The metaverse and its impact on human rights, the rule of law and democracy

IEEE

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

The metaverse and its impact on human rights, the rule of law and democracy

Council of Europe and IEEE

The views and opinions expressed in this collaborative work are those of the contributors and do not necessarily reflect the official policy or position of their respective affiliated institutions, The Institute of Electrical and Electronics Engineers (IEEE) or the Council of Europe. Neither IEEE nor the Council of Europe endorse companies, products or services. Any related mention serves purely illustrative purposes and are neither exhaustive nor necessarily the most representative examples. This work is published under the auspices of IEEE Standards Association and the Council of Europe for the purposes of furthering public understanding of the importance of addressing human rights and ethical and rule of law considerations in policy- and decision-making processes.

All other correspondence concerning
this document should be addressed
to the Council of Europe Freedom of
Expression and CDMSI Division
F-67075 Strasbourg Cedex
France

E-mail: CDMSI@coe.int or
metaverse.report@ieee.org

Cover design: Documents and Publications
Production Department (SPDP),
Council of Europe

Cover photo: Shutterstock

Layout: Jouve, Paris

Council of Europe Publishing
F-67075 Strasbourg Cedex
http://book.coe.int

ISBN 978-92-871-9465-7
ISBN 978-92-871-9466-4 (PDF)

Printed at the Council of Europe

This collaborative report by the Council of Europe and IEEE Standards Association, a globally recognised standard-setting organisation within IEEE, aims to aid Council of Europe member states in understanding the metaverse's potential, applications and associated risks concerning human rights, the rule of law and democracy. It emphasises the importance of an approach to technology development that is based on human rights, the rule of law and democratic principles, acknowledging the uncertainty of the metaverse's future evolution.

The report draws on insights from over 50 experts, encompassing various technical, ethical, legal and governance aspects of the metaverse.

Contents

Acknowledgements

The Council of Europe and IEEE are grateful to the experts who contributed to this report through written submissions or interviews: Prof. Melodena Stephens (Mohammed Bin Rashid School of Government); Monique Morrow; Patricia Shaw (Beyond Reach); Dr Katie Evans; Prof. Irene Kamara (Tilburg University); Dr Mark McGill, Dr Mohamed Khamis and Melvin Abraham (University of Glasgow); Dr Ola Michalec (REPHRAIN Centre, the University of Bristol); Andrés Domínguez Hernández (Alan Turing Institute); Richard Jones (the University of Edinburgh); Prof. Jan Gugenheimer (TU Darmstadt); Cristina Fiani (UKRI); Dr Alicia Cork (University of Bath); Dr Yu Yuan (IEEE SA 2023 President); Jason Douglas Evans, Dr Palak Patel and Dr John Bosco Acot Okello (Nurenyx); Ansgar Koene (EY), Ricardo Chavarriaga (Head of the Switzerland Office of the Confederation of Laboratories for AI Research in Europe (CLAIRE) and IEEE SA IC Chair Neurotechnologies for BMI), Prof. Silvestro Micera (EPFL and Scuola Superiore SantAnna), Dr Kim Barker (University of Lincoln and ObserVAW); Wenqu Chen and Cheng Chi (CAICT); Epaminondas Christophilopoulos (UNESCO Chair on Futures Research, FORTH); Dr Atif Wolfgang Bhatti, Dr Cecilia Drepper, Dr Alexander Andreas, Dr René Döring and Dr David-Julien dos Santos Goncalves (all Linklaters Germany); Karim Mohammadali and Tom Gault (Google); Bugge Holm Hansen (Copenhagen Institute for Future Studies); Cornelia Kutterer (University of Grenoble and Considerati), Prof. Eleni Mangina (University College Dublin); Prof. Ming Li (Utah State University); John Daozhuang (Johnny) Lin (1stCycle Corporation); Prof. Cecilia Metra and Prof. Martin Eugenio Omana (University of Bologna); Alejandro Moledo del Rio (European Disability Forum); Tyler Jaynes (University of Utah); Dr Ramesh Ramadoss (Chair, IEEE Blockchain Technical Community), Peng Yang (Huazhong University of Science and Technology), Zihang Yin (Wuhan Technology and Business University), Carol McDonald (Gneiss Concept), Denia Psarrou and Melina Efstathiou (Eversheds Sutherland). Special thanks go to Monique Morrow, Melodena Stephens, Katie Evans, Prof. Eleni Kosta (Tilburg University) and IEEE SA staff Moira Patterson, Sri Chandrasekaran, John Havens and Dr Clara Neppel for their valuable input, review and comments.

The report was led by Irene Kitsara, IEEE SA, edited by Jennie Steinhagen and Irene Kitsara and reviewed by the Council of Europe’s relevant sectors: Media and Internet Governance, Data Protection, Artificial Intelligence, Cybercrime, Democracy and Governance, Anti-discrimination, Youth, Children’s Rights and Sport Values, Education, Human Dignity and Gender Equality.

Enabling technologies and building blocks of the metaverse

An overview of some of the components, the underlying and enabling technologies of the metaverse can facilitate its understanding and related challenges. This overview should not be viewed as definitions or an exhaustive list because there is no alignment in terminology and the technology and technical implementation of the metaverse may vary in the future. It should rather be viewed as working descriptions for the purposes of this report, meant to help in the understanding of the technology making immersive experiences and virtual worlds possible. These components and enablers currently include the following.

Artificial intelligence (AI) and AI systems (AIS)

AI techniques and functional applications, such as machine and reinforcement learning, natural language processing, computer vision and affective computing, enable adaptive and realistic simulations, intelligent virtual entities or agents, customised recommendations and personalised user experiences in general. AI algorithms power virtual characters, natural language processing (NLP) and machine learning optimisation, enhancing the interactivity and responsiveness within the metaverse. By leveraging AI in a responsible and ethical manner, the metaverse can deliver transformative experiences and opportunities for users across a wide range of industries and applications. The recent advancements in generative AI, a subdomain of AI allowing for the generation of synthetic and partially original content, is powered mainly by the deep learning Generative Adversarial Networks, which can generate realistic and dynamic content within the metaverse (pictures, objects, even entire virtual environments) based on existing data and patterns, and the NLP large language models, which allow the understanding and generation of human language. This technology enables the metaverse to continually evolve and expand with new and diverse content, providing users with novel and engaging experiences, including more realistic interactions with AI agents employed in customer service scenarios, social interactions or gaming environments.

Augmented reality (AR)

AR technologies such as AR headsets, smartphone apps, smart glasses or contact lenses overlay digital content onto the physical world, blending the real and virtual worlds, offering a sophisticated on-device sensing, enhanced experience or perception of reality and contextual awareness, or even changing how people, places, adverts and other things look. An AR-powered metaverse is seen as the future of personal computing (replacing the smartphone).

Blockchain

Blockchain technology provides a decentralised and transparent framework for managing digital assets and transactions within the metaverse. Blockchain allows for the creation of unique digital tokens representing virtual assets, such as virtual land, virtual goods or digital collectibles that can be securely owned, traded and verified on the blockchain, ensuring ownership within the metaverse. Blockchain also enables interoperability among different virtual platforms and ecosystems within the metaverse.

Cloud computing

Cloud computing addresses the need in the metaverse for large storage and computing resources, by offering virtual machines. As such, cloud computing is considered to be a critical infrastructure to support immersive experiences, while hybrid clouds, including and combining local and cloud solutions, are under consideration to address concerns related to data security and privacy protection in the cloud.

Digital humans

Digital humans represent a ground-breaking development in XR technology, bringing virtual beings to life with remarkable realism and interactivity. By leveraging advanced computer graphics, animation and artificial intelligence techniques, digital humans replicate human appearance (face or full-body representation), behaviour and even emotions. Digital humans can enhance immersive experiences by serving as virtual avatars (with much more advanced and realistic human representation), guides or companions, providing users with a more engaging and personalised interaction within virtual environments. The rise of digital also raises ethical considerations, such as issues of consent, privacy and the potential for misuse or deception.

Digital twins

Digital twins technology is a powerful tool that enhances XR experiences by creating virtual replicas or representations of physical objects, systems or environments, connecting the virtual and physical worlds, allowing for real-time monitoring, simulation, visualisation and interaction with virtual models that accurately reflect the behaviour, characteristics and status of their real-world counterparts. Digital twins can provide real-time data and insights into immersive experiences, enhancing the sense of immersion, interactivity and realism. Additionally, the combination of digital twins and XR can facilitate collaborative decision making, enabling multiple users to interact with and manipulate virtual representations of physical objects or environments simultaneously.

Edge computing

Edge computing offers a distributed compute architecture which can support the metaverse for low latency and high bandwidth, by processing a large volume of data in a short period of time, for a seamless immersive experience. Edge computing is also expected to reduce the weight and cost of wearables as it will move the currently local compute to a distributed infrastructure, combined with cloud computing.

Extended reality (XR)

XR is another term sometimes used interchangeably with the metaverse that refers to a suite of immersive technologies including virtual, augmented and mixed reality, as well as spatial computing.

Human–machine interface (HMI)

"Human-machine interface [also called user interface or human-computer interface] [is a] means by which humans and computers communicate with each other. The human-machine interface includes the hardware and software that is used to translate user (i.e., human) input into commands and to present results to the user." (Encyclopaedia Britannica).

Internet of Things (IoT)

IoT technology plays a significant role in enhancing XR experiences by enabling seamless connectivity, data exchange and interaction between physical and virtual elements. In XR, IoT devices and sensors can be utilised to gather real-time data from the physical environment, such as motion, location, temperature and biometric information. These data can then be integrated into virtual environments or used to trigger interactive virtual content. The number of technologies involved is immense; there are over 300 platforms for IoT solutions (Burns, Cosgrove and Doyle 2019).

Mixed reality (MR)

Mixed reality combines the physical and digital worlds, immersing users in a world in which they can interact with digital objects using a combination of eye gaze, hand gestures and voice commands.

Neurotechnology

Neurotechnology is an umbrella term for technologies related to the brain. According to the Organisation for Economic Co-operation and Development (OECD), neurotechnology includes "devices and procedures used to access, monitor, investigate, assess, manipulate, and/or emulate the structure and function of the neural systems of natural persons" (OECD 2019). It comprises brain–computer interface (BCI)/ human–machine interface (HMI), medical implants and neurostimulation. The most relevant type of neurostimulation will be transcranial stimulation, performed with devices that use electrodes on the scalp to provide electrical stimulation to the cortex. Some studies have shown temporary improvement in cognitive capabilities and memory after the stimulation. Some parts of the DIY and gaming communities have shown interest in these systems to improve as cognitive enhancers. There could be a similar uptake for metaverse-mediated applications. Some of these devices are now being released for consumer markets (and can be easily built with off-the-shelf components) (Wexler 2017).

Spatial computing

Spatial computing maps virtual objects into the physical space and allows their integration along with further digital information in the physical environment, enabling a more natural and intuitive interaction and seamless navigation and immersion in the metaverse. Technologies like spatial audio complement the experience and allow a more realistic and immersive experience.

Virtual reality (VR)

VR technology provides users with a simulated environment that can replicate the physical world or imaginary settings. Virtual online worlds are predominantly experienced through either two-dimensional displays (smartphones, monitors) or immersive VR headsets. By wearing a VR headset, users can experience a three-dimensional virtual world and interact with objects and other users. In immersive VR, users experience increasing degrees of presence, body ownership (the illusion they are in that environment and "own" their virtual avatar body) and increasing degrees of perceptual realism (the multisensory fidelity of the experience, including visual, auditory, haptic and olfactory realism). Immersive VR experiences can mimic social experiences in reality, with a consequent degree of psychological realism.

Web3

The third iteration of the internet is focused on a decentralised infrastructure (such as blockchain) which brings openness and decentralisation and empowers users, with decentralised development, control and ownership shared among users and the community. In this phase of the internet, AI systems start doing seemingly intelligent things autonomously (Markoff 2006).

Chapter 1
Introduction and scope

The Council of Europe's Digital Agenda 2022-2025 points to the metaverse as a development that raises multiple and complex challenges, similar to those experienced with previous technology advances and disruptions like the internet, social platforms or artificial intelligence (AI). Yet the intensity and effects of the metaverse are only expected to multiply and increase. The lack of consensus about definitions and the polarisation of stakeholder opinions about the expected impact of the metaverse resemble the concerns that have emerged with AI in recent years, which range from enthusiasm to scepticism observed in the pattern of AI "winters and summers" hype cycles. Concerns about the legal implications of the metaverse likewise echo the discussions at the time of the internet's emergence in the late 1990s, as well as during the rise of gaming platforms and virtual worlds. As a cross-cutting environment with possible applications across various industries and all aspects of life, spilling across generations with a significant indirect impact on the planet, areas for consideration by policy makers span almost the full range of human rights and fundamental freedoms.

Since its signing in 1950, the European Convention on Human Rights (hereinafter "the Convention") has progressed and broadened in scope through the case law of the European Court of Human Rights ("the Court"). The Court regularly expands and deepens the rights afforded by the Convention, referred to as a living document, and considers their application in new contexts and circumstances not originally conceived by its drafters. In its guide to human rights for internet users based on the Convention and its interpretation by the Court, it is unequivocally stated that "fundamental freedoms and human rights apply equally online and offline". These frameworks are complemented by what are known as "Council of Europe standards": encompassing conventions, recommendations, guidelines and best practices; addressing specific issues; and setting out frameworks, rules and principles to be adopted and reflected in national legislative frameworks of its member states. A non-exhaustive list of existing relevant legal frameworks and standards, both international and regional, can be found in Appendix II, while specific references are included in the respective sections of the report. Some frameworks, resources and experiences from other jurisdictions and technology areas are sometimes mentioned as background; they reference different approaches and rationales, while the focus remains on the mandate and perspective of the Council of Europe. Some of these references and considerations are included in the tables referring to specific issues in Appendix III and should be read in combination with the respective sections in the body of the report, bearing in mind that they are illustrative and not exhaustive. The question that emerges is whether the current frameworks, applicable to offline and online reality, remain appropriate or sufficient to address current and future risks and threats to human rights, the rule of law and democracy in the metaverse.

The future composition of a virtual, immersive society, which includes virtual governments, marketplaces, etc., as well as the relationship and impact of this virtual world on the physical world and offline life remain unclear. Accordingly, both the current and the anticipated effects of engaging in the metaverse – known and novel – require active and timely attention. As with other technology disruptions, such as generative AI, the clemency of a long reaction time will not be granted. There is therefore an immediate need for policy makers and governing bodies to: 1. develop a baseline understanding of the technologies and concepts associated with the metaverse; 2. acknowledge the urgency of assessing the current situation and how it may evolve over time; 3. understand macro technological, economic, environmental and social contexts; 4. evaluate the scope, risks and opportunities concerning existing or missing safeguards (legal frameworks, standards and challenges with enforcement and self-governance); and 5. prioritise and enable the uncompromised exercise of human rights and fundamental freedoms to attain human prosperity and social well-being in any and all democratic environments – in the virtual realm just as much as in the non-virtual.

This report provides an overview of the principal issues identified jointly by the Council of Europe and the IEEE Standards Association, a global standard-setting organisation within the IEEE, within the framework of the Digital Partnership. The report aims to support the Council of Europe member states in their understanding of the metaverse and its potential, its applications and benefits, as well as the issues and risks that may arise from the development, deployment and engagement within the metaverse. It also looks at the impact on human rights, the rule of law and democracy – to be further analysed and assessed in the context of the Council of Europe's work so that policy may be applied and directed accordingly. While not exhaustive, it is grounded in a shared belief that technology, even when complex and still under development like the metaverse, can and should be human-centric, include ethical considerations and aspire to respect human rights, the rule of law and democracy by design (Nemitz 2018). With the knowledge that the metaverse may or may not develop in the way currently imagined, the highlighted issues may evolve in magnitude and importance. For the report, the IEEE brought together nearly 50 experts to share their perspectives and expertise on the technical, ethical, social, legal, policy, regulatory, standardisation and governance issues associated with the environment and applications of the metaverse. Related considerations for navigating within this shifting landscape are offered.

Understanding the metaverse and its current state

Currently there is no single and commonly accepted definition or understanding of the metaverse, although standardisation efforts to harmonise the language and related terminology are underway. The metaverse is often used interchangeably with terms such as virtual worlds, immersive realities, digital twins, virtual, augmented, mixed or extended reality (VR/AR/MR/XR) or Web3; other times it is viewed in a hierarchical relationship to those, either as an umbrella term or as a subset of these terms (Hupont Torres et al. 2023). Terms that are currently used at the European Commission level include virtual worlds – next generation digital worlds as per the EC Joint Research Centre (Hupont Torres et al. 2023) – and immersive realities, while other international initiatives and partnerships continue to refer to the metaverse (WEF Metaverse Initiative; IEEE Metaverse Congress and Metaverse Standardization Committee; ITU Forum on Embracing the Metaverse 2023).

The report does not aim to provide a definition but rather a description of the metaverse, a term coined in 1992 by Neal Stephenson in his science fiction novel, *Snow Crash*, to describe an immersive virtual world. As per Matthew Ball, author of *The Metaverse and How it Will Revolutionise Everything,* the metaverse can be described as a vision for a scaled, interoperable network of real-time rendered 3D virtual worlds and environments that can be experienced synchronously and persistently by an effectively unlimited number of users with an individual sense of presence and with continuity of data (Ball 2021). From that perspective, the metaverse can be viewed as "the envisioned end state – incorporating all digital worlds alongside the physical world, with interoperability between them all" (McKinsey 2022a). As such, these can be viewed as components/spaces of a single virtual universe – a metaverse with interconnected/interoperable elements, including virtual worlds and gaming platforms.

While much concerning the eventual materialisation of the metaverse remains uncertain, the complex concept it represents is no longer considered science fiction. Virtual worlds and immersive realities are already realities *simpliciter*. Over the past 30 years, explosive innovations in the enabling technologies of the metaverse – such as breakthroughs in augmented reality and gains in the autonomy of smart systems – have fuelled this rapid transition to our current situation. Related platforms and experiences offer glimpses of the metaverse's potential, but they are still fragmented and lack the seamless integration and interoperability required for a fully realised metaverse.

According to Merriam-Webster, "meta" means "after" in Greek and "verse" is an abbreviation of the "universe", "so 'metaverse' neatly implies a world or conception that requires the 'real' world in order to move beyond it and acknowledge another realm" (Merriam-Webster, "What is the Metaverse?"). As the borders between physical and virtual worlds may increasingly be blurring, the current understanding that the "real world" is the physical world will not necessarily be as easily distinguishable or obvious. The metaverse, conceived to be immersive, creates a virtual and digital extension of the present universe.

It should be noted that some consider that there are or will be several "metaverses" as opposed to the single "metaverse" vision. In the context of the IEEE's discussions, for example, metaverse refers to an experience in which the outside world is perceived by the users (human or non-human) as being a universe that is built upon digital technologies as a different universe ("virtual reality"), a digital extension of our current universe ("augmented reality") or a digital counterpart of our current universe ("digital twin") (IEEE SA 2023).

What makes the metaverse are its features:

- the immersiveness of the experience (with varying degrees, such as 2D versus a full sensorial experience);
- the element of presence (the illusion that the environment you are in is plausibly reality);
- persistence (the virtual worlds continue to exist even when you are not online);
- the convergence of the physical with the virtual world and the effects of one world on the other;
- the interconnectedness and interoperability of the different virtual spaces.

The metaverse brings together and integrates various existing and emerging technologies – related to hardware and software – that provide the architecture and infrastructure needed for the metaverse to function, along with the underlying and enabling technologies that enable immersive experiences and further features of the metaverse. These technologies include, among others: 5G/6G networks that allow data transmission and connectivity; AI systems (AIS); digital twins (a digital or virtual copy of a physical system allowing for simulations and modelling); the Internet of Things (IoT – connecting different devices in the physical world and allowing their seamless connection to the virtual world); blockchain (an infrastructure using cryptography techniques allowing, for example, transactions of physical or digital/virtual assets, typically using cryptocurrencies); augmented reality (AR, which overlays information to the physical world either adding onto or hiding parts of the physical world); virtual reality (VR – providing through the use of devices like VR headsets an immersive experience separate from the physical environment); mixed reality (MR – combining elements of AR and VR); extended reality (XR – referring to ways humans interact with, experience and visually interpret the physical environment through a digital interface (IEEE SA 2022a) and encompassing technologies like AR, VR or spatial computing); and brain–computer/human–machine interfaces (BCI, HMI – a means of communication between humans and computers and a translation of user input into machine-readable commands). When used together or in new ways, these technologies create new applications and experiences. In the different future scenarios of the metaverse its scope and impact on offline life and the physical world vary, as do the potential threats and risks to the exercise of human rights and fundamental freedoms, the rule of law and democracy. These technologies are described in more detail in the section "Enabling technologies and building blocks of the metaverse".

It is important to bear in mind that the enabling technologies may change over time (for example with the use of brain–computer or human–machine interfaces) and they should be viewed as a means to implementation, while their technical specifications and features may be linked to specific benefits, risks and mitigation possibilities. In that sense, the metaverse is technology agnostic and involves the seamless transfer of data, in real-time, between the virtual and physical worlds (Agile Nations 2023).

Whether and how the vision for the metaverse will materialise and develop in the future will depend on several factors like adoption, technology development, access to data, regulation and geopolitics. Implementation and mass adoption of the metaverse are linked to some technical requirements and challenges which still need to be addressed. First, it requires great computing power, since existing interactive equipment demands a large computing load and high power consumption. Immersive and compelling end-user experiences, with low consumer and enterprise hardware price points, and low software application development costs are needed to drive end-user adoption of XR technology for the metaverse to be successful. Developments in the enabling metaverse technologies such as AI are expected to bring improvements in the performance, accessibility and user experience of the metaverse and newer headsets are then expected to supplant reliance on physical smartphones and monitors, while heralding new capabilities in augmented intelligence (Zheng at al. 2017), perception (Schraffenberger and Van der Heide 2014; Hugues, Fuchs and Nannipieri 2011; Schraffenberger 2018), embodied communication (Artanim 2020), productivity (McGill et al. 2020a), accessibility (McGill et al. 2020b) and more.

While avatars already exist (a virtual representation of self), digital humans represent a ground-breaking development in XR technology, bringing virtual beings to life with remarkable realism and interactivity. These photorealistic 3D human models have the potential to revolutionise various aspects of XR, including entertainment, education, communication and customer service. Digital humans can enhance immersive experiences by serving as virtual humans in different roles, like virtual assistants, guides or companions, providing users with a more engaging and personalised interaction within virtual environments. They also introduce new avenues for storytelling, allowing users to interact with virtual characters in ways that were previously unimaginable and creating in this way a new type of (social) interaction with AI-controlled agents. The rise of digital humans also raises ethical considerations, such as issues of identity, consent, privacy and the potential for misuse or deception.

Application areas

The metaverse, like the internet and artificial intelligence, is transversal, with different applications covering all aspects of life. It can be linked to goods and services (retail, gaming, social platforms, media) as part of the consumer metaverse; education and research; industry, manufacturing and engineering as part of the industrial metaverse; health, justice, e-government and political participation.

Currently many of the use cases are driven from the gaming industry, with existing big communities of users; however, there is a lot of emerging cross-pollination between various sectors, with industry-specific sectors such as automotive and manufacturing expanding to gaming, for instance. The industrial metaverse is an increasingly important application environment of the metaverse (MIT Technology Review Insights 2023, WEF 2023b). It involves a new industry model and operation system based on the core infrastructure and application concept of the metaverse that serves the industrial economy. The significance and purpose of the industrial metaverse is to generate practical value for specific industrial applications, representing through digital twins, for example, exact physical systems, while the consumer metaverse is based on a user experience with a sense of surrealism. The industrial metaverse will fully rely on digital identity, blockchain and other enablers to build a new generation of industrial systems, while it is expected to bring many benefits, with probably more immediate deployment and scaling up than the consumer metaverse (Nokia 2023).

The metaverse is poised to transform the field of medicine by introducing innovative approaches to diagnosis, treatment and patient care, as well as medical training and telemedicine. Surgeries, potentially involving brain stimulation, will be experienced in new and immersive ways. Of course, the benefits will need to be considered alongside any associated risks concerning patient rights, privacy and mental autonomy. The balance of the benefits and risks will also come under consideration in national and defence environments. In the United States, "metaverse-related ideas are already part of some of the latest military systems. The high-tech helmet for the new F-35 fighter jet, for instance, includes an augmented reality display that shows telemetry data and target information on top of video footage from around the aircraft" (Knight 2022).

Governments are also actively involved in metaverse activities. In 2022, the Government of Barbados approved the establishment of the world's first metaverse embassy, providing an immersive way for individuals to access e-government services in the metaverse (Atjam 2022). That same year, the Korean Ministry of Science and information and communication technology (ICT) announced an investment of at least €186.7 million to create its virtual worlds ecosystem. The US organisation National League of Cities (NLC) published a "Cities in the Metaverse" report outlining its vision of a future where US citizens can quickly and easily access services and gatherings via the metaverse (Petkov 2023). In Europe there has been investment in major initiatives, such as Destination Earth (DestinE), local digital twins for smart communities, the European Digital Twins of the Ocean (European DTO), the European electricity grid and the European Blockchain Services Infrastructure, aimed at enabling public authorities to make informed public policy decisions. Governments are also using immersive realities to support the tourism industry and for data intelligence purposes (Yfantis and Ntalianis 2022). Moreover, there has been some initial experimentation with using the metaverse in the field of justice, for example in Colombia where a hearing was held in the metaverse (Reuters 2023).

Education and learning experiences have the potential to be revolutionised in metaverse environments. Virtual classrooms and immersive simulations enable interactive and experiential learning, engaging students in ways that traditional methods cannot. Virtual museums and historical reconstructions transport learners to different time periods, enhancing their understanding and appreciation of cultural heritage. The metaverse facilitates new forms of social and cultural engagement, transcending physical boundaries.

Exciting possibilities exist in metaverse environments for promoting health, fitness and overall wellness. Virtual reality programmes provide engaging and immersive workout experiences, motivating users to stay active and adopt healthy lifestyles. Virtual fitness communities allow individuals to connect regardless of their physical location.

The metaverse presents a paradigm shift in entertainment experiences. Virtual reality and augmented reality technologies enable users to immerse themselves in interactive and dynamic virtual worlds, transcending traditional boundaries of passive consumption. Virtual gaming experiences within the metaverse offer unprecedented levels of interactivity and social engagement, creating vibrant virtual communities and economies. Virtual concerts, events and performances allow artists to reach global audiences in unique and immersive ways.

Additional examples of metaverse applications, as well as an analysis of some of the related strengths, weaknesses, opportunities and threats in some of the application areas, can be found in Appendix I.

While the metaverse could be viewed as yet another case of technology push (offering a new technology or product to the market to create a new need as opposed to answering a specific need), it offers both new experiences and alternative or improved ways of carrying out or delivering existing activities, services and experiences. Some immersive experiences are already used for socialising, entertainment, learning and working, for example with VR conferencing, gaming and training, VR social platform spaces and digital twin applications for remote collaboration in business and industrial settings (Sykownik et al. 2021). The need for enhanced online interactions in lieu of in-person interactions has been reinforced during the Covid-19 pandemic (Oh et al. 2023). As a study shows though, younger populations are not the only early adopters of the metaverse; half of millennials and Gen Zers consider online experiences a meaningful replacement for in-person experiences (Deloitte 2023). The global XR market is projected to attain a value of $446.6 billion by 2031, exhibiting a robust compound annual growth rate of 30.1% (Allied Market Research 2023). The markets are growing: 75% of the metaverse-related inventions since 2016 were filed for patent protection (as an indicator of intended market entry) in the United States (57%), the Republic of Korea (19%), China (12%) and Japan (8%) (Park 2022).

Is it too early to deal with the metaverse?

As the metaverse is an emerging area and its development could be accelerated through breakthroughs from adjacent technological developments (such as synthetic biology) or the scaling up of enabling technologies (like generative AI), accomplishing the groundwork in understanding existing and possible risks and benefits of this developing area and assessing its potential impact on human rights, the rule of law and democracy is not only prudential but advisable. Recent experience has shown that disruptions and the uptake of technology are difficult to predict. In addition, although the benefits of participation to users, user groups and even governments are many, harm in the metaverse is not hypothetical and has already manifested itself in early virtual environments, calling for responses and solutions. As such, the potential of the metaverse and its impact is best addressed now before the technology increases in both complexity and widespread adoption, thereby threatening its meaningful oversight. Despite recent hype with generative AI, metaverse-related strategies, policies, issues papers and responsible metaverse initiatives are underway, indicating that this is the right time to embark on related discussions.

Ethical considerations

Human rights, democratic values and ethical principles have begun to play a more prominent and explicit role in recent regulatory work even outside the human rights context. Examples include the proposed AI Act of the European Commission, what are known as socio-technical standards, while such principles are also often part of responsible innovation and human-centric governance approaches. This illustrates the interdependence of ethical values with legal frameworks and technology development and deployment. Ethical principles tend to be broader and could be viewed as a superset of human rights set in legal frameworks, legally binding and evolutionary, similar to societal values and ethics and with reciprocal impact. In the context of emerging technologies and responsible innovation, some experts argue that ethics should guide the development of new rights, such as "neuro rights", that is, those rights protecting the brain, its activity and brain data. Issues and challenges arising from the development and deployment of technology that are identified in this report include legal and ethical considerations. Some of them are already enshrined in human rights, but also reflect broader ethical principles and considerations, which are often used as guiding principles for instruments such as guidelines and recommendations, as well as binding frameworks.

The development of the EU AI Act is one example of how challenges regarding technology and regulation can play out. Issues and concerns were identified and discussed over a number of years with the complexity and involvement of different disciplines to cover different perspectives. The EC High-Level Expert Group on AI developed the Ethics Guidelines for trustworthy AI, which informed the text of the EC Proposal for an AI Act. It took years for the resulting AI Act to become more concrete and it has yet to be finalised, also suggesting that these policies and regulations need to be regularly updated. A similar process took place within the Ad hoc Committee on Artificial Intelligence (CAHAI) and the Committee on Artificial Intelligence (CAI) at the Council of Europe, with the development of the draft AI Convention (Council of Europe 2023b), currently under discussion.

