the metaverse. Parliament has also begun considering the implications of the metaverse phenomenon, for instance in its discussions on the draft AI act and on its 2021 report on competition policy.

MAIN REFERENCES

Council of the European Union, analysis and research team, Metaverse – virtual world, real challenges, March 2022.

ENDNOTES

1 See Council of the EU, analysis and research team, Metaverse – virtual world, real challenges, March 2022.

2 See Marks M., 'Biosupremacy: Big Data, Antitrust, and Monopolistic Power over Human Behavior', *UC Davis Law Review*, Vol. 55, p. 513, 2021.

3 Marks M., 'Biosupremacy: Big Data, Antitrust, and Monopolistic Power over Human Behavior', *UC Davis Law Review*, Vol. 55, p. 513, 2021.

4 See also Answer given by Mr Breton on behalf of the European Commission, Parliamentary questions, 1 June 2022.

5 In that sense, see Egliston B. and Carter M., 'Critical questions for Facebook's virtual reality: Data, power and the metaverse', *Internet Policy Review*, Vol. 10(4), 2021, pp. 1-23.

6 See Marks M., Biosupremacy: Big Data, Antitrust, and Monopolistic Power over Human Behavior, *UC Davis Law Review*, Vol. 22, p. 513, 2021.

7 Chatellier R., Métavers : réalités virtuelles ou collectes augmentées ?, Laboratoire d'innovation numérique de la CNIL, 5 November 2021.

8 See Egliston B. and Carter M., 'Critical questions for Facebook's virtual reality: Data, power and the metaverse', *Internet Policy Review*, Vol. 10(4), 2021, pp. 1-23, section on Automated decision making: quantifying the qualitative, pp. 12-14.

9 See Catsro D., Content Moderation in Multi-User Immersive Experiences: AR/VR and the Future of Online Speech, 2022.

10 See B. Heller and A. Bar-Zeev, 'The Problems with Immersive Advertising: In AR/VR, Nobody Knows You Are an Ad', 2021, *Journal of Online Trust and Safety*, Vol. 1(1), 2021.

11 See D. Catsro, Content Moderation in Multi-User Immersive Experiences: AR/VR and the Future of Online Speech, 2022.

12 See L. Rosenberg, Regulation of the Metaverse: A Roadmap, 2022.

13 See N. Kshetri, 'Scams, Frauds, and Crimes in the Nonfungible Token Market', *Computer*, 2022.

14 See R. Tromans, 'The world is not enough: law for a virtual universe', *European Lawyer*, 2007, Vol. 70, pp. 21-25.

15 See Exploring the metaverse and the digital future / GSMA, February 2022, Section 4.2 Trust and safety.

16 See also Roesner and Kohno: Security and Privacy for Augmented Reality: Our 10-Year Retrospective.

17 As highlighted by a recent publication of the Institution of Engineering and Technology, these distress buttons alone are not enough, as by the time the victim has found the button, the damage is already done.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)