Established ethical principles in the AI space, promoted by frameworks like the IEEE's Ethically Aligned Design (IEEE SA 2016) and CertifAIEd, by UNESCO or by the Organisation for Economic Co-operation and Development (OECD), can also play a foundational role in the guidance of standards, certification and regulatory approaches for the metaverse. Compared to AI, these principles are expected to produce novel issues when applied to the metaverse; especially considering the differences in context and application domain, the complexity resulting from the globalised value chain and the diversity of technologies, cultures, societal norms and practices that will intersect in the metaverse.

From an ethical perspective, the risk landscape of the metaverse is diverse and must be assessed in terms of what it affords (benefits) and how it impacts both people and the planet (risks). This analysis must not be conducted in a vacuum. It must incorporate short, medium and long-term risks and impact, and consider the surrounding and supportive technologies of the metaverse and related issues.

Whereas some of these issues may be linked to existing legal and ethical considerations and frameworks, the metaverse also ushers in the need to consider the increasingly ambiguous boundary between the physical world and virtual harm. The metaverse also presents at least three novel and ethically salient problems: the role, legal status and treatment of digital humans (see the section on identity); the prospect of virtual abundance and its impact on concepts of justice in the metaverse (see the section on rule of law and democracy); and the expanded threat to mental autonomy and privacy via technologies used to access the metaverse.

Early development of the metaverse has been accomplished by a few large companies and nation states. If this trend persists, these players may have persistent and considerable power to control access, conduct and data of users globally. The fair and inclusive ownership, transparency, liability, accountability and control of the metaverse are pressing ethical concerns, and the risks are acute for vulnerable populations already subject to violence and discrimination in the real world. Further considerations are expected to emerge in areas of traditional state access and control, on the expectations, roles and responsibilities of different stakeholders of the metaverse ecosystem, considering the new dynamics that are being created.

The incorporation of ethics into the technology space was characterised until recently by its voluntary nature, by self-governance and by the adoption of industry alliances and framework-based initiatives by major technology companies as part of responsible innovation approaches. In the meantime, different jurisdictions and international organisations have been developing legal frameworks that are often fragmented. In the future, governments (individually and collectively) are expected to have a leading role in providing policy frameworks that successfully audit the extent to which these pledges and self-governance mechanisms effectively address identified metaverse-related harms, which can also be transboundary in nature.

Some government actors and international institutions have begun work on metaverse-specific frameworks aimed at the prevention of specific harm and the promotion of core ethical principles, including South Korea, the Agile Nations, the World Economic Forum (WEF) and the OECD, while Chile has incorporated neuro rights into its constitution.

Extensive stakeholder collaboration, including input from users and civil society, will be essential in shaping the metaverse in such a way that it is consistent in adhering to existing legislation and aligns with ethics and societal well-being globally. Proactive and co-operative ethical analysis is likely to be key to harnessing the metaverse's benefits on a global scale.

Chapter 2

Impact on human rights

In moments of heightened concern about the potential impact of emerging technologies on society, the value of safeguarding human rights, the rule of law and democracy becomes evident – as demonstrated by the response of the Council of Europe to other technological developments. This is also the case when considering the ways in which metaverse environments can and are changing how individuals, communities and societies interact. Some of the technologies involved in the metaverse have already been deployed and are linked to known issues and previous areas of work of the Council of Europe. The respect for fundamental rights and freedoms and for the principles of legality, legal certainty, prevention of abuse of powers, equality and access to justice are essential to ensure that the rule of law is not compromised when technologies with disruptive potential are developed and widely shared in markets. The metaverse environment is expected to exacerbate related concerns due to its immersive and invasive nature, requiring considerations to ensure the development and provision of a safe and productive space for society. Activities that are governed by law should provide the safeguards and remedies to ensure due prevention and protection against unlawful behaviour in the metaverse and to make the authors of such acts accountable. These concerns apply to issues related to privacy, identity, free expression, anti-discrimination, inclusion, diversity, accessibility, labour, political participation, social interactions, health, the environment and, importantly, children's rights.

Privacy and data protection

Immersive experiences most often take place in highly personalised and responsive user environments. Metaverse-enabling hardware is equipped with sensors that collect, process and create an unprecedented volume and range of data to drive key metaverse functionalities, including physiological, psychological and biometric data like pulse, breathing, temperature, eye movement/tracking (Kroger et al. 2020), facial expressions, gait and gestures, voice (Baxter et al. 2021; Chopra and Maurer 2020) and brainwaves. In just 20 minutes using a VR headset, roughly two million points of biometric data are collected (Khan 2022; Bailenson 2018). This results in more intrusive, or what some call requisite sensing (O'Hagan et al. 2023). These data provide insights into new frontiers such as users' mental and cognitive processes and phenomenological experiences (Heller 2020; Ienca 2017), as well as affective states, behavioural patterns and preferences (Kroger at al. 2020). User profiling for recommendation systems and highly customised experiences are now reaching new levels; referred to as "biometric psychography", this allows for easier collection of behavioural information of the user (Abraham et al. 2022), for unique identification (Moore et al. 2021) and more (McGill 2021). Such collection and processing of data needed for personalised experiences could be considered sensitive in the sense of

Article 6 of Convention 108, the Council of Europe convention on data protection. Privacy concerns are thus exacerbated in the metaverse context. Privacy protection (Article 8 the Convention) remains essential, especially considering potential issues related to concept of anonymity.

The increased appetite for data collection and processing is tied to a lucrative data brokerage industry, generating billions in revenue (Boutin 2016) for profiling, recommendations and advertising, despite many uncertainties about ownership of the data and related access rights. Privacy has been respected for thoughts and leisure, yet new invasive biometric technologies might challenge this in the future (Majerova and Pera 2022). While a lot of attention goes to data and data protection (Renieris 2023), there are further concerns tied to the freedom of thought (Article 9 of the Convention), mental privacy and autonomy/integrity. The Neurorights Foundation advocates a common UN framework for the protection of neuro rights and the monitoring of ethical developments in neurotechnology (Genser, Yuste and Herrmann 2021). The foundation proposed the following rights: the right to mental identity, mental agency, mental privacy and the right to fair access to mental augmentation. Moreover, there is a higher risk of discrimination or attacks affecting the dignity and identity of users when sensitive data become available, and a threat to access to information and freedom of thought if as a result of profiling and recommendation systems they are only shown a specific subset of the available resources and thus are deprived of certain information, what often serves as a basis for misinformation. There is a consideration of rights protecting our perception and the acceptable limits of perceptual mediation. These rights include perceptual autonomy (right to control what you perceive); cognitive autonomy (tensioning the right to free will and independence of thoughts against non-consensual manipulation through AR); and perceptual integrity, related to the extent to which users have the right to augment property, media and places, thus undermining the integrity of a common objective reality we all perceive.

Informed consent for data collection, processing and use is a challenging area. Even though passive acceptance of terms of service has been ruled out as unlawful practice in the context of social media, for example, and while recent European and US case law (CJEU 2023) have set stricter requirements on what constitutes "informed consent" for an active opt-in, problems persist – especially where personal information of children is involved. User awareness and understanding of the extent and types of data collection involved and the expected and authorised use of these data are not always well understood, in particular considering the capacity of some devices to carry out "persistent, ubiquitous recording" (Chatila and Havens 2019). Questions on how free and informed even specific consent could be are in particular raised in cases of power imbalances between a data subject and a data controller (see, among others, the Council of Europe Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data 2017).

The privacy and data protection of children, and other vulnerable groups who may not be aware of the risks and consequences or of their rights, especially related to the capture of biometric information or mental activity, merit particular attention and action. The Council of Europe made a call to step up the protection of children's privacy in the digital environment and their data protection with its

Recommendation CM/Rec(2018)7 on Guidelines to respect, protect and fulfil the rights of the child in the digital environment. They have also issued the Guidelines for children's data protection in an education setting (2021) and a special report on children with disabilities in the digital environment (2019).

Age-appropriate design principles (as included in the UK Age Appropriate Design code – ICO 2020), grounded in the UN Convention on the Rights of the Child and its General comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, are essential to the protection of young people and vulnerable persons in the digital age. These principles should be explored for the metaverse, and a child-centric design considered to address the privacy of children and their data protection. Similar considerations are needed for vulnerable populations such as the elderly, as well as persons with cognitive functional limitations, limited digital literacy or language barriers. Related work of the Council of Europe, besides Convention 108 (and its 2018 amending protocol establishing international standards that guarantee individuals the right to privacy and the protection of personal data, regardless of technological developments), includes Recommendation CM/Rec(2010)13 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, posing the question of necessity of collection and processing of sensitive data for a lawful and specific purpose, which would have to be assessed in the metaverse context.

"Worldscraping", a term coined by Adrian Hon, refers to data collection from private spaces, like individual homes, which were traditionally considered private (O'Hagan et al. 2023). However, with the unintended access to information (location, standard of living, personal preferences, etc.) through the sensors that enable immersive experiences, the definitions and boundaries between private and public spaces, and the meaning of consent for accessing and using related information, blur, raising concerns about "reasonable privacy". Privacy concerns in the metaverse extend to workplaces, civic and academic settings. Without the appropriate safeguards in place, the risk of biases, discrimination and exploitative practices due to the increasing use of biometric data and lack of research standards increases.

Consent and privacy are even more complex for bystanders – people who happen to be in the space where the metaverse user is physically based **–** along with the environment around them (O'Hagan et al. 2023; Rodriguez and Opsahl 2020; Ahmed et al. 2018; Harborth and Pape 2021). Bystanders lack the capacity to consent or be aware of XR headset activities that may involve them, potentially leading to constant surveillance. XR devices are capable of possibly sensing the biometric data of these bystanders as well (inferring identity from their gait, for example; Moore et al. 2021) and could obtain non-contact physiological data (Shao, Liu and Tsow 2021), capture and augment appearance (Rixen et al. 2021; Kyto, Hirskyj-Douglas and McGookin 2021), collect instrument behaviour and actions (Nassauer and Legewie 2021) and more. This surveillance of others (Mann 2013) may lead to an erosion of their reasonable expectation of privacy (Franks 2017), supporting "cyborg stalkers" (Khamis and Alt 2021) and creating a global panopticon society (Rodriguez and Opsahl 2020). This calls for a multidisciplinary dialogue to assess the technical feasibility of addressing this issue and public awareness about privacy concerns and the new connotations of expected privacy and data security in the metaverse context.

A further perspective to consider is that of anonymity. It can on one side protect privacy, for example, through an avatar that does not disclose certain aspects of an individual's identity. It can also be used to cloak inappropriate behaviour or crimes. Further privacy concerns are linked to safety and security, which may be threatened by third parties or even platform providers. In the metaverse environment it could be more complicated to implement the "right to be forgotten" (erasure right), which is considered part of the right to protection of private life, recognised in the General Data Protection Regulation (GDPR) at the EU level and addressed in the case law of the Court – see, for example, *Hurbain v. Belgium [GC]*, Application No. 57292/16.

Information and data that are needed for intended functionality in the metaverse must be considered alongside what may be collected unintentionally or without user consent. Legal rules, ethical guidelines and technical standards may help ensure transparent data practices, in particular in cross-border data transfer, data sharing and portability across different applications. In addition, informed consent, a user-centric approach, strong cybersecurity measures and user agency and control of personal information should be considered in the metaverse. A further issue for discussion would be the role of supervisory authorities and enforcement entities, in particular considering the complexities that fragmented approaches can bring in cases of cross-border or global enforcement of privacy and data protections.

Identity

Identity in the metaverse goes beyond an online profile: it is the digital embodiment of a person, visually represented as avatars, ranging from simple 2D representations to complex 3D models customised to reflect physical features, personality, expression of social-cultural affiliation and preferences, among other things. When persons interact and engage with others in the metaverse as game, social network or other application users, their identity plays a significant role in social interaction, privacy, security and overall experience. At the product design stage, developers should consider an inclusive design approach to ensure software application users are able to represent their personal characteristics and status in a way that allows free expression, inclusion and protection from discrimination, even more so when combined with anonymity, although anonymity can raise some security concerns. Behaviourally, human actions and interactions can become integrated with virtual personas. That can also entail risks, such as impersonation and identity fraud or adherence to perpetual expectations in terms of physical appearance, which may in fact jeopardise diversity and inclusion. These risks are increased for children and other vulnerable populations. The Cybercrime Convention Committee of the Council of Europe adopted in 2013 its guidance note on identity theft and phishing in relation to fraud, which in the metaverse context could take place through virtual doppelgangers for instance.[1] This note shows how different articles of the Budapest Convention apply to identity theft in a fraud context involving computer systems.

[1] For an overview of digital entities which may be part of metaverse interactions see also WEF 2024, even if related terminology is not yet harmonised.

In the metaverse environment, the awareness of the identity of others could be important when this information is used for compliance or identification purposes, for example recognising an employee or for age verification of users of avatars, and related minor protection. To help verify identity as well as attribute a violation of human rights to a specific stakeholder, one approach could be matching a physical ID to a digital one, with technologies such as decentralised identifiers (DID), including identifiers for corresponding avatar(s), which could be further broken down to a series of codes representing different features of an avatar. Related provisions in the EU Digital Services Act could serve as inspiration, while authentication could be managed by an independent body that could ensure greater co-ordination and consistency across platforms. The need for identification of users in the metaverse was identified as a priority area for debate by the European Parliament among others in an early 2024 resolution (European Parliament 2024).

Equally important is the information on whether a presented identity – an avatar, a digital human (an advanced version of an avatar that reflects not only the physical but also behavioural aspects of an individual) or a virtual human (a digital human with a specific function such as customer service or human resources assistant) is controlled by a human or is an AI agent. Thanks to advanced AI techniques like large-scale multi-modal learning it is possible to process and understand different types of information (images, audio, semantic), allowing for an increasingly natural interaction, which paired with increased photorealism can create confusion, foremost when user identity and nature is disguised. It is plausible that the metaverse, in conjunction with enabling technologies such as generative AI, will be populated by digital humans and virtual AI agents capable of impressive interactive capacities that may pursue human (or corporate) ends and may not necessarily be transparent to the humans they engage with (Bryson 2010; Evans, Robbins and Bryson 2023). According to findings from the Council of Europe, there have already been documented cases of AI generating child sex abuse materials with extremely explicit, vulgar and dangerous material. This raises several issues, including attribution of responsibility and accountability for violations of human rights in the metaverse and the jurisdiction and law applicable to agents in the metaverse, linked also to the legal nature of such agents/virtual humans. Personhood of digital humans, an issue also found in the AI systems (AIS) context, should be considered carefully as it could lead to complex and potentially dangerous conclusions, such as the recognition of human rights for AI agents.

A series of legal questions arise, including the right to access and ownership of one's own virtual representation/avatar (related data) and the right to amend the view of others without their consent (right to identity v. free expression) and related platform accountability. A right to be informed, recognised to date for user data held by public authorities, could come into question to provide transparency in the interaction.

The capability to augment the ways in which we or others are perceived can be risky considering the pressure users often feel to make their appearance conform to perpetuated ideals (Barker 2020; Ryan-Mosley 2021). This capability could enable new forms of abuse for malicious users. Beyond "identity hacks" such as identity theft (Slater et al. 2020), it is easy to envisage a convergence of AR sensing and cheap/deep fake technology (Chesney and Citron 2019) to, for example, generate synthetic identity and add a behavioural and more deceiving component to deepfakes (EUROPOL 2022), to sexualise (Citron 2018) or otherwise appropriate the identity of others for socially unacceptable reasons (for example black face filters; Joshi 2021). Lemley and Volokh (2017) considered the legality of this ability to augment a personal "sensescape" and the "sensescapes" of others, asking: "What if people use this ... to make [you] appear ridiculous ... without your knowledge or consent? Or what if they want to make you appear naked?" (Lemley and Volokh 2017). Should such views, hacks or layers be shared with others; is this a form of expression, or a publication for which the user and/or platform may be held accountable? And what kind of protections/remedies should be in place in the metaverse and outside it? Who should provide those protections? How can users be made aware of such dangers? Will they give informed consent to such exposure when entering the metaverse? These are some of the questions which may arise from such behaviours.

The psychologically and often damaging reaction from the perception of self (or portraying of self by others), others and the surrounding reality and how this may alter through constant exposure to an immersive environment is an evolving concept. With the emergence of different virtual spaces and avatar technologies, another aspect will be the consistency of an identity across different platforms and applications, posing the questions of portability, transferability of an identity and its data, compatibility and interoperability across different platforms and the relationship/treatment of multiple avatars and identities on the same platform or across platforms and the interplay between virtual and non-virtual identity.

Where identity data ownership is concerned, related legal and technological frameworks are not yet fully developed, hindering its full value realisation and depriving users of complete control over the flow and use of their identity data, which may lead to data and privacy disclosure and legacy issues and put identity security at risk.

Identity within the metaverse is a multifaceted and evolving concept that requires careful attention to technical, legal, ethical and policy considerations. Creating a strong framework and drawing from experiences with other technologies can help establish a responsible and user-centric metaverse identity ecosystem. Individuals should have a clear understanding and control of their digital identities, which may require rethinking human rights in the digital age. Through collaboration, education and regulation, risks can be mitigated, individual rights protected and a metaverse created that aligns with democratic principles and respects human dignity.

Free expression, content and behaviour moderation and safety

Virtual and immersive environments create new spaces for free expression. At the same time, they could also be used in ways that could compromise the right to safety, such as for bullying, hate speech, discrimination, (sexual) harassment and other types of violence and assault. Behavioural moderation becomes relevant in addition to content moderation when moving from digital to virtual worlds.

The immersive nature of the metaverse causes more intense perceptions than other online environments, especially when it comes to threats and their psychological effects – both in the virtual and the physical worlds. Freedom of expression is covered by Article 10 of the Convention, while the rights to personal and family life and non-discrimination are covered by Articles 8 and 14 of the Convention, with substantial case law from the Court on the question of responsibility and accountability for all content published online and especially social media (see also Spano 2017). Respective principles could apply in the metaverse. Content and behaviour moderation are more challenging in real-time environments, especially as much of this work is outsourced, but the Council of Europe recommendation on combating hate speech, the Council of Europe guidance note on content moderation and the Council of Europe Recommendation CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries should be explored to assess whether the principles and recommendations included therein could be directly applied or whether additional aspects would need to be taken into account.

The current digital era is marked by threats to some of the foundations of democracy, such as the role of active citizens, shared culture, free elections and trust in authority. This is driven by the manipulation of digital content, fake news and misinformation, which create filter bubbles and echo chambers (Flaxman, Goel and Rao 2016) and have the potential to incite hate or manipulate beliefs. Metaverse technologies could be used in unprecedented ways to persuade and manipulate (Pase 2012), including virtual agents who may be highly manipulative in promoting third party agendas in virtual real-time environments while not disclosing they are not authentic users (Rosenberg 2023). Metaverse-enabling technologies could thus become the *de facto* gatekeepers of human perception based on: user preferences (reinforcing biases and political leaning); biometric psychography (Heller 2020; Bye 2021); gatekeepers' interests (such as advertising); government mandates (propaganda, for instance); actions (through body tracking, context awareness etc; O'Hagan et al. 2022); or even an intention to act (through EEG-based analysis (Schurger et al. 2021)). This could result in enhanced behavioural nudging (Hummel and Maedche 2019; Schmidt and Engelen 2020), deceptive design (Mathur, Mayer and Kshirsagar 2021), the manipulation of actions (Tseng et al. 2022) and even change of preference (Franklin et al. 2022).

XR devices have the unique capability to control users' perceptions of reality through visual, auditory and haptic stimuli, allowing different stakeholders including the headset wearer, owner, vendor or governments, to remove, obfuscate or alter real-world content (diminished or altered reality). This makes them function as a *de facto* filter of the perceived reality of the user (AR) or create an illusion of a completely distinct virtual environment (VR) (Gonzalez-Franco and Lanier 2017).

This directed behaviour change may be overt (enacted through persuasion or positive reinforcement) or covert (via coercion or imperceptible manipulation, nudging), a concern that is elevated when considering the influences that these manipulations could have on children, adolescents and young adults as they go through the process of forming their personalities and opinions. While these manipulations, either consensual or imperceptible to the user, are currently used to enhance XR experiences, they could potentially harm users and give rise to dark and deceptive design patterns, such as change of attitude, biases or political exploitation, affecting political participation and global citizenship behaviours. Unlike digital disinformation limited to web-based social media, the metaverse can embed such manipulation into everyday experiences on a much larger scale. In such cases, it becomes questionable what freedom of expression, or even freedom of thought (see below), means.

Metaverse environments allow for extensive customisation based on user preferences (which may have been stated or revealed) and habits, using selection predictions like those used in social media to shape user experiences. Companies can use targeted virtual advertising based on contextual and psychographic data (DeGeurin 2022), forcing users to interact with immersive and constant advertising (Masnick 2014), with a consideration of an opt-out mechanism to allow a certain degree of choice. This customisation will create entirely new virtual realities for users that will influence purchase habits and behaviour, as well as personal experiences and even world views (how reality, history, etc. are perceived). Biases in data collection and use might exacerbate inequalities in experiences and the opportunities provided to users in their metaverse environments (see the relevant section on inclusion, diversity and accessibility). Emerging legislation like the EU's AI Act seeks to address such risks by banning AI systems that manipulate persons through subliminal techniques or exploit vulnerable individuals. However, these protections may not fully consider the unique capabilities of everyday augmented AR or VR, which can understand, manipulate or deceive users overtly and even with their consent, which may not be captured through risk categorisation. Additionally, if power in the metaverse is concentrated and controlled by a few technology companies, risks to pluralism and free expression could lead in some cases to *de facto* censorship and a threat to democracy.

Perceptual manipulation techniques require a fundamental re-evaluation by states and public authorities of the permissible digital content presented to users in XR to ensure perceptual integrity. Avoiding the creation of deceptive design patterns is crucial, and introduction of related limitations and rules may be necessary. The unique types of nudging that XR enables, such as controlling users' physical movement, should be thoroughly understood before the technology gains widespread acceptance among the general population.

Due to the prevalence of manipulation and the possibilities of misinformation, the meaning of freedom of thought (Article 9 of the Convention) should be explored in the metaverse context, along with freedom from interference in the thinking process and freedom of choice. In order to protect mental autonomy and human agency, some experts are discussing the need for the "neuro rights" (meant to safeguard independent clear thinking and critical thinking by limiting external sources of manipulation).

The metaverse can provide new channels for mass communication and as such related aspects should be considered in discussions around new notions of media (in line with Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media). The role of different actors (including who could be impacting people's right to seek, receive and impart information, in accordance with Article 10 of the Convention) should also be assessed. What freedom of expression and media freedom mean in the virtual realm will need to be understood. Sometimes the exercise of these rights may be in conflict with another right protected under the Convention, and the Court needs to assess whether the right balance was struck by national authorities, for example with the rights to privacy and data protection (Guide on Article 10 of the European Convention on Human Rights 2022). Special cases could be made for journalists and citizens who may be sharing information in the public interest via different virtual channels – decisions may need to be taken, on a case-by-case basis, on whether journalists are allowed to derogate from basic data-protection principles.

Another feature of the metaverse design that lends itself to greater misinformation vulnerability is the use of avatars in social interaction. Engagement with and between avatars may foster a greater sense of social presence and connection than is common within traditional online environments (Fox and McEwan 2017). Further, avatars may be designed or customised with the express purpose of influencing or manipulating individuals, and thus features such as the photorealism (Yuan et al. 2019) or facial expression (Luo et al. 2022) of the avatar could impact the perceived trustworthiness of the avatar. In addition to this, the immersive nature of the metaverse may intensify the impact of social validation, as users may feel greater pressure to conform to the beliefs and opinions expressed by avatars in the virtual space. At the moment, research within this area is preliminary and thus there are various unknowns about the way social interactions via the medium of avatars may pose risks to the acceptance or spread of misinformation within the metaverse.

Some concerns related to the potential impact of metaverse technologies on misinformation and fake news, which may pose threats to the rule of law and democracy, include the following:

- disinformation threats, such as conspiracy narratives;
- terrorist or violent extremist content, including terrorist propaganda, which directly seeks to spread and support anti-democratic movements, overthrow the constitutional order of states or promote acts of terror;
- fraud resulting from misinformation and fake news;
- the use of cryptocurrencies for money laundering in the absence of any anti-money-laundering regulation in the metaverse.

Considerations to address misinformation and disinformation and the spread of fake news include authentication (in particular from public authorities) and watermarking of original content (White House 2023) while, with regard to crypto-assets, it will be important for the European space to monitor how they will be regulated by the new Markets in Crypto-Assets (MiCA) Regulation and how this may impact related concerns in the metaverse.

Inclusion, diversity and accessibility

The prohibition of discrimination is enshrined at the Council of Europe level in Article 14 of the Convention (only in relation to the exercise of another right guaranteed by the Convention) and under Protocol No. 12 to the Convention. The immersiveness and location independence of the metaverse can support inclusion and the access of remote, vulnerable and marginalised populations to different experiences and aspects of life, allowing them to benefit from its potential.

One example is virtual concerts, which allow for increased participation of individuals with functional limitations. However, with this greater virtual access comes the risk that physical venues may use virtual alternatives and virtual accessibility as an excuse to avoid accommodating people with functional limitations. This could lead to the exclusion of some individuals who are left with virtual-only options (similar considerations may be applicable to other groups for different grounds of discrimination). Immersive or virtual inclusion should not be seen as a substitute for accessibility in the physical world and should not be allowed to lead to or result in offline exclusion; both options should co-exist and the choice should be left to the individual, where possible, for a truly inclusive experience.

At the same time, lack of required infrastructure and the cost of hardware pose the risk of an exacerbated digital divide, which could leave a significant part of the global population behind and unrepresented in the metaverse, threatening the exercise of basic freedoms and rights and an inclusive and democratic metaverse. Because VR/AR hardware could be considered emerging assistive technology (WIPO 2021), providing access to such devices to persons with functional limitations could be viewed from a human rights perspective and as a state obligation as per the UN Convention on the Rights of Persons with Disabilities. The cost of the devices would be expected to drop with mass adoption of the metaverse, yet the least privileged regions, individuals and groups would be the last to benefit and in the meantime be excluded from the benefits of the metaverse. Furthermore, existing disparities (because of age, gender, functional limitations, language or other personal characteristics or status) will persist and are likely to be perpetuated and amplified in the virtual world, leaving many experiences out of reach to those most in need of them.

As the metaverse is expected to become a virtual society, its design should resonate with both online and offline communities. Lack of representation of groups like the elderly or persons with functional limitations could create a distorted version of the world and further exacerbate bias and discrimination, with potentially serious implications for children and young people whose world views and values are being shaped by the technologies they are exposed to. The potential exclusion of non-English speakers in the metaverse also needs to be prevented. Technology should be used to facilitate language translation. AI-powered translation, speech-to text and speech-to-speech technologies can help address this issue and make the metaverse more inclusive.

Inclusive design helps to promote the participation of persons with disabilities in the metaverse by involving them in the development process, resulting in a more inclusive and accommodating virtual environment. Collaborating with disability advocacy organisations can be vital for a better awareness of disability diversity and an understanding of requirements and needs. The compatibility and interoperability of metaverse hardware and software with the assistive technology used by individuals with functional limitations also needs to be addressed since assistive technologies will still be needed to allow participation in the metaverse. Some accessibility features may be more challenging to implement in the metaverse, such as captioning, and may require additional considerations, guidelines and standards. Inclusion should also be considered in avatar design to ensure adequate representation not just of individuals with disabilities (EDF 2018) but also of under-represented or marginalised groups. Furthermore, the design of wearables should consider more women and young users, as poor fitting leads to "cybersickness" and thus exclusion. While having such a broad range of user profiles and needs may pose challenges to technology developers, the advanced sensors used in the metaverse and the customisation and personalisation allowed could contribute to more adequate and inclusive virtual environments.

Considering that AI systems are a major enabler of the metaverse, there is the risk of discrimination due to bias in used datasets, which can affect minority groups and under-represented individuals and communities because of input at the algorithmic level. This can lead to algorithmic stereotyping and digital violence against women, among other things (see the Council of Europe study on the impact of artificial intelligence, its potential for promoting equality, including gender equality and the potential risks in relation to non-discrimination 2023; Istanbul Convention). Such bias should be mitigated to avoid its permeation across the entire metaverse landscape. Addressing bias will yield a more inclusive and equitable metaverse as well as a more responsible and socially beneficial metaverse landscape. Still, some initial studies show that women, while they tend to be more engaged in the metaverse as consumers and leaders, receive less funding for metaverse-related projects and are excluded from metaverse leadership positions (McKinsey 2022b), a reality already experienced in the offline world. The Council of Europe, in its Recommendation CM/Rec(2019)1 on preventing and combating sexism, stresses that "the internet has provided a new dimension for the expression and transmission of sexism", and further steps may be needed to avoid this phenomenon being exacerbated in the metaverse. Some considerations may need to be taken even in overlooked areas such as the posture of avatars, which may reinforce unconscious bias against women and gender stereotyping.

As virtual worlds and immersive realities are adopted across different fields, individuals who have reservations or who avoid the metaverse for health or other reasons may be forced to choose between engaging or being left out. As with the internet, social pressure may apply and participating in the metaverse may even become a requirement to participate in education, work and cultural life. The private ownership of virtual spaces and the transition to digital public spaces and services will add further layers to the access issue and tackling these issues may require a global strategy.

Labour

The European Social Charter acknowledges the right to work and fair conditions, including health and safety. With the metaverse, new challenges will arise that are expected to drastically change labour conditions and affect well-being and society and that therefore require careful policy considerations.

The metaverse is expected to contribute significantly to global GDP, with growth worth an estimated 800 billion euros by 2030, and to transform the employment sector, with the potential to create 860 000 new jobs by 2025 (European Commission 2023). The adoption of virtual reality in the workplace is expected to bring numerous advantages, including flexibility, time and cost savings, reduced CO_2 emissions and access to a global talent pool (WEF 2023d), addressing scarcity in certain geographies (WEF 2023a). It will benefit remote and ageing populations, including people with disabilities. However, challenges remain, as a large portion of the world's population lacks internet access and the necessary skills to fully exploit these opportunities.

Employee interest groups like trade unions and work councils can utilise metaverse environments to facilitate social gatherings and interactions, making it easier for workers to organise and represent their interests, such as wages and safety. Enforcing an employer's duty to protect employees' occupational safety within the metaverse may present challenges, so having access to these interest groups that can advocate better worker safety and other rights could provide a necessary balance.

Working in the metaverse comes with some disadvantages, similar to digital work. It can blur the boundary between personal and professional life, making it challenging for carers, mostly women, to manage distractions and maintain work–life balance. Ergonomic working conditions may not be provided by employers, leading to potential physical and mental health issues. The lack of regulations on maximum working hours and needed breaks can exacerbate the negative impact on employees' well-being, especially if they feel constantly monitored. Additionally, recruitment processes in the metaverse could widen the digital divide by excluding candidates who lack access to the necessary hardware.

Incorporating the metaverse into the workplace raises concerns about employee privacy, as it involves data processing and (potentially constant) monitoring. Employers will need to strike a balance between ensuring professional conduct and respecting employee privacy. Special data-protection requirements have been partially established to address the legal concerns associated with data processing in employment relationships, considering the power imbalance between employer and employee. These will require ongoing attention.

Participation in the metaverse involves creating an avatar, which can be seen as a digital expression of the right of personality. For workers with disabilities, the avatar can give them the means to choose whether to disclose their disability and prevent discrimination. While employers may have limited influence over the avatar's design, they may request a professional presentation to maintain uniformity and recognisability among colleagues and customers.

The increased use of the metaverse and the AI that drives the experiences and services may lead to changes in the perceived value of existing skill sets, making labour a commodity product and creating obstacles to maintaining livelihoods in creator economies that are based on microtransactions. The metaverse, relying on AI, may lead to a significant increase in income inequality, impacting up to 70% of the wage structure (Acemoglu and Restrepo 2021) and making fair compensation challenging. During the Covid-19 pandemic, four billion people were not adequately protected from job losses (ILO 2021), highlighting the need to prepare the labour force for changing landscapes in order to avoid potential losses amounting to trillions of dollars (RAND Europe and Salesforce 2021). The challenge lies in identifying who will undertake the responsibility of preparing the workforce and determining the required skills for the future, which are continually evolving (Stephens et al. 2019).

Because of its borderless nature, determining the applicable laws in the metaverse is complex. The principle of territoriality is challenging to apply and multiple factors like employee residence, company headquarters and server location come into play. A multinational effort is needed to create a clear legal framework involving employers, employees, regulators and policy makers.

Political and social participation

The metaverse offers opportunities for increased political representation and the participation of marginalised communities in civic and political activities. Because governments and politicians follow popular platforms and bring their messaging into virtual worlds, crossing over from activity in online platforms into the metaverse is a likely continuation of an established trajectory. Governments are planning for the related consequences and changes, such as creating positions like a "Web3 minister" to address the challenges related to the entry into the metaverse (Petkov 2023). However, increased use of the metaverse in political environments also comes with risks. While the metaverse can amplify grass-roots voices, it can also drown them out (Miazhevich 2015). As with existing platforms, (sexual) harassment, hate speech, etc., present challenges to maintaining a fair and transparent political environment.

In virtual worlds, political opponents could be visually or audibly "blocked" or censored (Tibbets and Brooker 2014; Melnick 2022) and informational media could be augmented to create confusion (as in newspapers, magazines and augmented TV; Saeghe et al. 2022), for example with the use of deep fakes. Social augmentations could be used to spread political messages in targeted communities or suppress voter engagement through obfuscation and alteration of voting stations (ACLU 2021). Disinformation and conspiracy narratives can also result in or deepen polarisation or undermine inclusion and equality in a community, fuelling hate speech, bullying and harassment. This can affect the safety of the metaverse for those targeted and lead to their exclusion.

The availability of metaverse infrastructure, resources and technologies to countries with more access to the metaverse (currently 35% of the world population) could potentially lead to a larger influence by these countries over others in this space (Ericsson 2022). Additionally, the concentration of patents and metaverse companies in a few jurisdictions may lead to a political representation that not all countries endorse.

Similarly, limited language representation in online platforms (Bhutada 2021) and the web in general (Brandom 2023) is linked to the concern that the world may converge, leaving only a few prominent languages used in the virtual realm which could have a greatly detrimental effect on regional and minority languages protected by the Council of Europe's Charter for Regional or Minority Languages. To govern the metaverse effectively, it is crucial to increase language representation and ensure linguistic justice by removing bias based on linguistics. Representing national culture in virtual spaces of political participation can also be challenging as cultural norms and engagement differ across regions. Misalignments with national culture, including of national minorities and their languages, can impact user engagement (Prakash and Majumdar 2021). Culture can also be formed within gaming and social networking communities, who may also wish to express their perspectives politically. Governments are exploring how they want to be represented in the metaverse, with some, like Barbados (Wyss 2021), setting up consulates in virtual spaces and others, like Tuvalu, migrating their governments to the metaverse.

In the Council of Europe's framework, social participation involves the active involvement of individuals and civil society in public affairs at various levels. Key to this approach is the adoption of policies and measures, as outlined in Recommendation CM/Rec(2018)4 and in guidelines from September 2017 aimed at enhancing citizen participation in local public life and establishing effective dialogue and co-operation between civil society and government authorities. These policies are underpinned by practical tools like the CLEAR self-assessment tool and Civil Participation in Decision Making toolkits, designed to assist local authorities to bolster civil participation. Participation is also one of the guiding principles of the Convention on the Rights of the Child. The Council of Europe emphasises youth participation in policy-making processes to have their voices heard, for instance through co-management systems, where youth NGOs and government officials collaboratively develop and recommend youth policies (Council of Europe, Civil Participation in Decision Making).

Digital environments can enhance or transform traditional mechanisms of citizen engagement. The principles of citizen involvement could extend to virtual spaces, offering virtual avenues for citizen participation and dialogue between civil society and authorities. Similarly, co-management models involving young people, like Arnstein's ladder of participation, could find new expressions in the metaverse, allowing for more inclusive and diverse forms of civic engagement, especially among younger demographics who are often more attuned to digital environments.

Social interaction and community building

The metaverse, though not entirely novel in its aim of fostering social interactions and building immersive communities, distinguishes itself by its advanced technological capabilities, immersiveness and potentially seamless transition from one type of social interaction to another. It allows for social engagements and community building in a more intuitive and engaging way. The potential for disintermediated communication allows for peer-to-peer communication without gatekeepers and traditional central authorities. This can foster trust, freedom of expression and user control, but at the same time raises concerns about privacy, information integrity and security, requiring new approaches to content moderation and community management. While in social media everything relates to content, which tends to be addressed more easily, in the metaverse everything relates to conduct/behaviour, which is more complex. For this reason, safety needs to be considered more carefully at the design stage, as well as agency, choice, identity and empowerment.

The emergence of virtual societies provides users with opportunities to develop new relationships, collaborate on projects and participate in shared experiences. These communities may create their codes of conduct, social norms and even economies, leading to a rich tapestry of cultures within the metaverse. Community members may express their social identity in new ways and find a sense of belonging.

In the metaverse, the concept of society may undergo redefinition, where neighbours may be individuals who reside in virtual homes adjacent to yours rather than physically nearby. Relationships with AI agents could become more prevalent and add a layer to our traditional human interactions, creating new paradigms and blurring the lines between what is authentic and what is generated. These potential social transformations require further long-term analysis in terms of impact (Koike and Loughnan 2021; McKenna, Green and Gleason 2002). Younger populations are early adopters of the metaverse, with half of surveyed millennials and Gen Zs in one survey considering online experiences a meaningful replacement for in-person experiences (Deloitte 2023). What is acceptable and meaningful in terms of human interaction, or what constitutes a societal concern, may thus change over time. As society evolves, it is crucial to evaluate which changes are beneficial and desired and which put our societal values, individual rights and freedoms and humanity at risk and therefore need careful management.

Moreover, the metaverse inherits from online social platforms systemic concerns about protecting human rights and freedoms online, which are substantial with the evolution of the technologies (RightsCon 2021) and presents substantial health and social risks, in particular for children and young adults, demanding accountability from platform operators in addressing its unique challenges and potentially intervention from public authorities. The development of appropriate measures might include a legal response, preferably in co-operation with virtual world and immersive experience providers and internet intermediaries, and multidisciplinary teams. Creating guidelines and mechanisms to address harmful, offensive, discriminatory, deceitful or misleading content in virtual spaces, while balancing freedom of expression and preventing harm, is vital for fostering a safe and inclusive metaverse environment. Responsible content creation, user empowerment and dispute resolution mechanisms are needed to keep this in check.

Because of the enormous reach and scale of the metaverse, there is a risk of social exclusion, with the potential that existing issues related to bullying, hate speech and misinformation on social media are exacerbated (Frankel and Browning 2021), considering that nowadays online hate is more prevalent and may be more harmful than hate offline, with perpetrators often acting more spontaneously and anonymously, with a wider reach and a lasting impact on victims (see Council of Europe 2023a). The experience of self-governance in the social media world to combat this has proven to be flawed and has resulted in a number of negative experiences for users. It is thus crucial that the innovation ecosystem and international standard-setting instruments, including those of the Council of Europe, encourage sustainable and responsible business practices that aim to avoid conflicts of interests (for example platforms abusing their control of marketplaces, using dark patterns, that is tricks deceiving or manipulating users into certain choices or profiting from the spread of harmful content) and minimise the risks of immersive technologies creating and exacerbating individual and social harm in the virtual realm.

Health

The European Social Charter recognises health as a fundamental human right and the Court's case law requires states to safeguard people's mental and physical well-being, ensure access to healthcare, have a say in the treatment they receive and provide access to redress in case of medical errors. The metaverse's immersive virtual environment can have a substantial impact on various aspects of health, such as physical and mental well-being, healthcare access and therapeutic uses. These impacts need to be acknowledged in terms of not only the benefits they offer but also the potential risks (see also Evans 2022).

On one hand, the metaverse offers opportunities to promote physical health and well-being by offering engaging workout experiences, physical rehabilitation, assistance in regaining motor skills and facilitated recovery after injuries or surgeries.

However, immersion in 3D environments within the metaverse can have both short-term and long-term negative physical health effects. Headset hardware has latency issues, which can cause nausea or "cybersickness" for some people (Ball 2021), in particular women. The lack of awareness of surroundings during VR experiences can cause injuries (Cucher et al. 2023). Further effects include physical fatigue, eye strain, seizures (Park and Kim 2022) and potential risks from electromagnetic radiation (Connecticut Department of Public Health 2008; European Commission 2007). Excessive screen time in the metaverse not only takes individuals away from face-to-face interactions and time in nature but may also lead to issues like spinal pain and headaches (Joergensen et al. 2021).

The metaverse offers the advantage of overcoming barriers to healthcare access, as telemedicine enables remote consultations and delivery of healthcare services. This has the potential to benefit individuals in underserved areas, provided that the virtual consultations do not become inaccessible because of additional fees. Virtual reality and augmented reality technologies allow healthcare providers to remotely examine patients, provide diagnoses and deliver personalised care – all of which reduces travel burdens for those individuals for whom physical access to healthcare facilities is challenging. This is a great opportunity, considering that according to estimates by the World Health Organization around 50% of the world's population lack access to essential health services (WHO 2017).

The immersive and customisable experiences of the metaverse hold promise for therapeutic applications, such as VR-based exposure therapy for phobias, post-traumatic stress disorder, anxiety disorders and pain management, as well as minimising the risk of sensory overload for persons prone to it, though the same environments can pose such a risk to healthy users (WEF 2023e). These experiences can be designed to take place in controlled virtual environments where individuals are exposed to their fears or triggers in a safe manner. Some therapeutic uses of metaverse technologies can also involve brain stimulation for treating conditions such as depression. Brain stimulation involves directly stimulating the brain using sensors, affecting pulse rates and eye movements. Brain stimulation can also occur in non-therapeutic environments, such as learning and education, with benefits such as faster learning. However, there are also significant concerns about potential long-term effects and the lack of safety requirements in this area of the metaverse, in particular for the developing brains of children. As such, experts recommend prohibition of brain stimulation, unless it is for limited amounts of time and for therapeutic purposes, until extensive studies give a better understanding of the short and long-term effects. While brain stimulation may be beneficial for certain medical treatments, for instance for depression, brain stimulation may not be necessary or appropriate in recreational contexts like gaming. Proper education for medical professionals, legislators, parents and users is crucial in order to address this issue responsibly.

The metaverse offers transformative experiences for healthcare, with XR technologies revolutionising surgical procedures, medical training and patient care. It enables surgical planning, remote assistance and post-operative rehabilitation, benefiting both patients and healthcare professionals. Digital twin technology integrated with XR environments can be used to create accurate 3D models of patient organs, known as digital twins. These virtual representations facilitate various applications, including 3D printing, visualisation, biomedical testing and simulation technology for medical devices. The integration of digital twin technology and XR environments in healthcare offers significant potential for improved diagnostics, treatment planning, surgical outcomes and medical research. However, ensuring privacy, data security, model accuracy and ethical use will be crucial for the successful and responsible implementation of this technology. Regulatory frameworks should be developed to govern its use, leading to personalised, patient-centred care and transformative advances in the healthcare industry.

Some areas of promise include virtual wellness retreats, mindfulness applications and stress reduction spaces that can contribute to improved mental health outcomes, which in turn may positively impact physical health over time (Vaillant 1979; Ohrnberger, Fichera and Sutton 2017). While there are indications about benefits for psychosocial (self-esteem, socialisation), cognitive and social development for children, their prefrontal cortices, which help process the perceived information, are not yet developed, causing difficulty with distinguishing between the virtual and the real worlds, while the personalisation may lead to a fractured view of reality that can be dangerous for their development (UNICEF 2023).

As metaverse technologies advance and virtual experiences become more realistic, the ability to distinguish reality from fiction becomes distorted even for adults, which carries a risk of manipulation with it. Projected negative impacts of metaverse technologies on mental health relate to disassociation (Van Heugten-van der Kloet et al. 2018) and withdrawal from the physical world (depending also on the level of self-presence, social presence and spatial presence – see Stephens 2022), as well as internet addiction and excessive online gaming, which were recognised in 2018 by WHO as psychiatric disorders. Studies have shown that these behaviours often serve as coping strategies (Kardefelt-Winther 2014), and the tailored and immersive experiences of the metaverse can make them addictive, in particular since VR has been shown to also alter the perception of time spent in virtual spaces (Read, Sanchez and De Amicis 2021). Internet addiction includes online gambling, social media (posting, compulsive scrolling, tagging), online shopping and online gaming. The Council of Europe is expected to release a recommendation on online addictions in 2024. The growth of specialised treatment centres for these problems highlights the need for policy interventions as a preventive mechanism. Still, ensuring access to resources and long-term treatment is crucial to address mental health challenges arising from metaverse usage, as untreated severe mental health conditions can lead to significant life impacts and increased risks of injuries and diseases.

Existing studies on the metaverse's impact on mental health are limited and cannot yet provide comprehensive conclusions. Many of these studies, including those on VR, suffer from small and biased sample sets, predominantly representing a specific age range and gender. As a result, there is a need for the funding of more extensive and diverse research to understand the full scope of the metaverse's effects on mental well-being (experience can be drawn from 7010-2020 - IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being setting related metrics IEEE SA 2020) and overall health online and offline, at an individual and collective level, across generations. Health-related data are not just generated in health-related applications but can be potentially generated in every use of immersive technologies: the advanced sensors that are used to allow metaverse functionalities are indicators also of the physical and psychological health of the user, even if not collected or processed for health applications. Governments may need to set up policy tools like RegLabs or regulatory sandboxes to assess the robustness of existing policies. Already data trade deals are happening for health information and there may be a need for global consensus on best practices to ensure that the rights of the individual are safeguarded and not exploited for profit (the Committee of Ministers has provided recommendations on the protection of health-related data – Recommendation CM/Rec(2019)2).

Environment

On 16 and 17 May 2023, the Heads of State and Government of the Council of Europe's 46 member states met at the 4th Summit in Reykjavik to discuss the human rights impacts of current challenges, including the climate crisis and the development of new technologies. The Summit Declaration "United around our values" (Reykjavik Declaration 2023) laid out the Council of Europe's commitment to strengthen the Organisation in the fields of human rights, democracy and the rule of law, and to develop tools to tackle emerging challenges in the areas of technology and the environment. In a dedicated appendix, the declaration elaborates on the interlinks between human rights and the environment and recognises that a "clean, healthy and sustainable environment is integral to the full enjoyment of human rights by present and future generations".

A year earlier, the UN General Assembly recognised in a resolution it adopted that access to a healthy, clean and sustainable planet is a human right and made sustainability a state obligation (OHCHR 2022a). Several UN Sustainable Development Goals (SDGs) are directly linked to this right, including clean water and sanitation (Goal 6), affordable and clean energy (Goal 7), sustainable cities and communities (Goal 11) and responsible consumption and production (Goal 12). A sustainable planet is also a precondition for citizens to enjoy their fundamental freedoms and exercise their rights, in particular for persons in vulnerable situations (OHCHR 2022b). Climate change-related migration, health and labour implications will need to be looked at from a human rights perspective and it will be important to assess the specific implications of the right to a clean and healthy environment on the interpretation of other human rights.

The metaverse has applications that can help address climate change and sustainability: digital twins for example can be used for climate simulations and in design and manufacturing, leading to energy and resource efficiency. It is also expected that virtual consumption (substitution of physical with digital products), work and interactions will reduce mobility-related emissions and use of resources (EY 2022). Still, the metaverse is very energy-intensive with its heavy computing needs, data processing and transfer requirements and related intense use of data centres and blockchain. This raises concerns about the enormous energy consumption and related environmental footprint that would come with potentially exponential growth and adoption of the metaverse.

The environmental impact and energy requirements of the enabling technologies and components of the metaverse require careful oversight. As a response, discussions on green digital transition and sustainable information and communication technology (ICT) practices are starting to take place, with initiatives like the European Green Digital Coalition (EGDC) focused on addressing the environmental impact of digital solutions while there are increased discussions on the role of technical standards and further frameworks which can define a common language, co-ordinate metrics and indicators on how to develop and deploy sustainable technologies and measure their environmental footprint.

Green and sustainable ICT, including the metaverse, is now considered an essential part of the green digital transition. Initially seen as part of corporate social responsibility or responsible innovation, it is now becoming a compliance requirement due to energy crises and sustainability reporting requirements. Energy efficiency is no longer seen as voluntary reporting but a necessary aspect of a responsible industry.

Education

The education sector has embraced the metaverse in classrooms, in particular during the recent Covid-19 pandemic (Pew Research Center 2022), for history teaching (Curry 2007; Frischer 2014; Braithwaite 2018), medical training, research (Mystakidis 2022) and military simulations. Virtual companions are being used to teach children who, unsurprisingly as digital natives engaging with new media and digital technologies in general, are receptive to this format, especially when they are paired with virtual agents that appear to be of a similar age. It is not always clearly specified if and when parental consent is required or obtained for these interactions. Challenges like privacy, age-appropriate design and content, and resource trust, therefore, need to be addressed. Moreover, there is limited research on the long-term impact of virtual education, especially on children's development, and physical, cognitive, emotional and psychological capacities (see also the section on Health). Ideally, metaverse content development for the purposes of education should be done by a multidisciplinary team to ensure that the experience and skills are appropriate and can translate into the real world.

Online gaming platforms with AR and VR elements that are aimed at children have the potential to offer experiential learning. However, children need metacognition to fully benefit from these immersive environments. Traditionally, metacognition has been taught by human instructors, but in online games children lack such guidance. The importance of human teachers for pre-schoolers was highlighted in a campaign run in Singapore, an early promoter of AI and robots (Srivastav 2019). Additionally, studies show that children's brains are not developed enough to perceive all aspects of 3D environments, with unknown effects in the case of long exposure. There is a need for teaching programmes for educators, parents and guardians to embrace new digital literacies and for understanding the required protection for consent, security and privacy. There are currently no teaching programmes for educators to embrace the new types of literacies (Wohlwend 2010) as there is no understanding about the related needs and requirements. In the meantime, more guardrails should be developed to address consent, security and privacy issues related for instance to biometric data (Climent-Perez and Florez-Revuelta 2021): even if as per Convention 108+ parents should be informed about data processing, they are often providing consent without a full awareness of the risks or their rights. Children's data is a special data category of enhanced protection and the Council of Europe has developed guidelines on children's data protection in an education setting (Council of Europe, Children's data 2021).

Metaverse applications in educational environments can offer valuable opportunities for skills practice and training in hazardous situations. They can be especially beneficial for lifelong learning and for individuals displaced by digital technologies, allowing for skilling, reskilling and upskilling. The right to education is recognised by Article 2 of Protocol No. 1 to the Convention. Moreover, the new Council of Europe Education Strategy 2024-2030 ("Learners first") emphasises education through a human rights-based digital transformation. This strategy aims to develop three dimensions in every learner: the "citizen" learner, the "intercultural global" learner and the "digital" learner, that is, someone who competently and positively uses emerging digital technologies while being aware of their impact on human rights, democracy and the rule of law.

Immersive learning offers a unique approach to education. Still, in an exclusively virtual environment ensuring access to education would require providing access to enabling hardware or specific software applications, or else it could result in unintended discrimination that widens an already existing educational divide. That would lead to specific concerns about underprivileged populations or persons with functional limitations who do not possess appropriate assistive technology or accessibility software (Mangina 2021).

Children's rights

As children grow up in an increasingly connected world, virtual worlds and immersive realities are transforming their social interactions and play experiences. In metaverse environments, children can embody avatars, chat, play games and attend events with people from around the world. While VR can offer educational and therapeutic benefits for children, there are also safety concerns that need to be addressed, especially as younger users are attracted to social VR platforms originally designed for adults (Maloney, Freeman and Robb 2021).

Upholding the United Nations Convention on the Rights of the Child, the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention), the Council of Europe Strategy for the Rights of the Child 2022-2027 and Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment is essential to not only safeguard children from potential harm related to what are often known as the "4 Cs" – content, contact, conduct and contract – but to also protect their right to childhood (see also the section on Health). Further Council of Europe instruments examine children's data protection in educational settings and include a handbook for policy makers on the rights of children in the digital environment.

The increasing use of social VR by children and adolescents has raised concerns about their exposure to inappropriate content, harassment, cyberbullying and bullying, the potential risk of interaction with offenders and the limited awareness and understanding among parents regarding these platforms (Maloney, Freeman and Robb 2020 and 2021). The metaverse has the potential to greatly intensify existing online cyberbullying issues for children, create new forms of behavioural cyberbullying (such as avatars throwing virtual objects at other avatars) (UNICEF 2023) and move bullying from offline to online or vice versa. It is challenging to identify online bullying because it can manifest itself differently from offline culture and norms. Cyberbullying or bullying can trigger suicide, which is the fourth leading cause of death (WHO 2023) among 15 to 19 year olds. It also affects girls more than boys and can lead to lowered self-esteem and sleep loss (Global Digital Civility Index 2024). Special attention should be given to children with disabilities in the metaverse who may be exposed to increased risks of bullying, hate speech, discrimination and harassment, among other things (Council of Europe, Two clicks forward, report on children with disabilities in the digital environment 2019). Moreover, as pointed out in the Council of Europe Mapping Study on Cyberviolence, cyberbullying also impacts freedom of expression (Cybercrime Convention Committee 2018).

Grooming and sexual harassment are some of the dangers that children face in virtual environments and that have detrimental effects on their dignity, psychological status and well-being. To address these issues, which often constitute criminal offences (Lanzarote Convention), there is a need for effective safety-enhancement and detection tools, educational programmes to raise awareness among children and their guardians, appropriate reporting mechanisms and open communication with parents and other relevant authorities.

Ongoing research is also exploring the use of automated embodied moderators to safeguard children in social VR platforms. However, when implementing automated tools and detection technologies, trade-offs and careful consideration of user freedom and privacy are necessary to strike the right balance. In this context, the value of a human in the loop is worth exploring. Other potential solutions that prioritise safety, security and privacy for children include building in age-verification processes and safety measures similar to real-world scenarios at the very early design stages, or more systematically and holistically incorporating and using age-appropriate design principles (ICO 2020) and related technical standards like the IEEE 2089-2021 to address age-appropriate design for children's digital services (IEEE SA 2021).

Protecting confidentiality and children's privacy and data, even when intervening to ensure children's safety in online spaces, should be treated as a non-negotiable, considering how vulnerable children are to having their perception of reality and beliefs altered by the (manipulative) capacities of the technology. Due to their natural stages of brain development, children find it more challenging to distinguish the virtual from the real world. They also have a lowered sense of time spent in immersive environments, which can prove dangerous because prolonged exposure to virtual environments can increase the risk of negative psychological outcomes such as depression, anxiety and addiction. Consequently, safeguarding children's mental well-being within the metaverse becomes imperative. Age-verification methods, such as facial recognition, may be intrusive and raise privacy concerns. Practical considerations and careful examination of tensions are needed to develop effective regulatory measures that safeguard children while respecting privacy and confidentiality. Finding the right recommendations in this space requires a thorough understanding of the complexities involved. The Council of Europe has called for a stepping up of the protection of children's privacy in the digital environment.

The metaverse's growing prevalence raises concerns about its impact on children's physical health as well. Excessive engagement with virtual environments, like the metaverse, can negatively affect children's physical development, leading to visual damage, insomnia, motion sickness and sedentary behaviour-related health issues. Balancing virtual experiences with physical activity is essential for promoting regular exercise and a healthy lifestyle in children.

The metaverse's influence on children's psychological development requires thoughtful examination too, as immersive virtual experiences may impact identity and social interactions. Over-reliance on the metaverse for social connections may lead to isolation, limited face-to-face interactions and difficulties in developing interpersonal skills, which may linger well into adulthood, emphasising the need for appropriate safety measures and parental controls to manage VR usage effectively (McMichael et al. 2020; Fiani et al. 2023).

Children's privacy and data protection are discussed in the respective section of the report.

Chapter 3

The metaverse, the rule of law and democracy

The question of whether traditional democracy will shift into virtual reality and how it will be impacted by the metaverse is significant, as immersive technologies offer opportunities for public authorities to engage citizens through e-governance, e-participation, e-voting and other virtual democratic mechanisms that can facilitate civic engagement in the virtual world. The same technologies, though, also come with risks for democratic foundations and principles, as identified in previous sections.

Member states have the obligation to refrain from violating human rights in the digital environment and the positive obligation to protect universal and interdependent human rights through democratic frameworks. Member states are tasked with enforcing human rights with laws and policies at various levels, including the Convention and the case law of the Court, and ensuring compliance of private parties with relevant legislative and regulatory frameworks. The rule of law is a prerequisite for the protection and promotion of human rights and for pluralistic and participatory democracy. Moreover, it is indispensable for providing due process guarantees and facilitating access to justice and effective remedies vis-à-vis both states and intermediaries for the services in question, considering the possible barriers preventing some individuals from seeking redress because of their personal characteristics or status.

Public authorities are expected to face significant challenges in transitioning and adapting to metaverse technologies yet need to continue upholding existing human rights protections or implementing new ones to safeguard democratic principles in virtual environments, while understanding the dynamics of the metaverse and the roles and responsibilities of all stakeholders of the ecosystem, which may vary compared to existing frameworks. Specific challenges relate to digital territoriality, metaverse-related crime (also referred to as metacrime, INTERPOL 2024), personhood, protecting vulnerable populations, addressing policing concerns and managing competition, intellectual property and ownership in the metaverse. Further issues include supervision, verifiability of the information related to a violation, attribution of responsibility, liability and accountability, access to information and enforceability while still safeguarding equality and non-discrimination.

Digital territoriality and jurisdiction: virtual worlds as crime sites

The emergence of the internet in the 1990s led to the development of digital law, which addresses legal questions related to the violation of various fields of law through various actions and behaviors in the digital realm. Similar discussions are now occurring concerning the metaverse, particularly regarding jurisdiction, which involves considering different types of relationships, including those between platform providers and users, supply chain providers/intermediaries and users, government and other authorities, platform/technology developers and providers, states and other authorities and users, and among users themselves, while the involvement of avatars complicates the landscape. While some relationships may be governed by contractual frameworks and existing regulations, there are ongoing discussions about whether territorial jurisdiction in the metaverse should be based on the physical location of users, similar to how it applies to online disputes and whether traditional territoriality principles on jurisdiction or other established criteria are adequate to be used in the decentralised metaverse context (European Parliament 2023).

One of the primary challenges in dealing with crime within the metaverse is determining which legal frameworks apply. Virtual worlds often span multiple jurisdictions, perpetrators and victims may reside in different countries with their own laws and regulations, leading to complexities when establishing which jurisdiction has authority and the applicable laws to govern the case. Legal frameworks and international co-operation between countries, intergovernmental organisations and platform providers are crucial to address the challenges of digital territoriality and establish protocols for investigating and prosecuting crimes committed within the metaverse. In that respect it is worth noting the Council of Europe–EU guidelines for co-operation between law-enforcement agencies and internet service providers against cybercrime (2008), which provides some guidance, as well as the Second Additional Protocol to the Budapest Convention, which provides means for direct co-operation with service providers in other parties, thus allowing cross-border co-operation with service providers. A continued dialogue is important to foster public–private co-operation, considering the specificities of the metaverse.

Mutual legal assistance treaties and international law-enforcement agencies can play a significant role in facilitating cross-border investigations and extradition. Technological advancements can also contribute to mitigating digital territoriality challenges. Blockchain technology, for example, can provide transparent records of transactions and ownership within virtual worlds, assisting with investigations and establishing evidence. Similarly, digital forensics tools and techniques can aid in collecting and analysing digital evidence related to virtual crimes (see also below under "Policing, law enforcement and justice in the metaverse era"). As digital territoriality evolves, it is essential to consider ethical implications. Balancing the need for law enforcement with individual privacy rights and freedom of expression is crucial. Discussions around data protection, consent and the potential for abuse of power within the metaverse must be carefully considered to prevent the misuse of jurisdictional authority and cases of forum shopping or a race-to-the-bottom effect. Developing effective strategies for security and justice in the metaverse will be essential as it becomes more integrated into our lives.

Cybercrime and virtual crime

The metaverse and virtual worlds host a wide range of activities, from socialising and gaming to virtual commerce. In the same environments illegal and harmful behaviours in general can take place, like cyber-facilitated or cyber-enabled crimes, liable under criminal law, including hacking, virtual asset laundering and fraud, stalking and surveillance. Virtual misconduct in the metaverse encompasses actions that breach norms, ethical standards or legal frameworks, varying from minor violations of rules and terms of service to severe offences. The often anonymous nature of online interactions can lead to offensive behaviour, cyberbullying and psychological distress, compromising the safety and inclusivity of the virtual space. Virtual theft, fraud and hacking are prevalent in virtual economies, leading to financial losses and undermining trust. Virtual violence, including "briefing" (virtual game players intentionally irritating and harassing others) and virtual attacks, can harm individuals and community well-being. This next iteration of crimes in a digital environment includes known behaviours and the ways in which misconduct and crime take place (cyber-facilitated crimes), with possible impacts in and from the offline world, while some new types or variations of crime may emerge in immersive environments (cyber-enabled crimes). Such behaviours can blur the lines between the physical and digital worlds, making it challenging to establish jurisdiction and hold perpetrators accountable for crimes committed in these virtual environments. In the metaverse, behaviour and conduct are expected to add a layer to existing cyber and virtual crimes (INTERPOL 2024), such as behavioural cyberbullying, while new spaces such as a "darkverse" may arise (INTERPOL 2022).

Policing, law enforcement and justice in the metaverse era

Combating virtual crime in the metaverse involves technology, community efforts and legal measures. Reporting systems, user guidelines and co-ordination with law enforcement can help create a safer environment, with the promotion of responsible behaviour, implementation of effective mitigation strategies and the fostering of collaboration among stakeholders for a positive virtual environment. Law-enforcement agencies face the challenge of adapting their strategies to effectively uphold justice in the virtual realms.

There are a number of evolving techniques and innovative approaches that law enforcement can employ in the metaverse era to address virtual crimes, protect users and ensure an accountable digital environment partially using the same metaverse-enabling technologies, while in some other cases the nature of these technologies may create hurdles in law enforcement (INTERPOL 2024). Virtual policing units with officers trained in digital investigations, cybersecurity and virtual world dynamics can focus on monitoring, investigating and preventing virtual crimes within the metaverse, proactively identifying emerging threats and responding swiftly to incidents. Still, the technical understanding of stakeholders involved about the nature and variations of misconduct and crime in the virtual realm are important for an effective rule of law and the protection of human rights. The integration of artificial intelligence, blockchain technology, cryptocurrency analysis and predictive analytics can help identify patterns of suspicious behaviour, trace transactions and money laundering and assist in proactive monitoring, early intervention and predictive policing in the metaverse. Virtual forensics, involving the collection, preservation and analysis of digital evidence, must evolve to handle virtual crimes, using advanced tools and methodologies to extract and analyse data from virtual environments, including virtual transactions, chat logs and virtual assets ownership records. These techniques help build solid cases against virtual offenders and ensure justice is served. Collaborations where law-enforcement agencies work with virtual platform operators and technology companies in consultation with victims can help investigate virtual crimes effectively and combat virtual offences collectively. Collaboration in cross-border investigations or cross-border extradition can be backed by mutual legal assistance treaties and international law-enforcement agencies. Going beyond the market focus of many metaverse use cases and specifications, task forces could explore ways in which existing human rights and regulations can be applied and ways to prevent crimes in metaverse environments, as well as understand or create avenues and means for redress so that crimes do not go unregulated or unpunished. The metaverse has been tested in some jurisdictions as a virtual space for legal hearings (Reuters 2023) and it remains to be seen whether this would fulfil the requirements to be considered an effective remedy and way to access justice or whether biases or other factors should be considered.

The role and contributions of service providers (internet/platform providers) is very important: they are typically in possession and control of electronic evidence and are best informed about the technology in place, the options and limitations; they manage proprietary spaces, have access to data and are thus considered often as "gatekeepers" with increased responsibility and obligations (European Commission, n.d.). Here, it is worth mentioning the Council of Europe Convention on Cybercrime and its two additional protocols, an example of how the Organisation has been timely responding to the evolution of cybercrime, taking into consideration the growing importance of digital evidence in traditional crime. Law enforcement can also use procedural powers available in the Budapest Convention, which adapts traditional procedural measures to the new technological environment and creates new measures, such as the expedited preservation of data, while criminal justice authorities and law-enforcement agencies may use also powers under the Second Additional Protocol. Further relevant frameworks and tools developed by the Council of Europe include an electronic evidence guide (2022), providing guidance to criminal justice professionals on how to identify and handle electronic evidence to ensure authenticity for admissibility in court; a guide for criminal investigations into ransomware attacks; and a guide on seizing cryptocurrencies.

When considering how to treat cybercrime and virtual crime in the metaverse context, it is worth noting that case law from a decade ago has demonstrated that criminal activities in online and virtual environments do have an impact in the physical world and confirms that these cases are not a potential future threat or new to the judicial system. Accordingly, online violations must not be normalised or tolerated and there is a much closer and thinner line than previously anticipated between the online and offline relationship and its effects on law (Lodder 2013). Do existing protections for human rights go far enough to protect human interactions in virtual environments? Some answers have been provided by the case law of the Court (*K.U. v Finland*, *Beizaras and Levickas v. Lithuania*, *Buturuga v. Romania*); still, existing legal frameworks often do not suffice for effective prosecution of all types of cybercrime. Virtual worlds create complex dynamics where it is not clear where one's individual rights start and end, and an in-depth assessment would be needed to answer that question.

Personhood and ownership in the metaverse

In the metaverse, the concept of personhood and individual rights becomes complex, especially with the convergence of virtual and physical worlds (INTA 2023), including the presence of virtual clones and digital humans, which raises questions about the evolution from simple "digital identities" to more complex human digital "packages". Similar questions have also been explored in the field of AI for several years now (IEEE SA 2016).

In the metaverse context, personhood entails rights, such as property and ownership of digital assets like NFTs and avatars. Issues that arise concern their portability and safety in transactions, the protection of creations in the metaverse by intellectual property rights and accountability for the actions and behaviour of avatars/digital humans, in particular when AI agents are involved. The enforcement of these rights becomes complicated as the assignment of rights and control of identity partially lies within the platforms used. Users may assign their own identities, but platform companies may hold control over them, leading to compatibility issues across different platforms and accountability to multiple entities and possibly multiple jurisdictions.

Rule of law and democracy in proprietary virtual spaces

Both the metaverse and its enabler, Web3, are decentralised by design. Metaverse is not owned by a central entity or gatekeeper, but by its developers and users, thanks to its underlying blockchain infrastructure and decentralised and distributed data storage. As such, the metaverse comes with the promise of being more democratic, with distributed ownership, offering a space for disintermediated communication, where individuals can directly interact with each other without relying on centralised platforms or intermediaries. Metaverse enthusiasts expect that such an open, decentralised metaverse will be self-regulated through decentralised autonomous organisations (DAOs), that is, virtual blockchain-based entities without supervision from regulatory authorities or governing bodies that enable transactions through smart contracts and bottom-up decision making by their token holders. While this form of decentralised governance is meant to remove intermediaries in the governance of the metaverse, bring transparency and reduce risks like fraud, and despite the open, community-driven and streamline rationale of DAOs, yet legal and governance challenges (WEF 2023c) remain, such as power concentration by wealthy DAO members and token holders (Council of Europe 2023b).

Moreover, the promise described above may not materialise because of economic reasons or compliance challenges, which may make it prohibitive for smaller companies to navigate, leading to a concentration in the hands of a few and *de facto* oligopolies. These few players would have privileged knowledge of the actual state of the art, access to and control of the proprietary space and data linked to our future work, social interactions, education, political participation and exercise of basic human rights and freedoms. Visibility, transparency, verifiability and enforcement will be difficult for public authorities and it remains to be defined what roles private industry, independent authorities, government, enforcement and judicial authorities can play and in what way enforcement entities or third parties can obtain access for virtual forensics and effective functioning of the rule of law.

Trade, property, intellectual property (IP) and competition in the metaverse

The metaverse presents diverse economic opportunities, including the sale of collected and generated user data, real estate and services, as well as transactions involving non-fungible tokens (NFTs), which pose questions related to the right to property (Article 1 of Protocol No. 1 to the European Convention on Human Rights), among other things. To ensure fair competition, competition authorities will play a crucial role in regulating the metaverse ecosystem. Moreover, different levels of AI-generated or AI-enabled creations pose the question of attribution and eligibility for intellectual property (IP) protection, including patent and copyright law.

Advances in virtual worlds enable the conversion of real-world assets into digital tokens for trade within the metaverse. However, this gives rise to concerns about unauthorised use and potential brand dilution of third-party trademarks within virtual environments.

Trademark infringement in the metaverse raises questions about potential confusion between trademarks for physical and virtual goods. The term "virtual goods", terminology used in related European Union IP Office guidelines (EUIPO 2023), needs further specification in trademark applications to describe the type of protected virtual goods, such as downloadable virtual goods like virtual clothing (EUIPO 2022). Brand protection serves the protection of the uniqueness, reputation and goodwill of a brand from its infringement, dilution or abuse, and its importance is even higher in the metaverse than in the physical world, as brands face more risks like malicious registration, counterfeiting, embezzlement and defamation.

In the virtual context, copyright protection applies to works created both outside and within the metaverse. Users may create work such as music or images, typically stored on NFTs, which can be used as title of ownership and certificate of authenticity. All users are relevant from an IP rights perspective, considering that their use of the metaverse creates data stored in databases run by content creators, such as platform operators. In a sense, users of the metaverse become assets themselves through their data. Copyright infringement occurs when copyrighted works are reproduced or made available to the public without the owner's permission. Related assessment depends on the technology used for reproduction and the duration of storage (such as transient storage in the metaverse) (Loewenheim 2020). A further question is whether tokenised physical works infringe third-party copyright, with some authors considering there is a need for a licence agreement to use the copyright to the tokenised works. The anonymity of the metaverse poses challenges in identifying the author and owner of copyrighted digital works, as well as the infringer of the assigned copyright. Avatars and AI cannot be work authors under EU copyright laws, making the person behind the avatar the copyright owner. Significant human input is required for copyright protection, and AI used as a mere tool may not be eligible for copyright infringement. However, protection applies if the AI is used to create a personal intellectual creation. The enforcement of intellectual property rights in the metaverse faces challenges due to the territoriality of IP rights and difficulties in identifying infringers, especially in decentralised collaborative processes or when users are anonymous behind avatars. Governments and companies will find it expensive and challenging to monitor and promptly detect infringements in the vast expanse of the metaverse (which can be limitless, depending on compute power and storage capacity). Trademarks are enforceable only in the jurisdictions where they are registered and thus protected. While the metaverse is not tied to any specific territory or country and this may create ambiguity (Nordemann-Schiffel 2023), it is accepted that an infringement only occurs in a country where the infringement has a commercial impact (ECJ 2011). Owners must adapt to virtual environments, meet additional requirements, and implement effective monitoring measures for successful protection and enforcement in the metaverse.

Where patent protection is concerned, the European Commission has reported an increase in patent applications related to virtual reality (IPR Helpdesk 2022), reflecting the innovation and patent protection sought for hardware or software that enables virtual experiences. Unlike copyright and trademarks, patents pose less of a legal challenge and related discussions are linked to more traditional questions about patents and AI, as well as patentable subject matter.

The metaverse's dynamic markets present challenges in terms of defining markets, assessing dominance and ensuring fair competition and inclusivity. Various stakeholders, including competitors, end users and suppliers, add complexity to monetising metaverse services, especially when intermediaries are involved. Competition authorities are closely monitoring access and ecosystem closeness issues within the metaverse. While a dedicated Metaverse Competition Authority (Petit et al. 2022) is a theoretical concept, real-world competition authorities will investigate potential antitrust infringements. They may apply existing instruments, like abuse of dominance rules and gatekeeper regulations, to scrutinise dominant metaverse service providers for abusive conduct and to combat anti-competitive agreements. Authorities should also watch for competition law concerns in horizontal co-operations and standard-setting activities, ensuring that interoperability standards adhere to competition law boundaries. Additionally, early intervention through merger control is essential to prevent market concentration and support start-up growth. Mergers and acquisitions happen in this space for the acquisition of technologies, data and users.

Chapter 4

Governance

Governance of new technologies, their uses and impact can take place at a global, international, regional or national level. It can be accomplished by hard law – regulation and legislation, including international treaties and conventions – and soft law, such as guidelines or technical and other standards, as outlined in the recently adopted Recommendation CM/Rec(2023)5 of the Committee of Ministers to member States on the principles of good democratic governance, which establishes the first international legal instrument in this field. The governance of the metaverse requires ongoing research on impact, careful consideration, transparency and proactive measures, which may include new international standards or new digital rights. Since the metaverse functionalities are based on data generation, processing and analysis, including personal, mostly proprietary and often sensitive data, data governance and issues of access, ownership, cybersecurity, privacy and data protection will be important to address. Legal interoperability (WEF 2023f) will also be important considering the cross-border data flows and implications. By collaborating, adhering to law and standards and continuously reassessing and evaluating, we can create a fair and inclusive metaverse that addresses its unique challenges and respects and upholds human rights and the principles of democracy and the rule of law.

Regulation

Global discussions in the field of AI also raise for the metaverse the issue of whether we should be moving towards international regulation (as per the Council of Europe's draft framework convention on AI) or international/global governance frameworks (similar to the proposed creation of a Global AI Observatory (Carnegie Council 2023)). Independent from its specific implementation, a harmonised approach can help avoid the challenges related to fragmented regulation (including the risk of forum shopping and a race to the bottom) or cross-border value chains and address the limitations of stand-alone private-sector self-governance, as were witnessed recently in the case of generative AI. A further consideration is whether we should be moving towards technology-specific, or impact, outcome or principles-based, regulation. The answer may be a combination of both, depending on the issue in question and the appropriateness of each mechanism. Regulations will be developed depending on the perceptions we have of the technologies involved (for example, the proposed EU AI Act or the EU's "Thrive in the Metaverse" initiative) or how an industry is defined (for example the UK seems to focus on digital twins). Both approaches may not be enough, because enabling technologies may be left out and the technical implementation of the metaverse may look different in the future. Until a regulatory approach is chosen, self-regulation and self-governance will probably be needed, with principles that serve a human-centric, fair, responsible and inclusive metaverse.

Due consideration is also needed to strike a balance between over- and under-regulation, leaving at the same time space for innovation. Trade-offs, balancing and prioritisation across interests and human rights need to be thought through carefully, to offer guidance and ensure the rule of law.

Disruptive and emerging technologies bring different levels of uncertainty and threats to human rights, the rule of law and democracy – and typically at a time when policy making and regulation are not able to react and respond fast enough. However, if policy is built to address fundamental issues, then there is sufficient flexibility to absorb changes over time in the technology. It is important to consciously avoid technology lock-ins (defining a metaverse technology based on specific technical implementation, opening the door to circumventions, allowing for technology monopolies and dependencies). Anticipatory regulation is also an area to be considered closely; this refers to a more proactive approach to regulatory governance, aiming to address impacts and challenges of emerging technology before full maturity or widespread adoption, aligning them with societal values, ethical considerations and legal frameworks, as opposed to the traditional reactive approach of regulation, which is developed once societal impacts are already taking place. Agile regulations allow a more holistic integrated framework from design of policies to their implementation and impact, while foresight exercises can help in the design of policy and regulation in times of uncertainty.

Self-regulation/self-governance

Further governance approaches involve self-governance/self-regulation of technology providers, governments, users and individuals, including adhering to ethical frameworks and platforms and other principles in the form of internal governance and policy documents, adherence to charters or other principle frameworks, voluntary adoption of and compliance with technical standards, certifications and co-regulation. Co-regulation involves co-operation between the public and private sectors, with the industry developing and adhering to its own principles and rules and governments providing the required legislative backing for enforcement (OECD 2009). More discussions are needed on global citizenship behaviours in an environment like the metaverse. Due consideration is also needed for different values and societal concerns at national and regional levels. Harmonisation is crucial to address the unique challenges of the metaverse while safeguarding human rights and promoting user- and human-centricity. Through ongoing evaluation and adherence to standards, effective governance frameworks for the metaverse may be developed.

Self-governance extends beyond standards, through the adoption of charters, treaties, ethical frameworks, industry or research alliances/partnerships with ethical and/or responsible innovation principles or codes of conduct, and it can extend to self-moderation, self-policing, even self-enforcement (Di Porto, Foà and Ennis 2024). Another key issue about governance in the metaverse lies within its own regulations and related sanctions, their conformity with relevant national and international law, the necessary transparency around the system in place and the availability of appeal mechanisms. Currently the moderation of content in such worlds is made by the companies themselves, sanctioning non-compliance with temporary or permanent bans on accessing the metaverse, while content is typically assessed in relation to the terms of use of the companies. It is difficult to assign accountability when the issue that needs governance spills across worlds (physical to virtual and virtual to physical).

The self-governance of technology companies with codes of conduct, adhering to their internal principles and values, nevertheless clashes sometimes with users' values and behaviours and public regulation across jurisdictions. This can be problematic in a universal/global metaverse environment. The right combination of hard and soft law or co-regulation may be a good approach to governance of the metaverse to balance the need for conformity, enforceability, flexibility and room for innovation and self-regulation, always in conformity with relevant domestic and international law. The approach and principles of governance in the metaverse have a significant impact on human rights and democratic principles. Good governance, characterised by transparency, responsibility, accountability, participation and responsiveness to individuals' needs, fosters inclusivity, equity and freedom of expression. Conversely, poor governance can lead to issues like censorship, exploitation, harassment, violence and an unequal distribution of power and resources, emphasising the importance of responsible governance for legal certainty and technology adoption in the metaverse.

Technical standards

Technical standards are a means of self-regulation (soft law), and their voluntary adoption an indicator of uptake of agreed-upon principles. Technical standards serve as the bridge between policies, principles and practice. They set technical ground rules and best practices for developer interactions. Some existing technical standards already provide essential guidance for the metaverse; several of the issues addressed in this report are already under discussion in standards development (for example IEEE SA 2022b). Technical standards follow defined processes and are consensus-based and voluntary, although their adoption may be a requirement for public procurement or other purposes set out by public authorities or other entities ("technical regulations"). These characteristics make standards generally more flexible and adaptable than policy or regulatory instruments.

Standards, including socio-technical standards, can play an important role in the implementation of regulation and legislation and can assist in verifying the technical specifications for governance principles through a series of specific criteria. The importance of standards has been recognised in the field of AI ethics and the AI Act in particular. Standards can create a common language, establish a baseline understanding of the terminology and the technology and set verifiable criteria for compliance. Similar to anticipatory regulation, standards development frameworks need to involve ways for a quick response to societal and regulatory requirements, and for support of the development and enforcement of legal frameworks. Conformity assessments and certifications can also assist in increasing public trust and transparency as the industry-accepted method of demonstrating a product adheres and conforms to a standard.

There are fundamental core technology-focused standards that are required for metaverse implementation and interoperability in the metaverse (WEF 2023f). Immersive environments use very rich digital audio-video content and require a set of coding tools that enable compression and decompression of immersive visual content data. As the number of AR-focused applications increases (mobility, drones, healthcare, training, industrial automation), the need for audio-video standards becomes critical. Another key fundamental aspect is the evolution from a 2D to a spatial web, which requires a new spatial web protocol for interaction in this new virtual realm. These, along with Web3 on a decentralised internet, will provide the environment for and enable the implementation of metaverse applications and provide the right user experience.

Effective governance of the metaverse is essential to protect user rights and privacy and promote inclusion, but the decentralised development by different companies and platforms with proprietary technologies and data creates challenges like data access restrictions and interoperability issues that require collaborative efforts to address. Access control, data portability and interoperability are also critical areas and can be supported by standards while systems thinking can also be beneficial in governing the metaverse (Stephens 2022). As such, standards ensure that individuals are able to operate in a safe environment and have an immersive and seamless experience. Standards can define acceptable data collection and usage practices that include restrictions on gathering sensitive information from children. These standards can help mitigate potential privacy risks and ensure that data are used responsibly. Data compatibility, portability of identity and data, and interoperability involve the flow of data and identities (such as avatar profiles) across different environments and platforms ("cross-verse"). The Decentralised Identifier (DID) standard is an example of a technical specification that can enable metaverse identities to be seamlessly transferred and recognised across different platforms and applications. This promotes a more cohesive and inclusive metaverse ecosystem, allowing users to easily access different environments and services without losing their digital history or reputation.

Within metaverse environments, access control is vital for securing and managing data flows. Access control can be based on roles, attributes or decentralised access control. Identity and age verification are some of the related issues that require technical requirements and specifications, to create higher levels of trust.

The metaverse ecosystem continues to evolve. Technologies associated with it today may not be relevant tomorrow. Hence, ongoing discussions need to factor in anticipatory and agile regulations for user rights – balancing both hard and soft regulation. The complexities of the metaverse supply chain also need to be addressed to include responsibility and governance.

Chapter 5

Concluding observations and considerations

There is a lack of certainty about the way the metaverse will develop over time. The initial assessment about its impact is based upon a combination of existing and unknown issues in the current expressions of the metaverse in virtual worlds, social networks and gaming platforms, like the further development of generative AI, and includes lessons learned and issues from other areas that are expected to be exacerbated and have new scope and dimensions in the metaverse as a result of its pervasive nature and impact on the perception and experience of reality. To further safeguard human rights, the rule of law and democracy, the following points are shared for consideration and possible action.

” There is no common understanding about the metaverse, its complexity and impact

A first step to facilitate discussions about the metaverse is establishing a common, harmonised language and understanding. Technical standards can help towards creating a standardised language and provide related definitions and terminology.

A better understanding of the nature and specificities of the metaverse can take place through a first mapping of the metaverse ecosystem, stakeholders and power dynamics, the technologies involved and possible adjacent innovations, interdependencies and gaps, with attribution of roles, responsibility and accountability across the different ecosystem participants, including internet intermediaries and platform providers to create a transparent and clear framework. A further step could be short, medium and long-term assessments of the impact of the metaverse. In view of the transversal nature of the metaverse, it would make sense for such assessments to be holistic and include different aspects, including human rights impact assessments such as HUDERIA (Council of Europe 2022) and technology risk and environmental impact assessments, which are increasingly becoming part of technology governance frameworks and considerations and should be evaluated, adapted and repeated on a regular basis. Furthermore, awareness raising, training and dialogue between policy makers and industry and academia can facilitate a better understanding of the real dimensions of different points, the technical feasibility and verifiability of requirements that regulators may pose and the identification of gaps that could be addressed through the development of related technology and standards. As there are often requests to create regulation while a technology is still under development, it is important to assess how to create flexible frameworks allowing for adaptations, while the use of strategic foresight tools, such as the building of future scenarios in related workshops with technologists, futurists, lawyers and policy makers, could help in the process of thinking about and deciding upon the most appropriate approach.

❞ The metaverse is transversal in its nature and can change the very fabric of society

The metaverse is expected to alter the way physical and online/virtual environments connect, interact and impact each other, as well as our perception of reality – the view of ourselves, others and the world. This will not only bring changes in the way we live, learn, work, interact and participate in all aspects of life in general, it will lead us to question what is acceptable as behaviour and examine how we interpret concepts such as privacy, identity, freedom of expression and thought, or social interaction and addiction. Societal acceptance and concerns are closely linked to values that are evolving over time, also influencing human rights. The responsibility and decisions around the values we want for our future society should involve everyone. A participatory dialogue and consultation with different stakeholders could be beneficial to assess societal acceptance and concerns, involving them in the design, deployment, oversight and governance process.

❞ Leaving no one behind – towards an inclusive and responsible metaverse

As the metaverse becomes more prominent, special attention must be given to the experiences and challenges of vulnerable populations, including persons with disabilities, children, the elderly and all other groups at risk of discrimination or of being targets of hate, based on their personal characteristics and status, including women and minority groups. These groups face unique opportunities and risks in the virtual realm, requiring strategies to ensure inclusivity and safety for them within the metaverse, starting from the design of wearables that considers different user profiles, for instance in order to avoid increased cybersickness and thus exclusion from the onset. To promote the participation of persons with disabilities in the metaverse, it is essential to incorporate universal accessibility features and inclusive design principles, as appropriate, while collaborating with representative organisations of persons with disabilities can be vital (EDF 2018).

As the metaverse evolves, prioritising the needs of vulnerable populations through inclusive, participatory and responsible design, safety measures and educational programmes can create an enriching and empowering virtual realm. The ageing population, people with functional or other limitations, children and young people, and marginalised or underserved groups should be given the opportunity to enjoy the benefits that the metaverse can bring. This can be achieved by ensuring access to wearables and training, and by developing adapted awareness programmes on the risks of the metaverse. Implementing assistive technology or accessibility features contributes to the safe participation of everyone in the metaverse, regardless of functional limitations, while age-appropriate design principles can be beneficial both for design for and use by children and an elderly population. Striving for inclusion benefits society and promotes diversity, equality and digital citizenship, while preserving individuals' rights to opt out and ensuring alternatives in the physical world. Creating guidelines and mechanisms to address harmful, offensive or discriminatory content in virtual spaces, while balancing freedom of expression and preventing harm, hate speech and misinformation, is vital for fostering a safe and inclusive metaverse environment through responsible content creation, user empowerment, content and behaviour moderation, and dispute resolution mechanisms.

Building the right skills for the metaverse era will also ensure that states, companies and individuals are future ready. This could involve creating a series of new roles and study curriculums: metaverse ecosystem architects, with specialist knowledge of underlying technologies such as blockchain, artificial intelligence, computer vision, data analytics, quantum computing and high-speed networks, and others with relevant skills will be needed to lead the virtual transformation programmes.

” Even more attention should be given to the protection of children and young people in the metaverse

The impact of the evolving metaverse on children's physical and psychological development calls for a balance between virtual experiences and offline interactions for healthy physical and mental development and a greater appreciation of communities and the natural world. To uphold children's rights to a healthy childhood, platform operators, parents, educators and policy makers must collaborate to create a safe and rights-enhancing metaverse environment and develop regulations and other forms of governance in accordance with legal frameworks and due regard for the children's best interests.

Educating children about online safety, digital literacy and responsible digital citizenship is essential and collaboration between schools, educators and parents is necessary to provide comprehensive education on metaverse usage and privacy protection. To ensure a positive and inclusive online environment, there is a need for more than just digital hygiene factors like safety and privacy, as highlighted in the work of the 5Rights Foundation and the Digital Futures Commission, for example. As the metaverse develops, prioritising children's interests and rights in an age-appropriate design and children-centred approach, with appropriate age verification and related measures, could contribute to a safer and more responsible online experience for children and adults alike. Legislative, regulatory and standardisation efforts are being made globally to address these considerations in the metaverse's development.

” Law-enforcement authorities could be hindered by proprietary content or access to virtual spaces

Access to effective protection, supervision and enforcement of human rights is more challenging in a virtual space environment, which tends to be proprietary, along with the collected and processed data. This can be a challenge for law-enforcement authorities. Access and verifiability requirements should be the subject of discussion among concerned stakeholders who should also assess their roles and responsibilities. In the supervision or oversight context, inspiration may perhaps be drawn from the EU framework and the Digital Services Act (DSA), which looks into the service providers' related obligations. Moreover, these environments create additional complexities for digital forensics – training and the provision of appropriate tools would be necessary to ensure a fit-for-purpose judicial and enforcement system.

Lessons learned from other technology advances and differences in the metaverse: same issues, exacerbated scope and impact

Concerns about the legal implications and ethical considerations of the metaverse echo discussions held at the advent of the internet in the late 1990s, the disruption deep learning brought to AI applications and the rise of social platforms, gaming worlds and virtual worlds. Known concepts and issues are exacerbated or take on a new meaning in the metaverse context, while some new concepts arise. There is a risk of underestimating the different breadth and meaning of these same concepts and issues in the metaverse, and a need for a better understanding of the known and potential implications of the metaverse on human rights, the rule of law and democracy, which should be explored separately and in depth, along with assessing how fit for purpose existing legal frameworks are. Assessments should be made through in-depth studies into whether current legal frameworks and Council of Europe standards, applicable to the offline and online reality already, remain appropriate and sufficient and whether they can address the extent of potential human rights violations that may emerge with the metaverse. The experts consulted in the analysis were split on the need for ensuring application and enforcement of existing frameworks, which they consider sufficient, and deeming new regulations appropriate considering the higher risks, level of uncertainty in the technology's development and adoption, and the expected societal impact associated with the metaverse. These diverging opinions show the complexity of the issue and the fact there are no obvious answers. Given the plethora of issues in question, there may be different answers for each of the specific issues identified. The nature of the metaverse, with its immersiveness, invasiveness, real-time interaction, among others, exacerbates known issues from digital environments, while it also creates new layers and risks which need to be clearly identified, classified and addressed properly.

Moreover, it is crucial to assess the technical feasibility of mitigating the risks, identifying violations and harm and attributing behaviours to specific users or stakeholders and to assess whether provisions are in place or are still needed for digital/virtual jurisdiction, redress, supervision authorities and enforcement mechanisms, along with the options for being granted access to required information.

For example, we are dealing with the uncharted territory of brain stimulation and its short and long-term impact on human bodies and brains, in particular in developing children's brains. Indications from existing research are worrying, given the ways it can change the perception of reality. While related concerns are already expressed and further research and experience is probably necessary for definite conclusions, as metaverse-related hardware typically qualifies as consumer goods and not as medical devices, safety and health protection requirements are less strict and are most probably not looking into some aspects, considering that the intended use and nature of traditional consumer goods do not typically require validation of health-related considerations compared to medical devices. It may still be worth exploring health and safety-related risk and reconsider whether the current requirements to allow a product to enter into the market are sufficient to safeguard the users' health. Until the effects of the use of the metaverse are better understood, a more restrictive use of brain stimulation for specific applications and for shorter durations – for concrete medical and short-term educational purposes – may be prudent, while observing the effect of its use.

Besides the online platforms content management, in the metaverse we need to also consider means for behaviour and conduct control, as well as a combination of agent behaviour with space management, which bring up several governance discussion points.

Re-interpretation and effective enforcement of existing legal frameworks or towards the creation of new ones?

There is a challenge associated with keeping pace and catching up that emerging technologies pose to regulation and standardisation. Disruptive technologies and accelerations in technology open the way for discussions about anticipatory or adaptive regulation and policy making, as well as timely, if not agile, standardisation processes.

While the assessment of whether existing frameworks are sufficient or new ones are needed will require in-depth impact assessments, some new questions and rights may arise, either due to the highly transformative potential of the metaverse or the new challenges posed. The evolutionary nature of human rights can mean that certain provisions should be interpreted in case law or through legally non-binding standards and other tools.

Some considerations for new rights and regulation are linked to use cases with increased risks and potential impact on human rights, the rule of law and democracy, such as the invasive potential of brain–computer/human–machine interface (BCI/HMI), and the uncharted long-term impact of activities such as brain stimulation, in particular for developing children's brains. Discussions about the personhood of AI agents in the metaverse which are not controlled by humans can lead to dangerous conclusions and open a new layer of threats to humans; reserving human rights to humans may need to be explicitly stipulated. A further increased risk is the lack of self-determination through the loss of control over one's own data, which will be collected (and commoditised) in an unprecedented manner. Such risk may lead to the need for recognition of a right to access the own data independently from provision of consent for data collection, processing or use.

Chile was the first jurisdiction to introduce "neuro rights" into its constitution, Spain adopted the (non-binding) Charter of Digital Rights in 2021, including an article on "Digital rights in the use of neurotechnologies" (Charter of Digital Rights 2021, Article XXIV), while in the Council of Europe context the question is whether an evolving interpretation of freedom of thought (Article18 of the International Covenant on Civil and Political Rights and Article 9 of the Convention) is sufficient to address mental self-determination and brain data (Hertz 2023) or whether additional Council of Europe standards are needed to reinforce related guardrails. In general, as pointed out in the respective sections and as described in the appendices to report, the Council of Europe has a plethora of legal frameworks and standards to safeguard human rights and fundamental freedoms, to guide its member states and their stakeholders in their implementation, while the Court with its case law has already ruled on a multitude of legal issues in the context of online environments, media, children rights, etc. The number of available resources across different topics – which may even intertwine – may call for a mapping exercise of the available instruments and tools and a user-friendly presentation of the issues addressed.

⁊⁊ Trade-offs and human rights, rule of law and democracy by design

Trade-offs are to be expected when promoting innovation or economic development. Still, human rights should not be negotiable in the weighting of the various factors and considerations. Instead, they should be the framework and the baseline for innovation, thus offering protection of human rights, the rule of law and democracy by design (Nemitz 2018). A further issue arises when the exercise of one right conflicts with another human right. In this case, there is a need to balance the human rights or freedoms in question (for instance, the freedom of expression with the right to personal life). The Court has developed a methodology for this balancing exercise, as described in the Guide to Article 10.

Outlook

In conclusion, the report identifies technical, legal, societal and ethical issues related to the development and deployment of the metaverse, and the potential benefits and risks that the metaverse presents for human rights, the rule of law and democracy. The ideas expressed in this report reflect a range of subjective perspectives stemming from the different experiences, assumptions or conclusions of the respective experts who contributed to the report. However, the range and the aggregation of these ideas provide a useful insight into current metaverse environments and scenarios, considering past tech rollouts and how these rollouts have affected society.

The way to address these issues in a way that safeguards human rights, the rule of law and democracy is not obvious: the metaverse space is still under development so there is a degree of approximation and uncertainty, next to the impossible task of capturing all relevant risks; there is no clarity or alignment in the terminology; some issues are known issues from previous technology advances and enablers of virtual worlds, yet their dimensions and meaning within the metaverse are diverse; legal frameworks, case law and different standards address many of the points, without being clear whether their scope will cover the virtual iteration of the same issues; and all this while the impact of the metaverse in a scaled version on individuals and societies is still unknown.

At this point of early consideration, a series of decisions needs to be made, linked to the following questions, which are still to be explored.

What are the terms used to describe the metaverse and what is understood by them? How different is the metaverse in the issues it brings from known technologies and environments such as previous iterations of the internet, AI, gaming and social platforms? How much can the metaverse impact our lives, societies and the values we live by, and if that is so transformative, what are the societal values based on which we want to design the metaverse? What can we learn from the way issues in these areas were addressed? Are existing legal frameworks enough to safeguard human rights, the rule of law and democracy, or are new ones needed? Should we move towards international regulation or other global governance models and are regional or domestic regulation and approaches enough? Can the metaverse self-regulate, or is hard law needed? And, if the answer is both, for which areas is what approach more appropriate? Should regulation be technology-specific or principle/outcome/risk-based? What does jurisdiction, supervision and enforcement look like and what are the roles and responsibilities of governments, technology and platform providers and users themselves? How can we build an inclusive, democratic and responsible metaverse that does not violate, but rather promotes, the exercise of human rights, the rule of law and democracy? The answers to these questions will impact the way we decide to govern the metaverse and the way we experience the virtual environment.

References

Abraham M. et al. (2022), "Implications of XR on Privacy, Security and Behaviour: Insights from Experts", in *Nordic Human-Computer Interaction Conference*, NordiCHI '22, available at https://doi.org/10.1145/3546155.3546691.

Acemoglu D. and Restrepo P. (2021), "Tasks, Automation, and the Rise in US Wage Inequality", *National Bureau of Economic Research*, Working Paper 28920, available at DOI 10.3386/w28920: www.nber.org/papers/w28920.

ACLU (2021), "Block the vote: How politicians are trying to block voters from the ballot box", available at www.aclu.org/news/civil-liberties/block-the-vote-voter-suppression-in-2020.

Agile Nations (2023), Metaverse Regulations Working Group, "Non-Legislative Policy Paper: Responsible Metaverse Self-Governance Framework", available at https://accesspartnership.com/access-partnership-contributes-to-agile-nations-policy-paper-on-the-responsible-metaverse-self-governance-framework/.

Ahmed T. et al. (2018), "Up to a Limit? Privacy Concerns of Bystanders and Their Willingness to Share Additional Information with Visually Impaired Users of Assistive Technologies", *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, Vol. 2, Issue 3, available at https://doi.org/10.1145/3264899.

Allied Market Research (2023), Extended Reality Market, available at www.alliedmarketresearch.com/extended-reality-market-A06940.

Artanim (2020), Creating an Interactive VR Experience with the VRTogether platform, available at https://vrtogether.eu/2020/11/18/creating-an-interactive-vr-experience-with-the-vrtogether-platform/.

Atjam R. L. (2022), "Barbados to Establish the World's First Embassy in the Metaverse", *Diplomat Magazine*. 30 August 2022, available at https://diplomatmagazine.eu/2022/08/30/barbados-to-establish-the-world-first-embassy-in-the-metavesre/.

Bailenson J. (2018), "Protecting non-verbal data tracked in virtual reality", *JAMA Pediatrics*, available at https://jamanetwork.com/journals/jamapediatrics/article-abstract/2694803.

Ball M. (2021), "Framework for the Metaverse", available at www.matthewball.vc/all/forwardtothemetaverseprimer.

Barker J. (2020), "Making-up on mobile: The pretty filters and ugly implications of Snapchat", *Fashion, Style & Popular Culture* Issue 2-3, available at https://doi.org/10.1386/fspc_00015_1.

Baxter M. et al. (2021), "'You, Move There!': Investigating the Impact of Feedback on Voice Control in Virtual Environments", *Association for Computing Machinery*, New York, available at https://doi.org/10.1145/3469595.3469609.

Bhutada G. (2021), "Visualizing the Most Used Languages on the Internet", *Visual Capitalist*, available at www.visualcapitalist.com/the-most-used-languages-on-the-internet/.

Boutin P. (2016), "The Secretive World of Selling Data about You", *Newsweek*, 30 May 2016, available at www.newsweek.com/secretive-world-selling-data-about-you-464789.

Braithwaite P. (2018), "Google's 3D Models Are Saving the World's Most At-Risk Heritage Sites", *Wired*, 16 April 2018, available at www.wired.co.uk/article/google-arts-culture-cyark-open-heritage-chichen-itza-bagan.

Brandom R. (2023), "What languages dominate the internet?", *Rest of World*, 7 June 2023, available at https://restofworld.org/2023/internet-most-used-languages/.

Bryson J. J. (2010), "Robots should be slaves", *Close Engagements with Artificial Companions: Key social, psychological, ethical and design issues*, John Benjamins, Amsterdam, pp. 63-74.

Burns T., Cosgrove J. and Doyle F. (2019) "A Review of Interoperability Standards for Industry 4.0.", *Procedia Manufacturing,* Volume 38, pp. 646-53.

Bye K. (2021), "#988: Defining 'Biometric Psychography' to Fill Gaps in Privacy Law to Cover XR Data: Brittan Heller's Human Rights Perspectives", *Voices of VR* Podcast 8 April 2021, available at https://voicesofvr.com/988-defining-biometric-psychography-to-fill-gaps-in-privacy-law-to-cover-xr-data-brittan-hellers-human-rights-perspectives/.

Carnegie Council (2023), A Framework for the International Governance of AI, available at www.carnegiecouncil.org/media/article/a-framework-for-the-international-governance-of-ai.

Charter of Digital Rights (2021), Spanish Minister of Finance and Digital Transformation, available at https://espanadigital.gob.es/en/measure/protection-digital-rights.

Chatila R. and Havens J. C. (2019), "The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems", in Ferreira A. et al. (eds), *Robotics and Well-Being*, pp. 11-16, available at https://link.springer.com/chapter/10.1007/978-3-030-12524-0_2.

Chesney B. and Citron D. K. (2019), "Deep fakes: A looming challenge for privacy, democracy, and national security", *California Law Review* 107 (1753), available at https://scholarship.law.bu.edu/faculty_scholarship/640.

Chopra S. and Maurer F. (2020), "Evaluating User Preferences for Augmented Reality Interactions with the Internet of Things", in *Proceedings of the International Conference on Advanced Visual Interfaces*, Association for Computing Machinery, New York, available at https://doi.org/10.1145/3399715.3399716.

Citron D. K. (2018), "Sexual privacy", *Yale Law Journal*, 128(7), available at www.yalelawjournal.org/article/sexual-privacy.

Climent-Perez P. and Florez-Revuelta F. (2021), "Protection of visual privacy in videos acquired with RGB cameras for active and assisted living applications", *Multimedia Tools and Applications*, 80:23649-64, available at https://doi.org/10.1007/s11042-020-10249-1.

Connecticut Department of Public Health (2008) Fact Sheet: Electric and Magnetic Fields (EMF): Health Concerns.

Council of Europe (2022), Committee on Artificial Intelligence (CAI) (2022) CAI-BU(2022)03 Outline of HUDERIA Risk and Impact Assessment Methodology, available at https://rm.coe.int/cai-bu-2022-03-outline-of-huderia-risk-and-impact-assessment-methodolo/1680a81e14.

Council of Europe (2023a), Key messages of the international conference on xenophobia and racism committed through computer systems: www.coe.int/en/web/cybercrime/international-conference-on-xenophobia-and-racism-committed-through-computer-systems.

Council of Europe (2023b), Committee on Artificial Intelligence (CAI), Draft Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (explanatory report) available at https://rm.coe.int/-1497-10-1b-committee-on-artificial-intelligence-cai-b-draft-framework-convention/1680af0734&format=native.

Court of Justice of the European Union (CJEU) (2023), C-252/21, *Meta v. Bundeskartellamt,* available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=275125&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1.

Cucher D. J. et al (2023) "Virtual Reality Consumer Product Injuries: An Analysis of National Emergency Department Data". *Injury* Volume 54, No. 5, available at www.sciencedirect.com/science/article/abs/pii/S0020138323000347#:~:text=The%20most%20common%20VR%2Drelated,and%20upper%20trunk%20(7.0%25).

Curry A. (2007), "Rome Reborn", *Smithsonian Magazine*, available at www.smithsonianmag.com/history/rome-reborn-157825055/.

Cybercrime Convention Committee (2018), Mapping study on cyberviolence, available at www.coe.int/en/web/cyberviolence/home/-/asset_publisher/ro0bVQCWKTCt/content/t-cy-mapping-study-on-cyberviolence-recommendations.

DeGeurin M. (2022), Targeted Billboard Ads Are a Privacy Nightmare, available at https://gizmodo.com/billboards-facial-recognition-privacy-targeted-ads-1849655599.

Deloitte (2023), Insights - Digital Media Trends 2023, available at www2.deloitte.com/us/en/insights/industry/technology/digital-media-trends-consumption-habits-survey.html.

Di Porto F., Foà D. and Ennis S. (2024), "Emerging Virtual Worlds: Implications for Policy and Regulation", Cerre - Centre on Regulation in Europe, available at https://cerre.eu/publications/emerging-virtual-worlds-implications-for-policy-and-regulation/.

Ericsson (2022), 5G network coverage outlook, available at www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/network-coverage?gclid=CjwKCAjwqZSlBhBwEiwAfoZUIEYVd_D3RUzeKZt9Fr55DdpurJU7Ktr_3XFZEfi55FSSSyjSkbQJAhoCFhkQAvD_BwE&gclsrc=aw.ds.

EUIPO (European Union Intellectual Property Office) (2023), *Trade Mark and Design Guidelines*. 2023, available at https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/contentPdfs/trade_marks/draft-guidelines-wp-2023/Trade_mark_Guidelines_2023_consultation_en.pdf.

EUIPO (2022), "Virtual goods, non-fungible tokens and the metaverse", available at https://euipo.europa.eu/ohimportal/en/news-newsflash/-/asset_publisher/JLOyNNwVxGDF/content/pt-virtual-goods-non-fungible-tokens-and-the-metaverse.

European Commission (2023), Virtual Worlds and Web 4.0 – Factsheet, 2023, available at https://ec.europa.eu/newsroom/dae/redirection/document/97529.

European Commission (2022), The European Declaration on Digital Rights and Principles, available at https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles.

European Commission (2007), Electromagnetic Fields. DG Health and Consumer Protection, Public Health, available at https://ec.europa.eu/health/scientific_committees/opinions_layman/en/electromagnetic-fields07/index.htm.

European Commission (n.d.), The Digital Markets Act: ensuring fair and open digital markets available at https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

European Court of Justice (ECJ) (2011), Judgement of 12 July 2011 - C-324/09 L'Oréal/eBay, Rc. 64 et seq.; German Federal Patent Court, Order of 5 April 2011 - 33 W (pat) 526/10.

European Disability Forum (EDF) (2022), Recommendations for policy makers in the Plug and Pray document, available at www.edf-feph.org/publications/plug-and-pray-2018/.

European Disability Forum (EDF) (2018), "Plug and Pray?", available at www.edf-feph.org/publications/plug-and-pray-2018/.

European Parliament (2023), Draft report on policy implications of the development of virtual worlds - civil, company, commercial and intellectual property law issues (2023/2062(INI)), Committee on Legal Affairs - JURI. Available at https://www.europarl.europa.eu/doceo/document/JURI-PR-753772_EN.pdf.

European Parliament (2024), Resolution of 17 January 2024 on virtual worlds - opportunities, risks and policy implications for the single market available at https://www.europarl.europa.eu/doceo/document/TA-9-2024-0032_EN.html.

EUROPOL (2022), *Policing in the metaverse – what law enforcement needs to know*, available at www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know#downloads.

Evans J. (2022), "Whitepaper Ethics in Medicine, the IEEE Global Initiative on Ethics of Extended Reality (XR)", available at https://standards.ieee.org/wp-content/uploads/2022/02/whitepaper-ethics-in-medicine.pdf.

Evans K., Robbins S. and Bryson J.J. (2023), "Do We Collaborate with What We Design?", *Topics in Cognitive Science,* available at https://doi.org/10.1111/tops.12682.

EY (2022), Metaverse: could creating a virtual world build a more sustainable one?, available at www.ey.com/en_ch/digital/metaverse-could-creating-a-virtual-world-build-a-more-sustainable-one.

Fiani C. et al. (2023), "Parent and adult perspectives on children's use of social virtual reality", currently in review for ACM CSCW 2023.

Flaxman S., Goel S. and Rao J. M. (2016), "Filter Bubbles, Echo Chambers, and Online News Consumption", *Public Opinion Quarterly* (S1), available at https://doi.org/10.1093/poq/nfw006.

Fox J. and McEwan B. (2017), "Distinguishing technologies for social interaction: The perceived social affordances of communication channels scale", *Communication Monographs*, 84:3, pp. 298-318, available at DOI: 10.1080/03637751.2017.1332418.

Frankel S. and Browning K. (2021), "The Metaverse's Dark Side: Here Come Harassment and Assaults", *The New York Times*, available at www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.html.

Franklin M. et al. (2022), "Recognising the importance of preference change: A call for a coordinated multidisciplinary research effort in the age of AI", *The AAAI-22 Workshop on AI For Behavior Change*, available at https://doi.org/10.48550/arXiv.2203.10525.

Franks M-A. (2017), "The Desert of the Unreal: Inequality in Virtual and Augmented Reality" *U.C.D. L. Rev.*, available at https://repository.law.miami.edu/fac_articles/539.

Frischer B. (2014), "Cultural and Digital Memory: Case Studies from the Virtual World Heritage Laboratory", in Galinsky K. (ed.), *Memoria Romana: Memory in Rome and Rome in Memory*, University of Michigan Press, Ann Arbor.

Genser J., Yuste R. and Herrmann S. (2021), "It's Time for Neuro-Rights", *Horizons* 18, Winter 2021, pp. 154-164, available at www.cirsd.org/en/horizons/horizons-winter-2021-issue-no-18/its-time-for-neuro--rights.

Global Digital Civility Index (2024), Promoting digital civility, available at www.microsoft.com/en-us/online-safety/digital-civility.

Gonzalez-Franco M. and Lanier J. (2017), "Model of Illusions and Virtual Reality", *Frontiers in Psychology*, available at https://doi.org/10.3389/fpsyg.2017.01125.

Harborth D. and Pape S. (2021), "Investigating privacy concerns related to mobile augmented reality Apps – A vignette based online experiment", *Computers in Human Behavior*, 122:106833, available at https://doi.org/10.1016/j.chb.2021.106833.

Heller B. (2020), "Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law", *Vanderbilt Journal of Entertainment & Technology Law*, (1), available at https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss1/1.

Hertz N. (2023) "Neurorights – Do we need new human rights? A Reconsideration of the Right to Freedom of Thought", *Neuroethics* 16, 5, available at https://doi.org/10.1007/s12152-022-09511-0.

Hugues O., Fuchs P. and Nannipieri O. (2011), "New augmented reality taxonomy: Technologies and features of augmented environment", in *Handbook of Augmented Reality*, available at https://hal.science/hal-00595204.

Hummel D. and Maedche A. (2019), "How effective is nudging? A quantitative review on the effect sizes and limits of empirical nudging studies", *Journal of Behavioral and Experimental Economics*, available at http://dx.doi.org/10.1016/j.socec.2019.03.005.

Hupont Torres I. et al. (2023), *Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU*, Publications Office of the European Union, Luxembourg, available at https://data.europa.eu/doi/10.2760/51579.

Information Commissioner's Office (ICO) (2020), Age Appropriate Design: A Code of Practice for Online Services, available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/.

Institute of Electrical and Electronics Standards Association (IEEE SA) (2022a), Ethical Considerations of Extended Reality (XR), available at https://standards.ieee.org/beyond-standards/industry/technology-industry/ethical-considerations-of-extended-reality-xr/.

IEEE SA (2022b), Why Are Standards Important for the Metaverse?, available at https://standards.ieee.org/beyond-standards/industry/technology-industry/why-are-standards-important-for-the-metaverse/.

IEEE SA (2021), IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children," in *IEEE Std 2089-2021* , pp.1-54, 30 November 2021, available at https://ieeexplore.ieee.org/document/9627644.

IEEE SA (2020), IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being," in IEEE Std 7010-2020, Vol., No., pp.1-96, 1 May 2020, available at https://ieeexplore.ieee.org/document/9084219.

IEEE SA (2016), Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems, Ethically Aligned Design (EAD) Volume 1, available at https://standards.ieee.org/industry-connections/ec/ead-v1/.

Ienca M. (2017), "Do We Have a Right to Mental Privacy and Cognitive Liberty?", *Scientific American*, 3 May 2017, available at https://blogs.scientificamerican.com/observations/do-we-have-a-right-to-mental-privacy-and-cognitive-liberty/.

INTA (International Trademark Association) (2023), "Trademarks in the Metaverse", available at www.inta.org/news-and-press/press-releases/the-international-trademark-association-releases-white-papers-on-trademarks-in-the-metaverse-and-non-fungible-tokens/.

International Labour Organization (ILO) (2021), World Social Protection Report, available at www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_817653/lang--en/index.htm.

INTERPOL (2022), Technology Assessment Report on the Metaverse, available at www.interpol.int/News-and-Events/News/2022/INTERPOL-launches-first-global-police-Metaverse.

INTERPOL (2024), "Metaverse. A law enforcement perspective. Use Cases, Crime, Forensics, Investigation, and Governance, White paper", available at https://www.interpol.int/en/content/download/20828/file/Metaverse a law enforcement perspective.pdf.

IPR Helpdesk (2022), Intellectual Property in the Metaverse. Episode III: Patents, available at https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/intellectual-property-metaverse-episode-iii-patents-2022-05-30_en.

ITU Forum on Embracing the Metaverse (2023), available at www.itu.int/en/ITU-T/ssc/Pages/1st-forum-metaverse.aspx.

Joergensen A.C. et al. (2021), "Spinal Pain in Pre-Adolescence and the Relation with Screen Time and Physical Activity Behavior", *BMC Musculoskelet Disor.* 22, No. 1, p. 393, available at https://pubmed.ncbi.nlm.nih.gov/33902525.

Joshi S. (2021), It's 2021, but People Are Still Using a Racist Blackface Filter on Instagram, available at www.vice.com/en/article/g5gkxw/racist-blackface-filterinstagram-viral-videos.

Kardefelt-Winther D. (2014), "Problematizing excessive online gaming and its psychological predictors", *Computers in Human Behavior* 31, pp. 118-22.

Khamis M. and Alt F. (2021), "Privacy and Security in Augmentation Technologies", in Dingler T. and Niforatos E. (eds), *Technology-Augmented Perception and Cognition, Human – Computer Interaction Series*, available at https://doi.org/10.1007/978-3-030-30457-7_8.

Khan A. A. (2022), "How Cybersecurity is Changing with the Advent of the Metaverse", *Gulf Business*, 23 December 2022.

Knight W. (2022), "The US Military is Building Its Own Metaverse", *Wired*, 17 May 2022, available at www.wired.com/story/military-metaverse/.

Koike M. and Loughnan S. (2021), "Virtual relationships: Anthropomorphism in the digital age", *Social and Personality Psychology Compass*, 15(6), e12603.

Kroger J. L., Lutz O. H-M. and Muller F. (2020), "What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking", in Friedewald M. et al. (eds), *Privacy and Identity Management. Data for Better Living: AI and Privacy*: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Windisch, Switzerland, 19-23 August 2019, Revised Selected Papers, pages 226-241, Springer International Publishing, Cham, available at https://doi.org/10.1007/978-3-030-42504-3_15.

Kyto M., Hirskyj-Douglas I. and McGookin D. (2021), "From Strangers to Friends: Augmenting Face-to-face Interactions with Faceted Digital Self-Presentations", in *Augmented Humans Conference 2021,* available at https://doi.org/10.1145/3458709.3458954.

Lemley M. A. and Volokh E. (2017), Law, virtual reality, and augmented reality, U. Pa. L. Rev., available at https://scholarship.law.upenn.edu/penn_law_review/vol166/iss5/1/.

Lodder A.R. (2013), Ten Commandments of Internet Law Revisited: Basic Principles for Internet Lawyers, 22 Information & Communications Technology Law, 3, pp. 264-276, 266, available at http://ssrn.com/abstract=2343486.

Loewenheim U. (2020), "Urheberrecht Kommentar" (2020), in Gerhard Schricker and Ulrich Loewenheim (eds), *Copyright Law*, 6th Edition 2020, Para. 16, Rc. 19.

Luo L. et al. (2022), "The effect of avatar facial expressions on trust building in social virtual reality", *Vis Comput*, available at https://doi.org/10.1007/s00371-022-02700-1.

Majerova J. and Pera A. (2022), "Haptic and Biometric Sensor Technologies, Spatio-Temporal Fusion Algorithms, and Virtual Navigation Tools in the Decentralized and Interconnected Metaverse", *Review of Contemporary Philosophy (21)*, available at www.ceeol.com/search/article-detail?id=1071092.

Maloney D., Freeman G. and Robb A. (2021), "Stay connected in an immersive world: Why teenagers engage in social virtual reality", *Association for Computing Machinery*, 6 2021, pp. 69-79, available at https://doi.org/10.1145/3459990.3460703.

Maloney D., Freeman G and Robb A. (2020), "A virtual space for all: Exploring children's experience in social virtual reality", *Association for Computing Machinery*, pp. 472-83, available at https://dl.acm.org/doi/10.1145/3410404.3414268.

Mangina E. (2021), XR Ethics in Education, IEEE Global Initiative on Ethics of XR, available at https://ieeexplore.ieee.org/document/9650798.

Mann S. (2013), "Veilance and reciprocal transparency: Surveillance versus sousveillance, AR glass, lifeglogging, and wearable computing", in 2013 IEEE International Symposium on Technology and Society (ISTAS): Social Implications of Wearable Computing and Augmented Reality in Everyday Life, available at https://doi.org/10.1109/ISTAS.2013.6613094.

Markoff J. (2006), "Entrepreneurs See a Web Guided by Common Sense", *The New York Times,* 12 Nov. 2006, available at www.nytimes.com/2006/11/12/business/entrepreneurs-see-a-web-guided-by-common-sense.html.

Masnick M. (2014), "A Dystopian Future of Ads That Won't Stop Until You Say 'McDonald's' Could Be Avoided With More Transparency", available at www.techdirt.com/2014/11/03/dystopian-future-ads-that-wont-stop-until-you-say-mcdonalds-could-be-avoided with-more-transparency/.

Mathur A., Mayer J and Kshirsagar M. (2021), "What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods", available at https://doi.org/10.1145/3411764.3445610.

McGill M. (2021), "Extended Reality (XR) and the Erosion of Anonymity and Privacy", *The IEEE Global Initiative on Ethics of Extended Reality (XR) Report*, available at https://ieeexplore.Ieee.org/document/9619999.

McGill M. et al. (2020a), "Expanding the Bounds of Seated Virtual Workspaces", ACM Transactions on Computer-Human Interaction, (3), available at https://doi.org/10/ghwfhx.

McGill M. et al (2020b), "Augmenting TV Viewing using Acoustically Transparent Auditory Headsets", ACM International Conference on Interactive Media Experiences, available at https://doi.org/10.1145/3391614.3393650.

McKenna K. Y., Green A. S. and Gleason M. E. (2002), "Relationship formation on the Internet: What's the big attraction?", *Journal of Social Issues*, 58(1), pp. 9-31.

McKinsey & Company (2022a), Value creation in the metaverse, available at www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/value-creation-in-the-metaverse.

McKinsey & Company (2022b), Even in the metaverse, women remain locked out of leadership roles, available at www.mckinsey.com/featured-insights/diversity-and-inclusion/even-in-the-metaverse-women-remain-locked-out-of-leadership-roles.

McMichael L. et al. (2020), “Parents of adolescents perspectives of physical activity, gaming and virtual reality: Qualitative study”, *JMIR Serious Games* 2020;8(3):e14920, available at https://games.jmir.org/2020/3/e14920.

Melnick K. (2022), “Finally, an app that lets you censor reality”, available at https://vrscout.com/news/finally-an-app-that-lets-you-censor-reality/.

Miazhevich G. (2015), “Sites of subversion: online political satire in two post-Soviet states”, *Media, Culture & Society*, 37(3), pp. 422-439, available at https://doi.org/10.1177/0163443714567015.

MIT Technology Review Insights (2023), The Emergent Industrial Metaverse, available at www.technologyreview.com/2023/03/29/1070355/the-emergent-industrial-metaverse/.

Moore A. G. et al. (2021), “Personal Identifiability of User Tracking Data During VR Training”, in *2021 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, available at https://doi.org/10.1109/VRW52623.2021.00160.

Mystakidis S. (2022), Metaverse, Encyclopedia, available at https://doi.org/10.3390/encyclopedia2010031.

Nassauer A. and Legewie N. M. (2021), “Video Data Analysis: A Methodological Frame for a Novel Research Trend”, *Sociological Methods & Research*, (1), available at https://doi.org/10.1177/0049124118769093.

Nemitz P. (2018), “Constitutional democracy and technology in the age of artificial intelligence”, *Philosophical transactions. Series A, Mathematical, physical, and engineering sciences,* 376(2133), 20180089, available at https://doi.org/10.1098/rsta.2018.0089.

Nokia (2023), Powering the Industrial Metaverse, available at www.nokia.com/metaverse/industrial-metaverse/.

Nordemann-Schiffel in: Reinhard Ingerl, Christian Rohnke, Axel Nordemann and Anke Nordemann-Schiffel (2023), *Trademark Law*, 4th Edition, Introduction Rc. 44.

Organisation for Economic Co-operation and Development (OECD) (2019), Recommendation of the Council on Responsible Innovation in Neurotechnology, OECD/LEGAL/0457, available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0457.

OECD (26 Feb 2009), Alternatives to traditional regulation, available at www.oecd.org/fr/gov/latestdocuments/92/.

Oh H. J. et al. (2023), “Social benefits of living in the metaverse: The relationships among social presence, supportive interaction, social self-efficacy, and feelings of loneliness”, *Computers in Human Behavior*, available at www.sciencedirect.com/science/article/pii/S0747563222003181.

O’Hagan J. et al. (2023), “Privacy-Enhancing Technology and Everyday Augmented Reality: Understanding Bystanders’ Varying Needs for Awareness and Consent”, *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 6(4), available at https://doi.org/10.1145/3569501.

OHCHR (Office of the High Commissioner of Human Rights) (2022a), The human right to a clean, healthy and sustainable environment: a catalyst for accelerated action to achieve the Sustainable Development Goals, available at www.ohchr.org/en/documents/thematic-reports/a77284-human-right-clean-healthy-and-sustainable-environment-catalyst.

OHCHR (2022b), The impacts of climate change on the human rights of people in vulnerable situations, available at www.ohchr.org/en/documents/thematic-reports/ahrc5057-impacts-climate-change-human-rights-people-vulnerable.

Ohrnberger J., Fichera E. and Sutton M. (2017), "The relationship between physical and mental health: A mediation analysis", *Social Science & Medicine*, pp. 195 (42-49).

Park D. (2022), "U.S., Korea applied for over 75% of world's metaverse patents: report", *Forkast*, available at https://forkast.news/us-korea-over-75-worlds-metaverse-patents/.

Park S.-M. and Kim Y.-G. (2022), "A Metaverse: Taxonomy, Components, Applications, and Open Challenges", *IEEE Access*, available at https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9667507.

Pase S. (2012), "Ethical considerations in augmented reality applications", in *Proceedings of the International Conference on E-Learning, e-Business, Enterprise Information Systems, and e Government (EEE)*, available at www.semanticscholar.org/paper/Ethical-Considerations-in-Augmented-Reality-Pase/ce7a3f370e5dcf06a05d2b55f2abb1a0cb5e3cca.

Petit N. et al. (2022), Metaverse Competition Agency: White Paper (9 December 2022), VU University Amsterdam Legal Studies Paper Series (forthcoming), available at https://ssrn.com/abstract=4297960 or http://dx.doi.org/10.2139/ssrn.4297960.

Petkov M. (2023), "The Metaverse and its impact on politics and governance", LinkedIn, 25 January 2023, available at www.linkedin.com/pulse/metaverse-its-impact-politics-governance-martin-petkov.

Pew Research Center (2022), "The Metaverse in 2040", available at www.pewresearch.org/internet/2022/06/30/the-metaverse-in-2040/.

Prakash C. D. and Majumdar A. (2021), "Analyzing the role of national culture on content creation and user engagement on Twitter: The case of Indian Premier League cricket franchises", *International Journal of Information Management*, Volume 57, 102268.

RAND Europe and Salesforce (2021), The Digital Skills Gap Comes at a Cost: 14 G20 Countries Could Miss Out on $11.5 Trillion Cumulative GDP Growth, available at www.salesforce.com/news/stories/digital-skills-gap/.

Read T., Sanchez C. and De Amicis R. (2021), "Engagement and time perception in virtual reality", *Proceedings of the 2021 HFES 65th international annual meeting*, available at https://journals.sagepub.com/doi/abs/10.1177/1071181321651337.

Renieris E. (2023), *Beyond data: Reclaiming human rights at the dawn of the metaverse*, MIT Press.

Reuters (2023), Colombia court moves to metaverse to host hearing, available at www.reuters.com/world/americas/colombia-court-moves-metaverse-host-hearing-2023-02-24/.

RightsCon (2021), "As AR/VR becomes a reality, it needs a human rights framework", available at https://www.eff.org/event/rightscon-arvr-becomes-reality-it-needs-human-rights-framework.

Rixen J. O. et al. (2021), Exploring Augmented Visual Alterations in Interpersonal Communication, available at https://doi.org/10.1145/3411764.3445597.

Rodriguez K. and Opsahl K. (2020), Augmented Reality Must Have Augmented Privacy, available at www.eff.org/deeplinks/2020/10/augmented-reality-must-have augmented-privacy.

Rosenberg L. (2023), "The Metaverse and Conversational AI as a Threat Vector for Targeted Influence", IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2023, pp. 0504-0510, available at https://ieeexplore.ieee.org/document/10099167.

Ryan-Mosley T. (2021), Beauty filters are changing the way young girls see themselves, available at https://www.technologyreview.com.

Saeghe P. et al. (2022), "Evaluating and Updating a Design Space for Augmented Reality Television", in *ACM International Conference on Interactive Media Experiences*, IMX 2022, available at https://doi.org/10.1145/3505284.3529965.

Schmidt A. T. and Engelen B. (2020), "The ethics of nudging: An overview", *Philosophy Compass*, (4), available at https://doi.org/10.1111/phc3.12658.

Schraffenberger H. K. (2018), *Arguably Augmented Reality: Relationships between the Virtual and the Real*, PhD thesis, available at https://openaccess.leidenuniv.nl/handle/1887/67292.

Schraffenberger H. and Van der Heide E. (2014), "Everything augmented: On the real in augmented reality", *Journal of Science and Technology of the Arts*, (1).

Schurger A. et al. (2021), "What Is the Readiness Potential?" *Trends in Cognitive Sciences*, (7), available at https://doi.org/10.1016/j.tics.2021.04.001.

Shao D., Liu C. and Tsow F. (2021), "Noncontact Physiological Measurement Using a Camera: A Technical Review and Future Directions", *ACS Sensors,* available at https://doi.org/10.1021/acssensors.0c02042.

Slater M. et al. (2020), "The Ethics of Realism in Virtual and Augmented Reality", *Frontiers in Virtual Reality*, available at https://doi.org/10.3389/frvir.2020.00001.

Spano R. (2017), "Intermediary liability for online users: comments under the European Convention on Human Rights", *Human Rights Law Review*.

Srivastav T. (2019), "ECDA Singapore Shows Why Teachers Will Be Hard to Replace by Robots on Teacher's Day", *The Drum*. 6 September 2019, available at www.thedrum.com/news/2019/09/06/ecda-singapore-shows-why-teachers-will-be-hard-replace-robots-teachers-day.

Stephens M. (2022), Metaverse and its Governance, The IEEE Global Initiative on Ethics of Extended Reality (XR) Report, available at www.researchgate.net/publication/361362815_Metaverse_and_Its_Governance_-_The_IEEE_Global_Initiative_on_Ethics_of_Extended_Reality_XR_Report.

Stephens et al. (2019), Agile Government: Agile Skills Report (see table at the end – there is no alignment on skill for the future), available at www.mbrsg.ae/home/research/policy-council/agile-government-agile-skills-report.

Sykownik P. et al. (2021), "The Most Social Platform Ever? A Survey about Activities & Motives of Social VR Users", *2021 IEEE Virtual Reality and 3D User Interfaces (VR)*, Lisbon, pp. 546-554, available at https://doi.org/10.1109/VR50410.2021.00079.

Tibbets C. and Brooker C. (2014), "White Christmas", *Black Mirrors*, Season 2.

Tseng W-J. et al. (2022), "The Dark Side of Perceptual Manipulations in Virtual Reality", *CHI Conference on Human Factors in Computing Systems*, available at https://doi.org/10.1145/3491102.3517728.

UNICEF (2023), The Metaverse, Extended Reality and Children, available at www.unicef.org/globalinsight/reports/metaverse-extended-reality-and-children.

Vaillant G. E. (1979), "Natural History of Male Psychologic Health – Effects of Mental Health on Physical Health", *N Engl J Med*, 301: 1249-1254, available at https://pubmed.ncbi.nlm.nih.gov/1267569/.

Van Heugten-van der Kloet D., et al. (2018), "Out-of-body experience in virtual reality induces acute dissociation", *Psychology of Consciousness: Theory, Research, and Practice*, 5(4), pp. 346 -357, available at https://psycnet.apa.org/doi/10.1037/cns0000172.

WEF (Word Economic Forum) (2024), "Metaverse Identity: Defining the Self in a Blended Reality", available at https://www3.weforum.org/docs/WEF_Metaverse_Identity_Defining_the_Self_in_a_Blended_Reality_2024.pdf.

WEF (World Economic Forum) (2023a), "6 World of Work Challenges the Metaverse Will Help Address", available at www.weforum.org/agenda/2023/01/6-world-of-work-challenges-the-metaverse-will-address-davos2023/.

WEF (World Economic Forum) (2023b), "The metaverse will make its biggest impact on industry. Here's why", available at www.weforum.org/agenda/2023/01/metaverse-biggest-impact-industry-davos2023/.

WEF (World Economic Forum) (2023c), Decentralised autonomous organisation toolkit, available at www.weforum.org/publications/decentralized-autonomous-organization-toolkit/.

WEF (World Economic Forum) (2023d), Future of Jobs report, available at www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf.

WEF (World Economic Forum) (2023e), "Social Implications of the Metaverse", available at https://www.weforum.org/publications/social-implications-of-the-metaverse/.

WEF (World Economic Forum) (2023f), "Interoperability in the Metaverse", available at www3.weforum.org/docs/WEF_Interoperability_in_the_Metaverse.pdf.

Wexler A. (2017), "The Social Context of "Do-It-Yourself" Brain Stimulation: Neurohackers, Biohackers, and Lifehackers" *Front. Hum. Neurosci.*, Sec. Cognitive Neuroscience Volume 11, available at https://doi.org/10.3389/fnhum.2017.00224.

White House (2023), Executive Order, 30 October 2023, available at www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/.

WHO (World Health Organization) (2023), Suicide fact sheets, 28 August 2023, available at www.who.int/news-room/fact-sheets/detail/suicide.

WHO (World Health Organization) (2017), "World Bank and WHO: Half the world lacks access to essential health services, 100 million still pushed into extreme poverty because of health expenses", available at www.who.int/news/item/13-12-2017-world-bank-and-who-half-the-world-lacks-access-to-essential-health-services-100-million-still-pushed-into-extreme-poverty-because-of-health-expenses.

WIPO (World Intellectual Property Organization (2021), Technology Trends, Assistive Technology, available at www.wipo.int/publications/en/details.jsp?id=4541

Wohlwend K. E. (2010). A is for avatar: Young children in literacy 2.0 worlds and literacy 1.0 schools.

Wyss J. (2021), "Barbados is Opening a Diplomatic Embassy in the Metaverse", Bloomberg Technology, available at www.bloomberg.com/news/articles/2021-12-14/barbados-tries-digital-diplomacy-with-planned-metaverse-embassy.

Yfantis V. and Ntalianis K. (2022), "Exploring the Potential Adoption of Metaverse in Government", *Data Intelligence and Cognitive Informatics – ICDICI 2022*, Springer Nature, Singapore, pp. 815-824, available at DOI: 10.1007/978-981-19-6004-8_61.

Zheng N. et al. (2017), "Hybrid-augmented intelligence: collaboration and cognition", *Frontiers of Information Technology & Electronic Engineering*, (2), available at https://doi.org/10.1631/FITEE.1700053.

Further reading

European Green Digital Coalition (EGDC) (2022), available at www.greendigitalcoalition.eu/.

IEEE CertifiAIEd, available at https://engagestandards.ieee.org/ieeecertifaied.html.

IEEE Metaverse Congress, available at https://engagestandards.ieee.org/IEEE-Metaverse-Congress.html.

IEEE SA (2023), IEEE P2048: Standard for Metaverse: terminology, definitions, and taxonomy, available at standards.ieee.org/ieee/2048/11169/#:~:text=Standard%20for%20Metaverse%3A%20Terminology%2C%20Definitions%2C%20and%20Taxonomy&text=This%20standard%20specifies%20the%20terminology,a%20roadmap%20for%20metaverse%20developers.

IEEE (2016), Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems, Ethically Aligned Design v.1, available at www.standardsuniversity.org/e-magazine/march-2017/ethically-aligned-standards-a-model-for-the-future/.

IEEE (2024), “White Paper - Position, Posture, and Pose Definitions for 3D Body Processing”, available at https://ieeexplore.ieee.org/document/10486845.

Kaspersky (2021), “How to Stop Data Brokers from Selling Your Personal Data”, available at https://usa.kaspersky.com/resource-center/preemptive-safety/how-to-stop-data-brokers-from-selling-your-personal-information.

KPMG (2022), Shaping the metaverse towards sustainability, available at https://kpmg.com/dk/en/home/insights/2022/12/shaping-the-metaverse-towards-sustainability.html.

Maloney D., Freeman G. and Robb A. (2020), “It is complicated: Interacting with children in social virtual reality”, *Proceedings 2020 IEEE Conference on Virtual Reality and 3D User Interfaces, VRW 2020*, pages 343-347, available at https://doi.org/10.1109/VRW50115.2020.00075.

UNFPA (2021), Five ways climate change hurts women and girls, available at www.unfpa.org/news/five-ways-climate-change-hurts-women-and-girls.

WEF (World Economic Forum) (n.d.), Defining and Building the Metaverse Initiative, available at https://initiatives.weforum.org/defining-and-building-the-metaverse/home.

WHO and The World Bank (2011), *World Report on Disability*, World Health Organization, Geneva, available at www.who.int/teams/noncommunicable-diseases/sensory-functions-disability-and-rehabilitation/world-report-on-disability.

Council of Europe

Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, 2003, available at https://rm.coe.int/168008160f.

Children’s data protection in an educational setting, 2021, available at https://rm.coe.int/prems-001721-gbr-2051-convention-108-txt-a5-web-web-9-/1680a9c562.

Civil Participation in Decision-Making, available at www.coe.int/en/web/good-governance/civil-participation-in-decision-making-processes#:~:text=Over%20the%20years%2C%20the%20,Making.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), 1981, available at www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108.

Convention on Cybercrime (Budapest Convention), 2001, available at www.coe.int/en/web/cybercrime/the-budapest-convention.

Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention), available at www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=201.

Cooperation between law enforcement and internet service providers against cybercrime: towards common guidelines, 2008, available at https://rm.coe.int/2088-33-law-enforcement-isp-guidelines-2020/1680a091a7.

Cybercrime Convention Committee, Guidance note on identity theft and phishing in relation to fraud, 2013, available at https://rm.coe.int/16802e7132.

Digital Agenda 2022-2025, 2022, available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680a552e3.

Declaration by the Committee of Ministers on Internet Governance Principles, 2011, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f6.

Declaration by the Committee of Ministers on the need to protect children's privacy in the digital environment, 2021, available at www.coe.int/en/web/data-protection/-/council-of-europe-s-call-to-step-up-the-protection-of-children-s-privacy-in-the-digital-environment.

Digital Partnership, 2022, available at https://rm.coe.int/10-06-2022-digital-partnership-general-doc-updated/1680a6e634.

Education Strategy 2024-2030, 2023, available at https://rm.coe.int/education-strategy-2024-2030-26th-session-council-of-europe-standing-c/1680abee81.

European Convention on Human Rights, 1950, available at www.echr.coe.int/documents/d/echr/convention_ENG.

European Court of Human Rights (2002), Guide on Article 2 of the European Convention on Human Rights – Right to Life, 31 December 2020, available at www.refworld.org/docid/6048e29c2.html.

European Court of Human Rights, Guide on Article 10 of the European Convention on Human Rights, available at www.echr.coe.int/documents/d/echr/guide_art_10_eng.

European Social Charter, 1961, www.coe.int/en/web/european-social-charter/about-the-charter.

Guidance note on content moderation: Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation, 2021, available at https://rm.coe.int/content-moderation-en/1680a2cc18.

Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 2017, available at https://rm.coe.int/16806ebe7a.

Guidelines for the cooperation between law enforcement and internet service providers against cybercrime, 2008, available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3ba.

Human rights guidelines for internet service providers, 2008, available at https://rm.coe.int/16805a39d5.

Protocol amending the Convention for the protection of individuals with regard to automatic processing of personal data (CETS No. 223), 2018, available at https://rm.coe.int/16808ac918.

Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a67955.

Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, available at https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154.

Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168093b26e.

Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, available at https://rm.coe.int/0900001680790e14.

Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa.

Recommendation CM/Rec(2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c1e59.

Recommendation CM/Rec(2015)6 of the Committee of Ministers to member States on the free, transboundary flow of information on the Internet, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f20.

Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804d5b31.

Recommendation CM/Rec(2013)1 of the Committee of Ministers to member States on gender equality and media, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c7c7e.

Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805caa87.

Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805caa9b.

Recommendation CM/Rec(2011)7 of the Committee of Ministers to member States on a new notion of media, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2c0.

Recommendation CM/Rec(2010)13 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00.

Recommendation CM/Rec(2007)16 of the Committee of Ministers to member States on measures to promote the public service value of the Internet, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d4a39.

Reykjavik Declaration, United around our values, 2023, available at https://rm.coe.int/4th-summit-of-heads-of-state-and-government-of-the-council-of-europe/1680ab40c1.

Strategy for the rights of the child (2022-2027), 2022, available at https://rm.coe.int/council-of-europe-strategy-for-the-rights-of-the-child-2022-2027-child/1680a5ef27.

Study on the impact of artificial intelligence, its potential for promoting equality, including gender equality, and the risks to non-discrimination, 2023, available at https://rm.coe.int/prems-112923-gbr-2530-etude-sur-l-impact-de-ai-web-a5-1-2788-3289-7544/1680ac7936.

Two clicks forward and one click back, Report on children with disabilities in the digital environment, 2019, available at https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f.

Venice Commission Rule of Law Checklist, 2016, available at www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2016)007-e.

United Nations

International Covenant of Civil and Political Rights, 1966, available at www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

UN Convention on the Rights of Persons with Disabilities (CRPD), 2008, available at https://social.desa.un.org/issues/disability/crpd/convention-on-the-rights-of-persons-with-disabilities-crpd.

UN/OHCHR press release, 28 July 2022, available at www.ohchr.org/en/press-releases/2022/07/historic-day-human-rights-and-healthy-planet-un-expert.

Appendix I

Uses of the metaverse

The earliest iterations of the metaverse have been dominated by a recreational dynamic and many of the earliest successes have been games. Some of these games that are likely to be familiar to a large segment of the global population include Roblox (3D), Pokémon Go (augmented reality), Fortnite and Second Life (2D world). As the metaverse evolves, it is expected to integrate additional components of the social economy and also commercial production activities. The metaverse is a new generation of internet applications and social ecology built to realise the integration of virtual and physical worlds in time and space.

The metaverse holds immense potential across various application areas, revolutionising engagement with entertainment; medicine; health, fitness and wellness; education and learning; and cultural and social experiences. Below is an overview of some of the current and possible applications within these domains, showcasing the transformative power of the metaverse to enhance experiences and improve outcomes.

Entertainment

The metaverse presents a paradigm shift in entertainment experiences. Virtual reality and augmented reality technologies enable users to immerse themselves in interactive and dynamic virtual worlds, transcending traditional boundaries of passive consumption. Virtual gaming experiences within the metaverse offer unprecedented levels of interactivity and social engagement, creating vibrant virtual communities and economies. Virtual concerts, events and performances allow artists to reach global audiences in unique and immersive ways. Additionally, the metaverse has the potential to reshape storytelling, enabling users to become active participants in narrative-driven experiences. By considering these factors, stakeholders can navigate the opportunities and challenges within the entertainment industry in the metaverse, ensuring responsible and inclusive growth while providing immersive and engaging entertainment experiences for users.

Entertainment in the metaverse: SWOT (strengths, weaknesses, opportunities, threats) analysis

Strengths	Weaknesses	Opportunities	Threats
Immersive experiences: the metaverse provides an unparalleled level of immersion, allowing users to engage with entertainment content in interactive and dynamic virtual worlds. Social engagement: virtual gaming experiences within the metaverse foster vibrant communities and economies, enabling social interactions and collaboration among users. Global reach: virtual concerts, events and performances transcend geographical limitations, enabling artists to reach global audiences and expand their fan bases. Interactive storytelling: the metaverse offers the opportunity to reshape storytelling by allowing users to become active participants in narrative-driven experiences.	Technological requirements: access to the metaverse relies on the availability of compatible hardware and a stable internet connection, which may limit accessibility for some users. Steep learning curve: navigating virtual environments and mastering the intricacies of metaverse platforms may involve a steep learning curve for both content creators and users. Content moderation: ensuring appropriate content and enforcing community guidelines within the metaverse can be challenging, requiring robust content moderation systems and policies. Lack of diversity: a lack of diversity among developers can have an impact on content and economic opportunities for groups and individuals that may be excluded from experiencing related benefits. This may also apply to metaverse applications in the fields of medicine; health, fitness and wellness; education and learning; and social and cultural engagement.	Innovation and creative expression: the metaverse opens up new possibilities for content creators to experiment with innovative forms of entertainment and explore novel creative expressions. Collaboration and co-creation: virtual environments within the metaverse allow artists and users to collaborate on projects and experiences. Monetisation and economic opportunities: the metaverse presents avenues for new business models, involving virtual marketplaces, digital assets and virtual economies, offering monetisation opportunities for content creators and entrepreneurs.	Privacy and security risks: the metaverse raises concerns about privacy, data security and potential vulnerabilities that could be exploited by malicious actors, requiring robust security measures and user protection mechanisms. Intellectual property challenges: protecting intellectual property rights within the metaverse may be complex, with the potential for copyright infringement and unauthorised use of virtual assets. Fragmentation and interoperability: the metaverse is composed of various platforms and ecosystems, which may lead to fragmentation and interoperability challenges, hindering seamless user experiences and content distribution.

Medicine

The metaverse is poised to transform the field of medicine by introducing innovative approaches to diagnosis, treatment and patient care. Virtual reality simulations can be utilised for medical training, allowing students and professionals to practise complex procedures in realistic virtual environments. Telemedicine within the metaverse enables remote consultations, expanding access to healthcare services and facilitating personalised care for patients in remote or underserved areas. Further, virtual environments can help with rehabilitation and therapy, providing immersive and engaging experiences that aid physical and mental recovery. The healthcare industry can harness the potential of the metaverse while addressing associated risks and challenges. Through careful planning and collaboration, stakeholders can utilise metaverse technologies to transform medical education, expand access to healthcare and enhance patient care and rehabilitation.

Medicine in the metaverse: SWOT analysis			
Strengths	**Weaknesses**	**Opportunities**	**Threats**
Innovative training and education: virtual reality simulations within the metaverse offer realistic and immersive medical training experiences, allowing students and professionals to practise complex procedures and enhance their skills. Remote healthcare services: telemedicine in the metaverse enables remote consultations, expanding access to healthcare services and overcoming geographical barriers, particularly for patients in remote or underserved areas.	Technology reliability: the success of medical applications in the metaverse relies on the availability of stable and reliable technology, including VR and AR hardware and internet connectivity. Lack of access to technology could present barriers to implementing metaverse-based medical applications, limiting their adoption in certain regions or healthcare settings. Limited physical examination: telemedicine in the metaverse may have limitations for conducting physical examinations, which are essential for certain medical diagnoses and assessments.	Enhanced medical education: the metaverse provides opportunities for innovative and immersive medical education, fostering a deeper understanding of medical concepts and procedures among students. Improved access to healthcare: telemedicine in the metaverse can expand access to healthcare services, especially for individuals in remote or underserved areas, reducing geographical barriers and increasing patient reach.	Data security and privacy: medical data shared and stored within the metaverse must be safeguarded to protect patient privacy and ensure compliance with data-protection regulations. Ethical and legal considerations: the use of virtual environments in medicine raises ethical and legal questions, such as informed consent, liability, the appropriate use of virtual technologies in patient care and the potential impact on the doctor–patient relationship. It may also require

Medicine in the metaverse: SWOT analysis			
Strengths	**Weaknesses**	**Opportunities**	**Threats**
Personalised care and rehabilitation: virtual environments within the metaverse can provide personalised rehabilitation and therapy experiences, enhancing physical and mental recovery for patients.	Learning curve and training costs: implementing and adopting metaverse-based medical training programmes may involve a steep learning curve for healthcare professionals and there are costs for acquiring the necessary equipment and training resources. Unequal access to services: this could occur as a result of inequality in terms of resources, digital literacy, connection and materials. This is a weakness that can be found in other metaverse environments too.	Virtual rehabilitation and therapy: virtual environments within the metaverse offer engaging and personalised rehabilitation and therapy experiences, promoting physical and mental recovery for patients.	navigating complex regulatory frameworks, ensuring compliance with existing healthcare regulations and standards. Technical limitations: metaverse technology may have limitations in accurately simulating real-world medical scenarios, requiring ongoing development and advancements.

Health, fitness and wellness

The metaverse offers exciting possibilities for promoting health, fitness and overall wellness. Virtual reality exercise programmes provide engaging and immersive workout experiences, motivating users to stay active and adopt healthy lifestyles. Virtual fitness communities allow individuals to connect and exercise together regardless of their physical location. Moreover, virtual wellness retreats and mindfulness applications within the metaverse offer opportunities for relaxation, meditation and self-care, promoting positive mental health in an increasingly digital world. The health, fitness and wellness industry can maximise the metaverse's potential to encourage healthy lifestyles and improve health while also addressing any unintended mental or physical health consequences associated with constant use of screens and computers to replace physical human interaction and outdoor activities. Collaboration among fitness experts, technology developers and health professionals can ensure the responsible and effective use of metaverse technologies in promoting physical and positive mental health.

Health, fitness and wellness in the metaverse: SWOT analysis			
Strengths	**Weaknesses**	**Opportunities**	**Threats**
Engaging and immersive experiences: the metaverse provides engaging and immersive virtual reality exercise programmes, making fitness activities enjoyable and motivating for users. Connected fitness communities: virtual fitness communities within the metaverse enable individuals to connect, exercise together and support each other's fitness goals, fostering a sense of community and accountability. Convenient access: the metaverse allows individuals to access health, fitness and wellness programmes from the comfort of their own homes, eliminating geographical and time constraints.	Technical requirements: participation in metaverse-based health and fitness programmes requires access to compatible hardware and stable internet connections, which may limit accessibility for some individuals. Accurate tracking and reliable data collection are required for effective implementation and related systems need to be validated. Lack of physical interaction: virtual fitness experiences may not fully replicate the benefits of physical group activities or personal trainer interactions, which can provide tailored guidance and real-time feedback. Potential health risks: prolonged use of virtual reality devices may pose health risks such as motion sickness, eye strain, physical exertion or postural discomfort if not used appropriately.	Motivating and personalised experiences: the metaverse offers opportunities to create personalised fitness programmes that adapt to individual goals and preferences, enhancing motivation and adherence. Global accessibility: virtual fitness programmes within the metaverse can reach a global audience, providing access to health and wellness resources for individuals in underserved areas or those with limited mobility. Mental well-being: virtual wellness retreats and mindfulness applications in the metaverse enable relaxation, stress reduction and improved mental health, addressing the increasing need for digital self-care solutions.	Privacy and security: user data and personal information shared within the metaverse for health and fitness purposes need to be protected to ensure privacy and prevent unauthorised access. Mental health implications: virtual fitness experiences in the metaverse may perpetuate unrealistic body standards, potentially leading to body image issues or unhealthy behaviour among users. Prolonged metaverse engagement could affect issues of addiction, isolation and disconnection. Dependency on technology: relying heavily on metaverse-based fitness programmes may reduce individuals' inclination to engage in physical activities outside the virtual realm and opportunities to engage with nature, impacting overall physical fitness levels.

Education and learning

The metaverse has the potential to revolutionise education and learning experiences. Virtual classrooms and immersive simulations enable interactive and experiential learning, engaging students in ways that traditional methods cannot. Virtual museums and historical reconstructions transport learners to different time periods, enhancing their understanding and appreciation of cultural heritage. Collaborative virtual spaces facilitate global collaboration among students and researchers, fostering cross-cultural understanding and knowledge exchange. The education industry can harness the metaverse to transform teaching and learning. Collaboration among educators, technology developers and policy makers is vital to create inclusive, engaging and effective educational experiences in the metaverse.

Education and learning in the metaverse: SWOT analysis			
Strengths	**Weaknesses**	**Opportunities**	**Threats**
Interactive and experiential learning: the metaverse provides opportunities for interactive and experiential learning through virtual classrooms and immersive simulations, enabling students to engage with educational content in a dynamic and practical manner. Access to a range of learning resources: virtual museums and historical reconstructions within the metaverse offer access to a wide range of educational resources, promoting a deeper understanding of	Technology dependence: effective utilisation of the metaverse for education requires access to appropriate technology, including VR and AR devices, which may present barriers for some educational institutions and learners. Learning curve for educators: integrating metaverse technologies into educational settings may require educators to acquire new skills and adapt their teaching methodologies, which can involve a steep learning curve	Enhanced engagement and retention: the immersive and interactive nature of the metaverse can enhance student engagement and improve information retention compared to traditional teaching methods. Personalised and adaptive learning: the metaverse can support personalised and adaptive learning experiences, tailoring educational content and activities to individual	Equality and accessibility: the adoption of metaverse technologies in education should consider issues of equality and accessibility, ensuring that all students have equal access to resources and opportunities. Quality and reliability of content: with the proliferation of educational content in the metaverse, ensuring the quality, accuracy and reliability of information becomes crucial, requiring effective content curation and verification mechanisms and ongoing evaluation and improvement. Distraction and over-reliance on technology: balancing the use of metaverse

Education and learning in the metaverse: SWOT analysis			
Strengths	**Weaknesses**	**Opportunities**	**Threats**
cultural heritage and historical events. Global collaboration and knowledge exchange: collaborative virtual spaces in the metaverse facilitate global collaboration among students and researchers, breaking down geographical barriers and fostering cross-cultural understanding and knowledge exchange.	and potential resistance to change. Limited human and physical interaction: virtual learning environments lack the physical presence and interpersonal interactions found in traditional classrooms, which can impact certain aspects of the learning experience. Limited access to educational services: if learning environments move into the metaverse, learners who are unable to access metaverse environments would be excluded from these opportunities.	student needs and preferences. Expanded access to education: virtual learning environments in the metaverse can extend educational opportunities to individuals who face geographical, financial or other barriers to traditional education.	technologies with other forms of learning, as well as addressing potential distractions and over-reliance on technology, is essential for maintaining a well-rounded educational experience. Privacy and security: user data shared within the metaverse for education purposes needs to be protected to ensure privacy and prevent unauthorised access. The companies running the metaverse technologies will also have access to unprecedented amounts of data about users. Mental health: virtual educational experiences could affect self-image and perceptions of self, particularly for children with vulnerabilities (physical disabilities, learning disorders and difficulties). Prolonged metaverse engagement could affect issues of addiction, isolation and disconnection.

Social and cultural engagement

The metaverse facilitates new forms of social and cultural engagement, transcending physical boundaries. Virtual social platforms enable individuals to connect, interact and collaborate with people from diverse backgrounds and cultures. Virtual art galleries and exhibitions showcase the works of artists worldwide, providing new spaces for artistic expression. The metaverse also offers opportunities for preserving and sharing cultural heritage, allowing individuals to explore and experience historical sites and artefacts in immersive virtual environments. The social and cultural engagement industry can maximise the potential of the metaverse to increase global connections, artistic expression and cultural preservation while addressing the risks and challenges associated with privacy, authenticity and accessibility. Collaboration and accountability among stakeholders, including platform developers, artists, cultural organisations and policy makers, is crucial to ensure the responsible and inclusive development of social and cultural engagement in the metaverse.

Social and cultural engagement in the metaverse: SWOT analysis			
Strengths	**Weaknesses**	**Opportunities**	**Threats**
Global connectivity and collaboration: the metaverse enables individuals from diverse backgrounds and cultures to connect, interact and collaborate on virtual social platforms, fostering cross-cultural understanding and global collaboration. Inclusive artistic expression: virtual art galleries and exhibitions in the metaverse provide an inclusive and accessible space for artists worldwide to showcase their work, reaching audiences beyond physical limitations.	Potential for digital divide: access to the metaverse and its social and cultural engagement opportunities may be limited by factors such as internet access, availability of compatible devices and technological literacy, creating a digital divide. Loss of physical interaction: virtual social and cultural engagement in the metaverse may not fully replicate the richness of physical interactions, such	Cross-cultural exchange: the metaverse connects individuals from different backgrounds, fostering mutual understanding, appreciation and collaboration. Amplification of artistic reach: virtual art galleries and exhibitions expand the reach and visibility of artists, allowing them to showcase their work to a global audience, potentially leading to new opportunities and recognition. Virtual tourism and cultural exploration:	Privacy and security concerns: personal data and interactions may be vulnerable to unauthorised access or misuse. Authenticity and trust: ensuring the authenticity and trustworthiness of virtual social and cultural experiences becomes essential to maintaining credibility and preventing the spread of misinformation. Fragmentation and exclusivity: the proliferation of different metaverse platforms and virtual communities may lead to fragmentation and exclusivity, potentially

Social and cultural engagement in the metaverse: SWOT analysis			
Strengths	**Weaknesses**	**Opportunities**	**Threats**
Preservation of cultural heritage: the metaverse offers opportunities for the preservation and sharing of cultural heritage through immersive virtual environments, allowing individuals to explore and experience historical sites and artefacts.	as face-to-face conversations or the tangible experience of visiting a physical art gallery.	immersive virtual environments in the metaverse provide opportunities for individuals to virtually explore and experience diverse cultures, historical sites and artefacts, promoting cultural understanding and appreciation.	creating digital echo chambers or limiting access to specific groups or demographics. Cultural appropriation and representation: to mitigate this, cultural sensitivity and inclusivity in the design and implementation of virtual social and cultural experiences are needed.

Addressing these weaknesses and threats will be crucial for the successful and responsible development of the metaverse in the sectors outlined above, ensuring user safety, privacy, ethical standards and equal access while maximising the transformative potential of these technologies.

Metaverse use cases	
Sector	**Use cases**
Manufacturing	BMW pilot plant in Munich; Renault Group's industrial metaverse; Anheuser-Busch InBev for breweries and supply chain models (using Azure Digital Twins)
Government	Barbados with their metaverse embassies Dubai with its RegLab on Sand (VARA) Santa Monica, USA Seoul, Republic of Korea
Health	Surgery (separation of conjoined twins in Brazil) Surgical consultation – Proximie Telehealth and telemedicine Pharmaceutical discovery Hostile Environment Surgical Training Peloton

Metaverse use cases	
Sector	**Use cases**
Education	PrismVR (used in schools in the USA, Romania, Singapore and China) Labster's Virtual Labs Metaversities (built by Meta and Victory XR) Japan's N and S high schools
Training	Nokia Learning Space Bosch maintenance Accenture Nth Floor US Army synthetic training environment JetBlue, BMW and Honeywell for training their technicians
Engineering	Volkswagen for Nivus production and prototyping Nvidia Omniverse and digital twins
Architecture	Architect for the metaverse: Decentraland Architects Architects who use the metaverse
Business/work	Microsoft Mesh Apple Vision Pro
Gaming (and engines)	Microsoft: owns Minecraft, Activision Blizzard, ZeniMax Media, among others Epic Games (co-owned by Tim Sweeney and Tencent): developed Unreal Engine, Sky Mavis, Nvidia
Entertainment (movies, music, books, events)	Pokémon Go; Fortnite; Arianne Grande RIFT concerts; Dubai Expo 2020; NBA's NET's Netaverse
Retail	Gucci (on Roblox); Hyundai Mobility Adventure; Nikeland (on Roblox)
Art	NFTs (non-fungible tokens) like Hugo Fournier's Blueberry House or Krista Kim's Mars House
Real estate	Decentraland (JP Morgan) and SAND (HSBC), Voxel Architects (who built the headquarters of Sotheby's and Consensys in the metaverse) in partnership with ONE Sotheby's created a nine-bedroom Meta Residence in SANDBOX in virtual Miami
Travel	Thomas Cook's Virtual Reality Holiday "Try before you Fly"; Virtual Tours with Ariva Digital concept idea
Socialisation	Wunderman Thompson's Inspiration Beach
Defence	DARPA R&D; US Air Force briefing
Finance	Walmart

These application areas represent just a glimpse of the possibilities that lie ahead. The transformative nature of the metaverse in entertainment, medicine, health, fitness and wellness, education and learning, and social and cultural engagement opens doors to innovative solutions, improved experiences and enhanced health for individuals and societies. It is essential for policy makers, industry experts and stakeholders to collaborate and navigate the opportunities and mitigate the challenges that arise, ensuring that the metaverse is harnessed responsibly and inclusively across these diverse application areas.

Appendix II

Human rights and digital rights protection frameworks and definitions (international and European)

Existing human rights frameworks

There are established, stable and essential regulations, protocols and frameworks that already exist for the governance of human rights that are affected by the metaverse. The focus of this report is the perspective of the Council of Europe but other frameworks are provided for illustration purposes and are not exhaustive. These include the following (they are not exhaustive and further frameworks and tools can be found in the references).

Council of Europe level

- The European Convention on Human Rights contains relevant provisions on the human rights to:
  1. conscience (freedom of thought, conscience and religion, Article 9);
  2. expression ("freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers", Article 10);
  3. life (Guide on Article 2 of the European Convention of Human Rights – Right to life);
  4. property (Protocol No. 1, Article 1). Building on this is a complex web of national and international legislation addressing digital safety.
- **European Social Charter**

  Guarantees fundamental social and economic rights as a counterpart to the European Convention on Human Rights, which refers to civil and political rights. It guarantees a broad range of everyday human rights related to employment, housing, health, education, social protection and welfare. The Charter puts specific emphasis on the protection of vulnerable persons such as elderly people, children, people with disabilities and migrants. It requires that enjoyment of the above-mentioned rights be guaranteed without discrimination. No other legal instrument at pan-European level can provide such an extensive and complete protection of social rights as that provided by the Charter, which also serves as a point of reference in European Union law; most of the social rights in the EU Charter of Fundamental Rights are based on the relevant articles of the Charter. The Charter is therefore seen as the "social constitution of Europe" and represents an essential component of the continent's human rights architecture. It includes provisions related to the right to health and social security; the protection of the family and children; and fair working conditions (fair remuneration, freedom of association, access to vocational training, etc.).

- **Convention on Cybercrime (ETS No. 185): The Budapest Convention**

  An example of how the Council of Europe has been timely in responding to the evolution of cybercrime, taking into consideration the growing importance of digital evidence in traditional crime. Also, the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189) entails an extension of the Cybercrime Convention's scope, including its substantive, procedural and international co-operation provisions, to also cover offences of racist or xenophobic propaganda. Importantly, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224) – opened for signature in May 2022 – provides a legal basis for direct co-operation with service providers for subscriber information and a number of other tools for obtaining e-evidence across borders.

- **Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201, Lanzarote Convention)**

  This convention applies to all forms of sexual exploitation and abuse: offline, facilitated by ICT or that takes place entirely online (including in metaverse technologies). The substantive criminal law provisions will be applicable to metaverse technologies, especially as regards solicitation/grooming, child pornography/child sex abuse material, coercion and extortion, causing a child to view pornographic material, etc. There may also be implications for rules governing avatars and depictions of a child's sexual organs (e.g. if it is possible to undress the avatar of a child or not).

- **Data Protection Convention**

- **Istanbul Convention**

  Provides a legal basis for prohibiting digital violence against women, including algorithmic stereotyping and online violence such as cyberharassment, bullying and online sexist hate speech. Article 17 of the Istanbul Convention encourages states parties to involve media companies and the ICT sector in measures to prevent and combat violence against women. GREVIO's General Recommendation No.1 on the Digital Dimension of Violence against Women developed more details for ICT companies.

- **Framework Convention for the Protection of National Minorities**

  Provides a legal basis for combating algorithmic discrimination on grounds of national minority status as well as online violence such as hate speech.

- **CDADI (Steering Committee on Anti-Discrimination, Diversity and Inclusion) GEC (Gender Equality Commission) study on artificial intelligence systems (Autumn 2023)**

- Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), **Guidelines on artificial intelligence and data protection (2019)**
- Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), **Guidelines on facial recognition (2021)**
- "Convention 108", modernised in 2018 by an amending protocol ("**Convention 108+**"), establishes international standards that guarantee individuals the right to privacy and the protection of personal data, regardless of technological developments.
- **Declaration on Internet Governance Principles**

  These include: 1) human rights, democracy and the rule of law; 2) multistakeholder governance; 3) responsibilities of states; 4) empowerment of internet users; 5) universality of the internet; 6) integrity of the internet; 7) decentralised management; 8) architectural principles; 9) open network; 10) cultural and linguistic diversity.
- **European Charter for Regional or Minority Languages**

  Article 7(2) of the charter:
  "The Parties undertake to eliminate, if they have not yet done so, any unjustified distinction, exclusion, restriction or preference relating to the use of a regional or minority language and intended to discourage or endanger the maintenance or development of it". In principle, this provision extends to the algorithmic and online realms, where it can be relied on to address digital discrimination in its many forms.
- **Draft recommendation on online addiction(s)**
- **Guidance Note on Content Moderation** Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation (adopted by the Steering Committee for Media and Information Society (CDMSI)) (2021).
- Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems
- Recommendation CM/Rec(2022)13 of the Committee of Ministers to member States on the impacts of digital technologies on freedom of expression
- Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries
- Content Moderation – Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation
- Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech
- Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom
- Recommendation CM/Rec(2014)6 and explanatory memorandum of the Committee of Ministers to member States on a Guide to human rights for Internet users
- Strategy for the Rights of the Child (2022-2027)

European Union level

- **European Declaration on Digital Rights and Principles for the Digital Decade**

  According to the declaration, "Technology should serve and benefit all people living in the EU and empower them to pursue their aspirations. It should not infringe upon their security or fundamental rights. Signatories of the declaration will commit to making sure that the digital transformation benefits everyone and improves the lives of all people living in the EU. They will take measures to ensure our rights are respected online as well as offline. The EU will promote this approach both at home and on the international stage". The principles are shaped around six themes: 1) Putting people and their rights at the centre of the digital transformation; 2) Supporting solidarity and inclusion; 3) Ensuring freedom of choice online; 4) Fostering participation in the digital public space; 5) Increasing safety, security and empowerment of individuals; 6) Promoting the sustainability of the digital future.

- **Digital Markets Act (DMA)**

  This is a tool for the European Commission to overcome the limits of the traditional instruments in the digital environment. It aims to regulate gatekeeper online platforms. Content or providers found in the metaverse may fall into the category of central platform services, which would be within scope of the DMA. The DMA intends to lower entry barriers, prevent self-preferencing and rebalancing user relationships (such as free access to data). An operator of a metaverse may thus be prevented from favouring its own sales and services to the detriment of others.

- **Digital Services Act (DSA)**

  Digital services include a large category of online services, from simple websites to internet infrastructure services and online platforms, and mainly concern online intermediaries and platforms, such as online marketplaces, social networks, content-sharing platforms, app stores and online travel platforms. The act partly addresses malicious content and deceptive designs.

- **AI Act**

  The AI Act is a proposed European law on artificial intelligence (AI). The law assigns applications of AI to three risk categories: 1) applications and systems that create an unacceptable risk, such as government-run social scoring; 2) high-risk applications, such as a CV-scanning tool that ranks job applicants; and 3) applications not explicitly banned or listed as high risk are largely left unregulated.

- **General Data Protection Regulation (GDPR)**

  The GDPR is considered the strongest privacy and security law in the world. Though it was drafted and passed by the European Union, it imposes obligations on organisations everywhere, so long as they target or collect data from people in the EU. The regulation came into effect on 25 May 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.

- **European Privacy and Electronic Communications Regulations**

  These are derived from European law and implement European Directive 2002/58/EC, also known as "the e-privacy Directive."

United Nations level

- **UN International Covenant on Civil and Political Rights**

  An international treaty that guarantees civil and political rights, including the right to a fair trial, freedom of expression and freedom of assembly. A total of 173 nations, including the United States of America, are parties. Article 19(1) of the International Covenant on Civil and Political Rights (ICCPR) states that "Everyone shall have the right to hold opinions without interference". As the UN's special rapporteur for freedom of expression and opinion noted some years ago, there has however been "limited interpretation around this right because the authors of Article 19 likely believed the right to hold an opinion is indisputable – governments can't access what's in our minds". It also contains an article relating to freedom of expression.

- **United Nations Convention against Corruption**

  A global anti-corruption treaty that promotes the rule of law, transparency and accountability in both public and private sectors.

- **United Nations Convention on the Rights of the Child**

  The obligation to take account of the best interests of the child in all activities that have an impact on children can be found in Article 3(1) of the UN Convention on the Rights of the Child. Relevant children's rights can be: the right to freedom of information, the right to access to (non-harmful) media, the right to free forming of opinion and thought, the right to freedom of association, the right to privacy and data protection, the right to identity forming, play and relaxation and the right to protection from violence (including bullying and sexual abuse) and from economic exploitation. There is also the optional protocol on the sale of children, child prostitution and child pornography. See also General Comment No. 25 on children's rights in relation to the digital environment.

- **United Nations Sustainable Development Goal #3**

  Ensure healthy lives and promote well-being for all at all ages.

- **United Nations Universal Declaration of Human Rights**

  Adopted by the United Nations General Assembly, it sets out the fundamental human rights and principles that underpin the rule of law.

International

Organisation for Economic Co-operation and Development (OECD)

- OECD Enhanced Access to Publicly Funded Data for Science, Technology and Innovation
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Principles

- **Alliance for Universal Digital Rights (AUDRI)**

  AUDRI focuses predominantly on the impact that the digital environment has on women and children (particularly girls) and people from other groups that experience discrimination, marginalisation, violence and oppression. The AUDRI principles are: i) Universal and equal rights, including in the digital realm; ii) Personal safety and data privacy: everyone has a right to control information about themselves and to secure protection from digital harms; iii) Digital self-determination: everyone has a right to exercise self-determination in the use of digital technologies; iv) Digital access for all: everyone has a right to access the digital realm and to be free to participate in digital life; v) Freedom of expression and association: everyone has a right to freedom of expression, peaceful assembly and association online; vi) Secure stable and resilient networks: everyone has a right to benefit from secure, stable and resilient digital networks and technologies; vii) Linguistic and cultural diversity: everyone has a right to use any language of their choice to create and share digital information; viii) Universal standards and regulation: everyone has an equal right to benefit from the development and use of digital technology; ix) Good digital governance: everyone has the right to multilateral, democratic oversight of the internet and digital technologies.

National level

- **UK – Age Appropriate Design Code**

  The United Kingdom's Age Appropriate Design Code (AADC) came into force in 2021 to help organisations design services that comply with the GDPR and the European Privacy and Electronic Communications Regulations and to take a proportionate and risk-based approach to protecting children as well as other vulnerable groups. This code is grounded in the UN Convention on the Rights of the Child and its General comment No. 25 (2021) on children's rights in relation to the digital environment.

- **Germany – Patient Data Protection Act or Patientendaten-Schutz-Gesetz (PDSG)**

- **Netherlands – Dutch Code for Children's Rights**

  In March 2021, the Dutch Ministry of the Interior and Kingdom Relations published the Code for Children's Rights to help designers focus on the rights of children in the development of digital products, with regard to the UNCRC and GDPR.

Appendix III

Selection of issues and some considerations shared by the contributors

Issue: ways that data are collected	
What creates or contributes to the issue?	The hardware and software involved, with many layers of sensing, collection, applications; consent mechanisms are complicated, not always obvious and not always updated. Awareness of the user and agency will become more complicated with new sensing users are not aware of, difficulty to verify and enforce what data are collected, for what purpose it is used and who has access to or owns the data. Some metaverse platforms may rely upon a large existing user base and a business model that trades on an economy of data and attention where users are incentivised to spend more time online and share more data. This drives companies to strive for market monopoly and network effects to grow their user base.
What stakeholders are currently doing	Some consent mechanisms in place. Some indications of when data are being collected.
Prevention and mitigation options (expert contributions)	Promote the development and adoption of privacy-preserving identity solutions that enable cross-verse identity verification without compromising user privacy and security. Emphasise the importance of user consent and control over their identity-related data. This may require new initiatives like the right to be forgotten (similar to the GDPR), recognised by case law as an integral part of the right to protection of private life – see Guide on Article 10, the right to disconnect or the right to disclosure (if dealing with an AI agent). Consider data anonymisation and use of synthetic data where appropriate. Even if in-depth information can be pinned to a user ID (whether such an ID contains personally identifiable information or not), the attributes collected could be treated as sensitive or biometric information due to the unique circumstances under which it is collected.

Issue: ways that data are collected	
Prevention and mitigation options (expert contributions)	Develop appropriate frameworks for the collection of data in the metaverse. These guidelines should promote transparent data collection practices, informed consent, data anonymisation and robust cybersecurity measures. Consent mechanisms need to be simple enough for users to participate meaningfully. Platforms should regularly update consent forms. If there is no assumption of permanent licensing and for each new data type, these mechanisms must be kept up to date. Companies make money from the collection of advertising revenue, focusing on advertising positioning based on user data. By compensating users for managing their information, companies can avoid some privacy issues in the metaverse. For example, privacy-conscious browsers can default to disabling cookies and if users are willing to watch advertisements, they can receive rewards or vouchers as a result. There may be situations where companies must choose between data privacy and user convenience or ease of use, considering of course their obligations by law. Ideally, for the benefit of users, companies should update their consent at every point of data re-input, even if it means additional authentication layers. There should be training and awareness raising of policy makers, legislators and consumers; standards to support the implementation of and compliance with the law; principles safeguarding users’ and bystanders’ privacy. Collection of bystanders’ data should by default be excluded. Companies should commit to invest in cybersecurity and insider-threat safeguards. Awareness. Enforce some compliance with transparency. Work with tech companies for early identification of issues and their mitigation. Ensure an ethical data redundancy plan if companies become bankrupt. Ensure data privacy rights for mergers and acquisitions. Ensure that the scrapping of public data and open-source data is also subject to standards.

Issue: ways that data are collected	
Examples of relevant existing frameworks (non-exhaustive)	The Council of Europe's Data Protection Convention GDPR The Fair Information Practice Principle (USA) Enhanced Access to Publicly Funded Data for Science, Technology and Innovation (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD) California Privacy Act (USA) Health Insurance Portability and Accounting Act (HIPPA; USA) Patient Data Protection Act or Patientendaten-Schutz-Gesetz (PDSG) (Germany)
Related discussions	GDPR for data collection and what this will mean. Already data collection and privacy are issues with AI (even more so generative AI), on social platforms and in the Web 2.0 era.
Level of complexity for enforcement in the metaverse	Higher, because of the scale of deployment, low transparency and awareness of rights and their enforceability. The current fragmented approach is leading to legal complexity and challenges in enforcement, while enforcement needs to be cross-border/global.
Human rights considerations	As gene and biometric data become more intrusive, and as AI competes with humans, there may also be a need to have the right to be human (work and live without technology intrusion).

Issue: data privacy and security	
Factors that create or contribute to the issue	The ways in which data are used are not always explained to users. Users are not always informed when they are interacting with AI.
Mitigation options (expert contributions)	Develop appropriate frameworks for the use of data in the metaverse. These guidelines should promote transparent data usage practices, informed consent, data anonymisation and robust cybersecurity measures. Individuals should have agency and control over their personal information and be empowered to make informed decisions regarding its usage within the metaverse.

Issue: data privacy and security	
Mitigation options (expert contributions)	Metaverse platforms should comply with all applicable data privacy and security laws and regulations. This includes laws and regulations in the countries where users are located. Metaverse platforms should educate users about data privacy and security risks. This education should include information about how to protect their personal information and how to report data breaches. Metaverse platforms should develop their own self-regulatory frameworks for data privacy and security. These frameworks should be based on the principles of transparency, consent, anonymisation and cybersecurity. The digital human model developed by artificial intelligence developers is based on humans willing to share their biometric data, so developers must clearly state the rights and consent rules that govern these transactions. The metaverse contains a large amount of user data, so the platform must remain impeccable. Developers must keep vulnerabilities to an absolute minimum and adopt secure coding principles. In the long run, data breaches and accidental leakage may make enterprises pay a high price. Companies can avoid risks through regular testing and upgrades. Due to the complete transparency of the right to know, artificial intelligence robots (digital humans) must carry labels so that users always know how they share data.
Examples of relevant existing frameworks (non-exhaustive)	Council of Europe "Convention 108" AUDRI GDPR UK Age Appropriate Design Code (AADC)
Do these issues exist for other emerging technologies?	Yes – data privacy is an issue with AI (even more so generative AI), on social platforms and in the Web 2.0 era.
Enforcement in the metaverse	Enforcement complexity is increased, because of the biometrics involved and the potential impact on mental autonomy. Data protection and privacy laws are not consistent around the world. For example, the EU's GDPR has specific rules for European Union citizenship. At the same time, the metaverse may become an independent field, which generally operates independently and requires strict self-regulation.
Are new human rights needed?	Non-negligible potential for access to the internal mental states of individuals.

Issue: privacy for children	
What creates or contributes to the issue?	Data collection (including geolocation); data usage (mining; extraction). No or limited safeguards for age-appropriate content exposure.
Prevention and mitigation (expert contributions)	Promote digital literacy and privacy education initiatives targeted at children, parents and educators to raise awareness about privacy risks and responsible online behaviour. Implement mechanisms to verify users' age and obtain parental consent before granting access to certain areas or features in the metaverse. Provide robust privacy settings and controls that empower parents and children to manage shared information, restrict access to personal data and limit interactions with others. Ensure strict content moderation to prevent the dissemination of inappropriate or harmful content that could compromise children's privacy and well-being. Age-appropriate realism: tailor metaverse experiences to age-appropriate levels of realism and emotional engagement to minimise potential negative effects on vulnerable users, particularly children. For protection to be consistent (and the ethical profile maintained) across the life cycle of a technology's use, the adherence to the AADC should be monitored and audited to ensure consistency and to truly provide safeguards for children.
Examples of existing frameworks (non-exhaustive)	Council of Europe Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment Guidelines for Children's Data Protection in an Education Setting Report on Children with Disabilities in the Digital Environment European Convention on Human Rights. The right to respect for private and family life under the European Convention on Human Rights has been interpreted as protecting "the right to personal development, whether in terms of personality or of personal autonomy". It also includes "the right for each individual to approach others in order to establish and develop relationships with them and with the outside world, that is, the right to a 'private social life'".

Issue: privacy for children	
Examples of existing frameworks (non-exhaustive)	EC BIK+. European Strategy for a Better Internet for Children (May 2022). The EU will continue to address children's digital protection, privacy and participation needs. UN Convention on the Rights of the Child. The obligation to take account of the best interests of the child in all activities that have an impact on children can be found in Article 3(1) of the UN Convention on the Rights of the Child. Relevant children's rights include the right to privacy and data protection. UN General comment No. 25 on children's rights in relation to the digital environment. General comment No. 25 calls on states parties to "require all businesses that affect children's rights in relation to the digital environment to implement regulatory frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services" (paragraph 39); as well as to "require the business sector to undertake child rights due diligence, in particular, to carry out child rights impact assessments and disclose them to the public" (paragraph 38). UN General comment No. 25 warns against the misuse of children's data, including for commercial exploitation (paragraph 103). It specifies that "any digital surveillance of children, together with any associated automated processing of personal data, should respect the child's right to privacy and should not be conducted routinely, indiscriminately or without the child's knowledge … and consideration should always be given to the least privacy-intrusive means available to fulfil the desired purpose" (paragraph 75). The general comment also prioritises data protection and privacy-by-design to ensure that commercial interests do not take precedence over the best interests of the child. GDPR. The General Data Protection Regulation seeks, among other things, to contribute to the "well-being of natural persons" (recital 2). However, the interests of the child are most clearly expressed in recital 38, which states that children enjoy specific protection in the light of their fundamental right to data protection. DSA. The Digital Services Act aims to update the regulatory framework for digital services in the European Union. While the DSA does not specifically focus on privacy for children, it includes provisions that can indirectly impact children's

Issue: privacy for children	
Examples of existing frameworks (non-exhaustive)	privacy in the digital space. It obliges all online platforms (defined as anything with a user-to-user function) to "put in place appropriate and proportionate measures to ensure a high level of privacy, safety and security of minors, on their service" (Article 28) – a provision to be underpinned by the development of standards. Platforms are also prohibited from showing ads to children based on profiling or using "dark patterns" to influence user choices. Dutch Code for Children's Rights. Threaded throughout the code are indicative examples of compliance and good practice, including ensuring the legitimate processing of personal data of children, carrying out a privacy impact assessment based on children's rights, providing a child-friendly privacy design and preventing the profiling of children. UK Age Appropriate Design Code (AADC)
Related discussions	In the AI context, the current AI Act draft does not explicitly recognise children's vulnerabilities, despite its commitment to a human-centric and ethical development of AI based on EU values and the public interests of health, safety and fundamental rights, including those set out in the UN Convention on the Rights of the Child and its General Comment 25.
Enforcement in the metaverse	The complexity of privacy protection for children increases in the metaverse. Some of the specific challenges to privacy protection for children in the metaverse include the following. The use of avatars: children can create avatars that represent them in the metaverse. These avatars can be used to collect personal data about children, such as their age, gender and interests. The use of tracking technologies: metaverse platforms often use tracking technologies to collect data about users, including children. These data can be used to track children's movements in the metaverse, their interactions with other users and the content they view. Pervasive data collection: in the metaverse, children interact with a wide range of platforms, virtual worlds and social spaces. These environments often collect extensive data on user behaviour, interactions and preferences, which can be challenging to monitor and regulate effectively. Many metaverse platforms integrate with third-party services, which can lead to data sharing and additional privacy risks, especially if the third parties have different privacy practices.

Issue: privacy for children	
Enforcement in the metaverse	Limited parental oversight: unlike some traditional online platforms where parents may have more control over their children's activities, the metaverse can be vast and decentralised, making it harder for parents to supervise and protect their children effectively. Difficulties in age verification: it can be challenging to verify the age of users in the metaverse accurately. Children might misrepresent their age to access platforms that have age restrictions, making it harder to apply age-appropriate privacy protections.
The role of technical standards	Technical standards can play a significant role in filling the gaps and addressing some of the complexities in privacy protection for children in the metaverse. These standards can provide a framework for developers, platform operators and policy makers to ensure that privacy considerations are adequately addressed in the design and operation of metaverse platforms and virtual environments. Some instances include the following. Consistency and interoperability: Technical standards help establish consistent practices and interoperability among different metaverse platforms. When privacy protection measures are standardised, it becomes easier for users, including children, to understand and manage their privacy settings across various virtual spaces. Best practices and guidelines: standards can offer best practices and guidelines for developers to implement privacy features that align with industry norms and legal requirements. This ensures that privacy protection becomes an integral part of the design process. Age verification and parental consent mechanisms: technical standards can provide guidance on robust age-verification methods to prevent underage users from accessing age-restricted content or platforms. They can also outline effective parental consent mechanisms, enabling parents to control their children's participation and data sharing. Data collection and use limitations: standards can define acceptable data collection and usage practices, including restrictions on gathering sensitive information from children. These standards can help mitigate potential privacy risks and ensure that data are used responsibly.

Issue: privacy for children	
Further possible actions (expert contributors)	Support the promulgation of the Age Appropriate Design Code.
Further rights considerations	Children's rights must be asserted within the broader context of human rights, addressing the challenges and tensions of these rights being translated into the digital world. The protection of children's privacy in the metaverse raises unique challenges, and while new human rights may not be needed, a nuanced and targeted approach to existing human rights frameworks is essential. Children's privacy in the metaverse can be addressed within the existing framework of established human rights, with a focus on adaptation, clarification and specific application.

Issue: free expression	
Aspects creating or contributing to the issues	Content moderation algorithms. Automated content moderation algorithms may lack the nuance to distinguish between legitimate expression and harmful content. Overly aggressive algorithms might censor lawful speech, leading to an unintentional suppression of freedom of expression. Filter bubbles and echo chambers. Personalisation algorithms in the metaverse can create filter bubbles and echo chambers, where users are exposed only to content that aligns with their existing beliefs and opinions. This can limit exposure to diverse viewpoints, inhibiting open discourse. Immersive social interactions. Avatars used in the metaverse's immersive social interactions can impact users' perceived trustworthiness of the source. Misinformation propagated by persuasive avatars may lead to a higher acceptance rate, as users feel a stronger connection and pressure to conform to the beliefs expressed by these digital personas. Geographical restrictions. Metaverse platforms may implement geolocation-based restrictions that limit access to content based on users' physical location, potentially curbing certain viewpoints or expressions in specific regions. Centralised control. Platforms with centralised authority may enforce rules and guidelines that restrict freedom of expression, leading to censorship and limiting diverse opinions.

Issue: free expression	
Aspects creating or contributing to the issues	Some features of metaverse technologies are designed to leverage emotion. Avatar activities and appearances could be used for deceptive purposes.
Prevention or mitigation options (contributors' suggestions)	Put into place tools to identify and address false, misleading or manipulative behaviours, especially those intended to limit or alter free expression.
Examples of related existing frameworks (non-exhaustive)	European Convention on Human Rights ► Conscience (freedom of thought, conscience and religion, Article 9) ► Expression ("freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers", Article 10) ► Property (Protocol No. 1, Article 1) Council of Europe ► Guidance Note on Content Moderation: Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation ► Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech ► Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries The EU Digital Services Act (DSA) in part addresses malicious content and deceptive designs. User accountability and virtual identity regulation: in line with the proposals of the EU Digital Services Act (European Commission 2022), users must be held legally accountable for illegal content that they generate. This accountability can be achieved through ensuring that virtual identities link to real-world identities. While this may present concerns around privacy, this authentication need not be managed by a platform or commercial interest, but instead by an independent regulatory body such as Ofcom (or its EU counterpart). Further, the use of an independent body will enable greater co-ordination across platforms/metaverses.

Issue: free expression	
Examples of related existing frameworks (non-exhaustive)	EU AI Act. International Covenant on Civil and Political Rights (ICCPR) (to which 173 nations, including the United States of America, are parties). Article 19(1) states "Everyone shall have the right to hold opinions without interference". As the UN's special rapporteur for freedom of expression and opinion noted some years ago, there has however been "limited interpretation around this right because the authors of Article 19 likely believed the right to hold an opinion is indisputable – governments can't access what's in our minds". As AR develops, however, this assumption may become less certain.
Related discussions	Artificial Intelligence (AI) and automated systems: AI-powered content moderation and recommendation systems may inadvertently suppress freedom of expression by over-policing or under-policing content. The lack of transparency in AI decision making can lead to concerns about bias and censorship. Brain–computer interfaces (BCIs): BCIs can raise ethical questions about the privacy and security of users' brain data, potentially affecting their willingness to express themselves in ways that interact with these interfaces. Quantum computing: as quantum computing advances, concerns about its potential to break conventional encryption could impact individuals' freedom to communicate securely.
The role of technical standards	Content moderation guidelines: technical standards can establish common content moderation guidelines and criteria for the metaverse. These guidelines can help platform operators create consistent and transparent policies for handling different types of content, including distinguishing between freedom of expression and harmful content. Contextual analysis: standards can incorporate methodologies for context-aware content analysis. This helps in understanding the nuances of expressions within the metaverse environment, considering factors like role-playing, satire and cultural differences. AI and algorithm transparency: standards can promote transparency in the use of AI and algorithms for content moderation. Platforms can be encouraged to disclose how algorithms work and address any potential biases to avoid over-policing or under-policing of content.

Issue: identity in the metaverse	
Factors that create or contribute to the issue	Lack of interoperability among platforms, limiting the ability to use the same identity on multiple platforms. The metaverse offers users the option to maintain multiple identities or engage in anonymous interactions. While this can empower users to explore new experiences without fear of discrimination or judgment, it also raises concerns about potential misuse, such as harassment or malicious behaviour. As users participate in various activities within the metaverse, they generate a wealth of personal information, such as preferences, social connections and transaction histories. Managing and protecting these data is essential to ensure users' privacy rights and prevent unauthorised access or misuse.
Prevention and mitigation options (expert contributions)	Mechanisms should be put into place for users to have control over their metaverse identity, including the ability to manage and authenticate their digital attributes. Implementing user-centric design principles ensures that individuals have autonomy over their digital presence and the ability to protect their privacy. Ensuring that users are who they claim to be is essential for maintaining trust and security in the metaverse. Approaches to identity verification and authentication may include biometrics, digital certificates and multifactor authentication methods that combine multiple layers of security. Establishing reliable methods of authentication and verification is essential to prevent identity fraud and malicious activities within the metaverse. Leveraging emerging technologies like decentralised identifiers (DIDs), digital signatures and zero-knowledge proofs can enhance the trust and security of metaverse identities. Blockchain technology and other decentralised systems can provide secure, private and portable solutions for managing metaverse identities. These technologies can ensure that users have control over their personal information and how it is used, while also promoting interoperability between different metaverse platforms. Establish mechanisms for ongoing monitoring and evaluation of metaverse identity systems. Leverage the technological capabilities of companies and collaborate with financial institutions to expand the range of application scenarios and conduct comprehensive evaluations of the technology's effectiveness in specific contexts.

Issue: identity in the metaverse	
Prevention and mitigation options (expert contributions)	Regular assessments can identify potential risks, emerging issues and areas requiring further attention to ensure the protection of human rights and democratic values. Distributed digital identity technology faces challenges related to the lack of algorithm verification tools, limited performance and capacity. Currently, there is a need for a comprehensive and reliable mechanism for verifying and authenticating distributed digital identity systems. To overcome these obstacles, it is essential to prioritise research and exploration of detection and authentication technologies. Building a scientific, rational and necessary testing and certification system will be instrumental in ensuring the robustness and effectiveness of distributed digital identity solutions. Integrate privacy-enhancing technologies, such as decentralised identity systems and secure data storage, into the core architecture of the metaverse. Privacy should be prioritised from the initial design phase to protect individuals' personal information. Promote awareness among metaverse users about the implications of metaverse identity and the importance of protecting their privacy and digital rights. Provide accessible educational resources to empower individuals to make informed decisions about their metaverse identity.
Examples of relevant frameworks (non-exhaustive)	Council of Europe ▶ CDADI/GEC Study on artificial intelligence systems (Autumn 2023) ▶ Guidelines on Children's Data Protection in an Education Setting ▶ Guide to human rights for internet users ▶ Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment ▶ Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech
Related discussions	Empowering users with control over their digital identities, informed consent and granular privacy settings has been a focus in various technology domains. Applying similar principles to the metaverse can help mitigate concerns regarding data exploitation and unauthorised profiling.

Issue: identity in the metaverse	
Related discussions	Data minimisation: minimising the collection and retention of personal data as much as possible is a principle applicable across platforms. Applying data minimisation practices to the metaverse can reduce the risks associated with data breaches and unauthorised access. Ethical considerations: ethical frameworks for AI and social networks have emphasised the importance of transparency, fairness and accountability. These principles can be extended to the metaverse to ensure that identity-related practices align with ethical standards and promote user well-being.
Enforcement in the metaverse	The metaverse introduces the concept of avatar-based identity, where individuals can embody different personas or avatars. This raises questions about authenticity, accountability and the potential for identity manipulation. Unlike traditional online platforms, the metaverse can create a persistent digital footprint. Actions and interactions within the metaverse can have lasting effects on an individual's reputation and privacy, necessitating careful management of one's digital presence, which requires knowledge and, therefore, appropriate training for children and adults. The metaverse enables interactions across different virtual environments and the physical world. This interplay between virtual and real identities introduces complexities that must be addressed, including issues of jurisdiction, legal frameworks and cross-platform identity verification. Ethical questions surrounding metaverse identity include potential discrimination, harassment and other forms of misconduct in the digital world. It is vital to establish ethical guidelines and design principles that promote inclusivity, respect and safety for all metaverse users.
The role of technical standards	The development of open standards and protocols that allow seamless interaction and transfer of identity across different metaverse platforms is crucial, such as the Decentralised Identifier (DID) standard, and can enable metaverse identities to be seamlessly transferred and recognised across different platforms and applications. This promotes a more cohesive and inclusive metaverse ecosystem, allowing users to easily access different environments and services without losing their digital history or reputation.

Issue: identity in the metaverse	
The role of technical standards	Foster collaboration among technical experts, policy makers, industry stakeholders, civil society and user representatives to develop inclusive and interoperable standards for metaverse identity. This collaboration should prioritise user rights, privacy and security. The development of interoperability standards and protocols is crucial to facilitate cross-verse governance. This includes establishing mechanisms for data exchange, identity validation and communication between different metaverse platforms.
Prevention and mitigation options (expert contributions)	Evaluate existing legal frameworks and identify areas where adaptation or new regulations may be necessary to address metaverse identity issues. This includes considerations of jurisdiction, cross-platform interactions, data anonymisation, data protection, distributed storage of personal identity data and user rights. Provide a framework for responsible identity management practices and encourage platforms to adopt ethical standards. As the metaverse evolves, it may raise new legal challenges and regulatory requirements related to identity management, data protection and intellectual property rights. Policy makers must carefully consider the unique aspects of the metaverse and develop appropriate legal frameworks that balance user rights, innovation and public interest. The metaverse presents unique challenges related to legal jurisdiction and enforcement. Developing legal frameworks and enforcement mechanisms that can accommodate the complexities of the metaverse is essential for creating a safe and responsible digital environment.
Further rights considerations	Right to digital self-determination: this right could encompass the right of individuals to have control over their virtual identities, personal data and how they are represented in the metaverse. Right to anonymity and pseudonymity: preserving individuals' rights to use anonymous or pseudonymous virtual identities in the metaverse, where appropriate and necessary.

Issue: digital inclusion	
What creates or contributes to the issue?	Affordability: the cost of XR headsets, internet connections, paywalls, additional hardware, etc. can be a barrier for many people. Disabilities: some people with disabilities may have difficulty using XR headsets or lack full understanding if there are no subtitles or hearing assistance, etc. Technological literacy: not everyone is comfortable using new technologies (age and gender gaps) and not everyone has the technological skills needed to successfully enter and thrive in metaverse environments because of language barriers, social constraints, etc. Maturity levels and levels of understanding of children should also be considered.
Prevention and mitigation options (expert contributions)	Affordability: metaverse platforms should make their products and services affordable to everyone. This could be done by offering subsidies or discounts to people who cannot afford the necessary hardware or software and minimising recourse to paywalls to access metaverse environments. Disability ► Inclusive design: this is a philosophy for guidelines to be inclusive for disabilities, languages, backgrounds, personal characteristics, status, etc. This can be applied in terms of the metaverse, as well. In the metaverse specifically, customisation and individualisation can help with access. ► Universal design: this is another approach to designing inclusive spaces and states that “the design of products and environments to be usable by all people, to the greatest extent possible, without the need for adaptation or specialised design”. ► Metaverse platforms should design their products and services with accessibility in mind. This could include features such as closed captions, text-to-speech and adjustable controls. ► Metaverse platforms should collaborate with disability organisations and other stakeholders to develop and implement accessibility features. ► Metaverse platforms should invest in research to better understand the needs of people with disabilities.

Issue: digital inclusion	
Prevention and mitigation options (expert contributions)	Technological literacy ▶ Metaverse platforms should provide educational resources and support to help people learn how to safely use their products and services. This could include tutorials, online courses and in-person workshops. ▶ One interesting proposal comes from RespectZone (respectzone.org), suggesting that new avatars should require an onboarding/permitting process, so that users are aware of the most important considerations around using these tools.
Examples of existing relevant frameworks (non-exhaustive)	Council of Europe Recommendation CM/Rec(2020)1 on artificial intelligence and human rights. This recommendation addresses the impact of artificial intelligence (AI) on human rights, including the right to non-discrimination, privacy, freedom of expression and access to information. Ensuring that AI applications are developed and deployed in a way that promotes digital inclusion and does not perpetuate biases or discrimination is emphasised. Recommendation CM/Rec(2020)3 on the human rights impacts of algorithmic systems. This recommendation addresses the human rights implications of algorithmic decision making, which is relevant to digital inclusion as algorithms may impact access to information, services and opportunities. Ensuring transparency, accountability and non-discrimination in algorithmic systems is emphasised. Recommendation CM/Rec(2012)12 on the protection of personal data in the context of electronic communications. This recommendation calls on states to ensure that the processing of personal data in the digital environment is done in a way that respects privacy and that everyone has the right to access digital technologies and services. The Declaration on the Freedom of Expression and Information in the Digital Age (Declaration on Freedom of Expression). The Declaration on Freedom of Expression is a non-binding declaration that sets out principles for the protection of freedom of expression in the digital age. The declaration includes a number of provisions that are relevant to digital inclusion, such as the right of everyone to access the internet and the right to use the internet without discrimination.

Issue: digital inclusion	
Examples of existing relevant frameworks (non-exhaustive)	Recommendation CM/Rec(2022)13 of the Committee of Ministers to member States on the impacts of digital technologies on freedom of expression. Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), Guidelines on facial recognition (2021). Guidance note on content moderation. Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation (adopted by the Steering Committee for Media and Information Society (CDMSI)) (2021). Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), Guidelines on artificial intelligence and data protection (2019).
Related discussions	The issue of digital inclusion is not unique to the metaverse or any specific emerging technology; it is a broader concern that applies to various emerging technologies and digital advancements. ► Internet of Things (IoT): IoT devices and systems can enhance various aspects of life, but access to these technologies can be limited for certain communities, leading to potential exclusion from their benefits. ► Artificial intelligence (AI): the use of AI applications, such as automated decision-making systems, can raise concerns about transparency, fairness and biases that may disproportionately affect marginalised groups. ► Blockchain: while blockchain technology offers various possibilities, barriers to access, technical complexity and lack of understanding may hinder broader adoption and inclusion. ► Augmented reality (AR) and virtual reality (VR): similar to the metaverse, AR and VR technologies can provide immersive experiences, but they may require specific hardware or internet connectivity, limiting access for some individuals. ► Autonomous vehicles: the development of autonomous vehicles may transform transportation, but their widespread adoption may face challenges in areas with limited infrastructure or access to advanced technology.

Issue: digital inclusion	
Related discussions	▶ Renewable energy technologies: access to renewable energy technologies can empower communities, but affordability and infrastructure may affect equitable distribution and inclusion. ▶ Biotechnology and health technologies: advancements in biotechnology and health technologies can benefit public health, but concerns about data privacy and access to healthcare resources can impact digital inclusion. ▶ 5G connectivity: the deployment of 5G networks can enhance internet speed and capacity, but its implementation may be concentrated in urban areas, leading to a digital divide between rural and urban communities.
Enforcement in the metaverse	As inclusiveness in a co-created world with avatars may mean different things to society and will keep evolving, enforcement is expected to be more challenging.
Further considerations	Metaverse platforms should work to develop and adopt standards for accessibility. This will help to ensure that accessibility features are consistent across different platforms.
	▶ Review and clarify accessibility, anti-discrimination and privacy laws for immersive technologies. ▶ Introduce inclusion-oriented AR/VR solutions across government activities. ▶ Establish redress mechanisms. Transparency comes first in order to know what is happening so violations can be identified. ▶ Set expertise in public sectors and judicial systems to understand technology. ▶ Understand who owns the technology. ▶ Set liability aspects for service providers in the metaverse. ▶ Perform risk and impact assessments throughout the life cycle of algorithmic systems according to their specific uses. ▶ Make use of certification mechanisms to ensure that biases have been mitigated and risks of discrimination eliminated as far as possible. ▶ Consider legal obligations to publish statistical data to assess the discriminatory effects of a given system.

Issue: digital inclusion	
	▶ Create mechanisms for transparency with a view to allowing interested parties to assess the potential discriminatory effects of a given system. ▶ Invest in capacity building, including interdisciplinary research into non-discriminatory algorithms and into strategies to protect equality in the use of algorithmic systems.
Further rights considerations	Legal frameworks, regulations or rights that protect access to the metaverse and accessibility concerns should be assessed.

Issue: algorithmic bias	
What creates or contributes to the issue?	Algorithmic systems are too often built and sustained by old data and models that reproduce stereotypes and false assumptions about gender, race, sexual orientation, ability, class, age, religion or belief, geography and other socio-cultural and demographic factors. Selection bias: data used to train algorithms may not be representative of the entire population or relevant context. This can lead to skewed results and exacerbate existing biases in the data. Data bias: algorithms learn from historical data, and if the training data used to develop the algorithm are biased, the algorithm can perpetuate and amplify those biases. Biased data may reflect historical discrimination or under-representation of certain groups, leading to biased predictions or decisions. Inadequate evaluation metrics: evaluating the performance of an algorithm based solely on accuracy can overlook biases. Algorithms may achieve high accuracy overall but perform poorly for specific subgroups, leading to biased outcomes. Feedback loops: biased predictions or decisions generated by an algorithm can create feedback loops that reinforce existing biases in the data, perpetuating the problem over time.
Related efforts	The Council of Europe Study on the impact of artificial intelligence systems, their potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination (2023)

Issue: algorithmic bias	
Prevention and mitigation options (expert contributions)	Focus on responsible design, development and deployment of AI systems to mitigate algorithmic bias, promote fairness, transparency and accountability. Technologies should be designed to respect diversity, uphold ethical principles and avoid perpetuating societal biases within the metaverse.
Examples of related frameworks (non-exhaustive)	Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108). This Council of Europe convention safeguards individuals' rights regarding the automatic processing of personal data, including principles related to data accuracy and fairness in algorithmic decision making. Council of Europe Recommendation CM/Rec(2019)2 on the roles and responsibilities of internet intermediaries addresses the responsibilities of internet intermediaries, including those operating algorithms, with respect to upholding human rights and freedom of expression. Council of Europe Recommendation CM/Rec(2020)1 on the human rights impacts of algorithmic systems. This recommendation addresses the human rights implications of algorithmic decision making and calls for measures to identify and prevent discriminatory effects. EU Charter of Fundamental Rights. The EU Charter of Fundamental Rights enshrines several rights that are relevant to addressing algorithmic bias, including the right to non-discrimination (Article 21), the right to privacy (Article 7) and the right to data protection (Article 8). General Data Protection Regulation (GDPR). The GDPR provides strong data-protection rights to EU residents, including the right to fair and transparent processing of personal data. It emphasises the importance of avoiding discriminatory practices when processing personal data through algorithms. Audiovisual Media Services Directive (AVMSD). The AVMSD includes provisions to safeguard the right to freedom of expression in the digital sphere, aiming to ensure that algorithmic recommender systems do not lead to content filtering that restricts pluralism and diversity of viewpoints

Issue: algorithmic bias	
Related discussions	The AI Now (New York University) report identified a “diversity crisis” in the AI sector, especially in the global technology industry, which is overwhelmingly white and male, and asserts that this has contributed to algorithmic gender and racial biases.

Issue: labour	
What are the tech issues that create or contribute to the issue?	Job loss from generative AI Devaluation of jobs Metaverse jobs require strong internet and certain skills Under-representation of women in the ICT sector
Examples of related frameworks (non-exhaustive)	European Convention on Human Rights European Social Charter

Issue: social interaction and community building	
What are the tech issues that create or contribute to the issue?	The metaverse is a large and complex space, making it difficult to identify and remove harmful content. There is a lack of consistent rules and guidelines regarding interactions and violations. The meaning of content can vary depending on the context in which it is created and shared. This can make it difficult to determine whether content is harmful or not. Content moderation is often done by humans, who can be biased in their decisions. This can lead to the removal of legitimate content or the retention of harmful content.
Related efforts	Companies are developing codes of conduct for virtual experiences. Enabling the lack or removal of “gatekeepers”.
Prevention and mitigation options (expert contributions)	Ensure that digital identities are secure, trustworthy and resistant to fraud and impersonation. The emotional and psychological effects of social interactions in the metaverse on users need to be considered. Issues such as addiction, isolation and mental well-being should be addressed through thoughtful design, user education and supportive community management practices.

Issue: social interaction and community building	
Prevention and mitigation options (expert contributions)	While disintermediated communication offers freedom of expression, mechanisms should be in place to address harmful or malicious behaviour. Encourage the development of community-driven moderation systems and content policies that strike a balance between fostering open dialogue and ensuring a safe and inclusive virtual environment. Provide platforms and tools that facilitate the creation and growth of virtual communities. This includes offering resources for community management, collaboration and shared ownership, as well as incentivising positive engagement and contribution within virtual societies. Develop guidelines that strike a balance between freedom of expression and preventing harm, hate speech, misinformation and discriminatory practices. Metaverse platforms should be transparent about their content moderation policies and procedures. This includes providing users with clear and concise information about what content is allowed and what content is not allowed. Metaverse platforms should be accountable for their content moderation decisions. This means providing users with a way to appeal against content moderation decisions and to hold metaverse platforms accountable for any harm that is caused by their content moderation policies. Metaverse platforms should involve the community in the development of their content moderation policies and procedures. This will help to ensure that the policies are fair and reflect the needs of the community. Metaverse platforms should use technology to help them identify and remove harmful content. This could include using artificial intelligence (coupled with human supervision) to scan for harmful content or using human moderators to review content. There is also the need to co-operate and co-ordinate with law enforcement to secure e-evidence. Metaverse platforms should educate users about harmful content and how to report it. This education should include information about the different types of harmful content, how to identify it and how to report it.

Issue: social interaction and community building	
Prevention and mitigation options (expert contributions)	Metaverse platforms should collaborate with other stakeholders, such as governments and non-profit organisations, to develop and implement content moderation policies and procedures.
Examples of relevant frameworks (non-exhaustive)	Council of Europe Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of Internet intermediaries. Content Moderation – Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation. GDPR Council of Europe standards on content moderation.
Related discussions	Comparisons can be made with the social dynamics on existing platforms such as social media and online games. Lessons learned from these technologies can help mitigate potential social challenges within the metaverse.
The role of technical standards	Develop robust infrastructure and protocols that enable secure, peer-to-peer communication within the metaverse while addressing concerns related to privacy, security and harmful content. Encourage the development of open standards and interoperability to facilitate seamless communication across virtual environments.

Issue: the environment	
What are the tech issues that create or contribute to the issue?	The metaverse depends on hardware that is manufactured using extractive processes that produce greenhouse gases and that is not fully recycled. E-waste is currently the fastest growing category of waste in the world.
Related efforts	Green or sustainable ICT, including the metaverse, is often seen as part of the green digital transition. From a private industry perspective, matters related to sustainability are sometimes tagged as part of corporate responsibility, and then as part of responsible innovation. More recently, in view of the energy crisis and more specific measures (such as the Green Deal and Fit for 55 package or Corporate Sustainability Reporting Directive), energy efficiency became part of compliance as opposed to voluntary reporting or a sign of a responsible industry.

Issue: the environment	
Prevention and mitigation options (expert contributions)	Prioritising environmental considerations.
Related existing frameworks (non-exhaustive example)	UN Sustainable Development Goal #3 United Nations General Assembly declaration (2022): everyone on the planet has a right to a healthy environment. OHCHR General comment No. 26 (2023) on children's rights and the environment with a special focus on climate change, Committee on the Rights of the Child, 22 August 2023: there is an urgent need to address the adverse effects of environmental degradation, with a special focus on climate change, on the enjoyment of children's rights. This comment clarifies the obligations of states to address environmental harm and climate change. Children's rights under the Convention on the Rights of the Child apply to environmental protection.
Related discussions	The internet, AI, green digital/green ICT initiatives and discussions.
Enforcement in the metaverse	Related enforcement is complex as a result of the scale and speed of the metaverse context.

Issue: children's rights	
What are the factors that create or contribute to the issue?	Online risks include the 4Cs: content, contact, conduct and contract. Flawed or no age identification measure resulting in exposure to inappropriate materials and individuals. Lack of age-appropriate design.
What are stakeholders doing?	Some apply the following in their products and services: ► age-verification schemes ► age-appropriate design
Prevention and mitigation options (experts' contributions)	Leveraging existing standards, such as the Age Appropriate Digital Services Framework standard (IEEE Std. 2089-2021), provides processes to accomplish many of the key points identified above and encompasses the following key principles: ► recognition that the user is a child ► acknowledgement of the diversity of children and young people

Issue: children's rights	
Prevention and mitigation options (experts' contributions)	▶ presentation of information in an age-appropriate way ▶ utilisation of fair terms appropriate for children ▶ prioritisation of children's best interests over commercial interests. This could address significant challenges relating to privacy, safety, trust, security and usability among the vulnerable population of children, all of which are critical in the metaverse also. Getting the right people into the room to discuss the issues, especially from companies, because even within companies there are different interests. If discussions are had with someone whose job is to really push safety forwards, the conversation will be much different than with someone whose job is to get products released or to look at user interfaces. Regular audits and updates. Encouraging girls to enter STEM (science, technology, engineering and maths) sectors. Metaverse developers and platform operators must prioritise age-appropriate content and design features that promote healthy development. Implementing adequate age-verification measures and providing tailored experiences for different age groups can ensure child safety and well-being. Stakeholders should adopt "do no harm" principles and perform best-interests assessments and risk assessments. Stakeholders should assess how a specific feature, such as nudging, will affect children and also integrate risk assessments focused specifically on children into design and auditing phases. They can also consult with children about what they want from services and the types of protections and means of accessing help and protection that would work for them. Any consultations should only take place in accordance with child participation safeguards. Other activities include: ▶ holding workshops that walk through multidimensional issues, similar to collaborative design exercises; ▶ promoting digital literacy and educating children about online safety and responsible digital

Issue: children's rights	
Prevention and mitigation options (experts' contributions)	citizenship, which are essential. Collaboration among schools, educators and parents is necessary to provide comprehensive education on metaverse usage, privacy protection and appropriate behaviour in virtual environments; ▶ the investment by metaverse platforms in robust safety measures, including content moderation, reporting mechanisms and preventive measures against cyberbullying and harmful content. Regular audits and updates to address emerging risks can help maintain a safe environment for children.
Related existing frameworks	Council of Europe ▶ Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment ▶ Interpretative Opinion on the applicability of the Lanzarote Convention to sexual offences against children facilitated through the use of information and communication technology (ICT) ▶ Lanzarote Committee implementation report 2nd monitoring round: The protection of children against sexual exploitation and sexual abuse facilitated by information and communication technology (ICT): Addressing the challenges raised by child self-generated sexual images and/or videos (2017-2022) ▶ European Social Charter ▶ Handbook on Children's Participation: Listen – Act – Change CP4Europe. General comment No. 25 on children's rights in relation to the digital environment. UK Age Appropriate Design Code (AADC) GDPR. The General Data Protection Regulation seeks, among other things, to contribute to the "well-being of natural persons" (recital 2). However, the interests of the child are most clearly expressed in recital 38, which states that children enjoy specific protection in the light of their fundamental right to data protection. Other considerations in the GDPR emphasise the specific protection of children: recital 58 (transparency of data

Issue: children's rights	
Related existing frameworks	processing), recital 65 (right to be forgotten), recital 71 (automated decision making and profiling) and recital 75 (risks of processing personal data). These recitals were drawn up as provisions of the GDPR. EU Audiovisual Media Services Directive (AVMSD) 6a(1): member states shall take appropriate measures to ensure that audiovisual media services provided by media service providers under their jurisdiction which may impair the physical, mental or moral development of minors are only made available in such a way as to ensure that minors will not normally hear or see them. Such measures may include selecting the time of the broadcast, age-verification tools or other technical measures. They shall be proportionate to the potential harm of the programme. The most harmful content, such as gratuitous violence and pornography, shall be subject to the strictest measures. UN Convention on the Rights of the Child. The obligation to take account of the best interests of the child in all activities which have an impact on children can be found in Article 3(1) of the UN Convention on the Rights of the Child. Relevant children's rights can be: right to freedom of information, right to access to (non-harmful) media, right to free forming of opinion and thought, right to freedom of association, right to privacy and data protection, right to identity forming, play and relaxation, right to protection from violence (including bullying and sexual abuse) and from economic exploitation. In the implementation of relevant children's rights a balance must be found between the data-protection rights of children and their other rights, including their rights to development (Article 6), freedom of expression and freedom to seek, receive and impart information (Article 13) and association and assembly (Article 15).
Related discussions	Related discussions take place in the AI context.
Options for consideration	Consider models such as the AADC.

Sales agents for publications of the Council of Europe
Agents de vente des publications du Conseil de l’Europe

BELGIUM/BELGIQUE
La Librairie Européenne -
The European Bookshop
Rue de l’Orme, 1
BE-1040 BRUXELLES
Tel.: + 32 (0)2 231 04 35
Fax: + 32 (0)2 735 08 60
E-mail: info@libeurop.eu
http://www.libeurop.be

Jean De Lannoy/DL Services
c/o Michot Warehouses
Bergense steenweg 77
Chaussée de Mons
BE-1600 SINT PIETERS LEEUW
Fax: + 32 (0)2 706 52 27
E-mail: jean.de.lannoy@dl-servi.com
http://www.jean-de-lannoy.be

CANADA
Renouf Publishing Co. Ltd.
22-1010 Polytek Street
CDN-OTTAWA, ONT K1J 9J1
Tel.: + 1 613 745 2665
Fax: + 1 613 745 7660
Toll-Free Tel.: (866) 767-6766
E-mail: order.dept@renoufbooks.com
http://www.renoufbooks.com

FRANCE
Please contact directly /
Merci de contacter directement
Council of Europe Publishing
Éditions du Conseil de l’Europe
F-67075 STRASBOURG Cedex
Tel.: + 33 (0)3 88 41 25 81
E-mail: publishing@coe.int
http://book.coe.int

Librairie Kléber
1, rue des Francs-Bourgeois
F-67000 STRASBOURG
Tel.: + 33 (0)3 88 15 78 88
Fax: + 33 (0)3 88 15 78 80
E-mail: librairie-kleber@coe.int
http://www.librairie-kleber.com

NORWAY/NORVÈGE
Akademika
Postboks 84 Blindern
NO-0314 OSLO
Tel.: + 47 2 218 8100
Fax: + 47 2 218 8103
E-mail: support@akademika.no
http://www.akademika.no

POLAND/POLOGNE
Ars Polona JSC
25 Obroncow Street
PL-03-933 WARSZAWA
Tel.: + 48 (0)22 509 86 00
Fax: + 48 (0)22 509 86 10
E-mail: arspolona@arspolona.com.pl
http://www.arspolona.com.pl

PORTUGAL
Marka Lda
Rua dos Correeiros 61-3
PT-1100-162 LISBOA
Tel: 351 21 3224040
Fax: 351 21 3224044
E-mail: apoio.clientes@marka.pt
www.marka.pt

SWITZERLAND/SUISSE
Planetis Sàrl
16, chemin des Pins
CH-1273 ARZIER
Tel.: + 41 22 366 51 77
Fax: + 41 22 366 51 78
E-mail: info@planetis.ch

UNITED KINGDOM/ROYAUME-UNI
Williams Lea TSO
18 Central Avenue
St Andrews Business Park
Norwich
NR7 0HR
United Kingdom
Tel. +44 (0)333 202 5070
E-mail: customer.services@tso.co.uk
http://www.tsoshop.co.uk

UNITED STATES and CANADA/
ÉTATS-UNIS et CANADA
Manhattan Publishing Co
670 White Plains Road
USA-10583 SCARSDALE, NY
Tel: + 1 914 472 4650
Fax: + 1 914 472 4316
E-mail: coe@manhattanpublishing.com
http://www.manhattanpublishing.com

Council of Europe Publishing/Éditions du Conseil de l’Europe
F-67075 STRASBOURG Cedex
Tel.: + 33 (0)3 88 41 25 81 – E-mail: publishing@coe.int – Website: http://book.coe.int

IEEE Standards Association
445 Hoes Lane, Piscataway, NJ 08854, United States
Phone: +1 732 981 0060 – Email: metaverse.report@ieee.org

This collaborative report by the Council of Europe and the IEEE Standards Association navigates the complexities of technology and human rights, emphasising the importance of a human-centric approach to immersive realities development, such as the metaverse.

The report highlights key issues and risks while exploring the potential benefits of the metaverse. Grounded in ethical considerations, it underscores the necessity of upholding principles of human rights, the rule of law and democracy.

Authored by a consortium of over 50 IEEE experts and peer reviewed by the Council of Europe relevant sectors, the report provides essential perspectives on technical, ethical and governance dimensions. As the metaverse evolves, so too will the guidance offered within, ensuring policy makers remain informed and adaptable in this dynamic landscape.

PREMS 010924

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 46 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

9 789287 194664

http://book.coe.int
ISBN 978-92-871-9466-4
€13/US$26

IEEE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE