The metaverse

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

DG1 (2023)06

Abridged version of the report

IEEE
Advancing Technology for Humanity

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

DISCLAIMER

The present Synopsis was produced to provide an overview of the issues identified in the joint report of the Council of Europe with the IEEE Standards Association on the metaverse and its impact on human rights, the rule of law and democracy.

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 institutions of 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 pure illustrative purposes and are neither exhaustive, nor most representative examples. This work is published under the auspices of the IEEE Standards Association and the Council of Europe for the purposes of furthering public understanding of the importance of addressing human rights, ethical and rule of law considerations in policy- and decision-making processes.

Layouts and Cover Page:
Information Society Department
Council of Europe

Images: Shutterstock

This publication has not been copy-edited by the SPDP Editorial Unit to correct typographical and grammatical errors.

The metaverse

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

Abridged version of the report

This collaborative report by the **Council of Europe** and the **IEEE Standards Association**, a globally recognised standard-setting organisation within the IEEE (Institute of Electrical and Electronics Engineers), 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 driven approach to technology development, acknowledging the uncertainty of the metaverse's future evolution.

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

Council of Europe

Acknowledgements

The IEEE is 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; Chair of IEEE Decentralised Metaverse Initiative; Chair of IEEE Digital Finance and Economy Standards Committee); 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 (IEEE 3D Body Processing chair and Gneiss Concept) and Denia Psarrou. Special thanks go also to Dr Yu Yuan, Monique Morrow, Melodena Stephens, Katie Evans, Prof. Eleni Kosta, IEEE SA staff Moira Patterson, Sri Chandrasekaran, John Havens and Dr Clara Neppel for their valuable input 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 (Freedom of Expression and CDMSI, Data Protection, Artificial Intelligence, Cybercrime, Democracy and Governance, Anti-discrimination, Youth, Children's Rights and Sport Values, Education, Human Dignity and Gender Equality).

Contents

Introduction and scope 3

Application areas 5

Is it too early to deal with the metaverse? 5

Ethical considerations 6

Impact on human rights, the rule of law and democracy 7

- Privacy and data protection 8
- Identity 9
- Free expression, content and behaviour moderation and safety 10
- Inclusion, diversity, and accessibility 11

Labour 13

Political and social participation 14

Social interaction and community building 14

Health 15

Environment 16

Education 17

Children's rights 18

Trade, property, IP and competition in the metaverse 19

Metaverse, the rule of law, and democracy 20

- Cybercrime and virtual crime 21
- Personhood and ownership in the metaverse 22
- Rule of law and democracy in proprietary virtual spaces 22

Governance 23

- Regulation 23
- Self-regulation/Self-governance 24
- Technical and socio-technical standards 24

Concluding observations and considerations 25

References 29

Introduction and scope

The Council of Europe's Digital Agenda 2022-2025 points to the metaverse as a development that raises multiple 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 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 held at the time of the internet's emergence in the late 1990s, as well as during the rise of gaming platforms and virtual worlds.
The metaverse presents a cross-cutting ecosystem with possible applications across various industries and all aspects of life, spilling across generations with a significant indirect environmental impact. This presents many areas for consideration by policymakers, spanning 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. 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, a long reaction time will have severe consequences. 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, the report 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). Given 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 close to 50 experts to share their perspectives and expertise on the technical, ethical, social, legal, policy, regulatory, standardisation and governance issues associated with the metaverse. The report offers relevant considerations for navigating this shifting landscape.

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, next generation virtual worlds (JRC, 2023), immersive realities, digital twins, virtual, augmented, mixed or extended reality (VR/AR/MR/XR), or Web3. Further, the metaverse is often confused with other developments like blockchain, or other enablers or experiences. At the European Commission level, currently used terms include virtual worlds and immersive realities, while other international initiatives and partnerships continue to refer to the metaverse. The report does not aim to provide a definition, but rather a description of the metaverse. The term was 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). As such, these virtual worlds can be viewed as components/spaces of a single virtual universe - a metaverse with interconnected/interoperable elements, including virtual worlds and gaming platforms. These virtual worlds, which function independently and do not always allow a seamless transition from one to another, can have different levels of convergence or fusion with the physical world: they can exist separately and in parallel to the physical world; can be overlaid on the physical world; or can have an effect/impact on or interact with the physical world, or vice-versa (Stephens 2022). It should be noted that some consider that there are or will be several “metaverses” as opposed to the single “metaverse” vision. Standardisation efforts are ongoing to create a common language and definition of the metaverse. For instance, in the context of the IEEE discussions, the 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").

What makes the metaverse are its **features*:*** The metaverse is characterised by several features:

- the ***immersiveness*** of the experience (with varying degrees, such as 2D versus 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

For the metaverse to function, several existing and emerging technologies (both hardware and software) are brought together and integrated. Further underlying and enabling technologies facilitate the immersive experiences and features of the metaverse.

These technologies include, among others: 5G/6G networks that allow data transmission and connectivity; AI systems (systems that performs tasks without significant human oversight, or that learns from experience and improves performance over time); 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 an immersive experience, separate to the physical environment, through the use of devices like VR headsets); 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 2022b) 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. 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. Whether and how the vision for the metaverse will materialise and develop in the future is not known and it will depend on several factors like adoption, technology development, access to data, regulations, societal acceptance, and geopolitics.

Application areas

The metaverse, like the internet and like AI, is transversal, with different applications covering all aspects of life: it can be linked to consumer goods and services (retail, gaming, social platforms, media) as part of the **consumer metaverse**, education and research, industry, and manufacturing as part of the **industrial metaverse;** health and even justice, e-government, and political participation. There is no consensus on whether there is or will be one single metaverse, with some experts referring to several metaverses which will not necessarily be interconnected. While the metaverse could be viewed as yet another case of technology push (i.e., offering a new technology or product to the market, creating 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 are used for remote collaboration in business and industrial settings (Sykownik et al. 2021). Relevant studied show that younger populations are early adopters of the metaverse, with half of the surveyed millennials and GenXers in one study considering online experiences a meaningful replacement for in-person experiences (Deloitte 2023).

Is it too early to deal with the metaverse?

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). Therefore, 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.

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 and what are known as socio-technical standards. Ethical 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 which are 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 “neurorights”, 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 exemplifies how challenges regarding technology and regulation can play out. Issues and concerns were identified and discussed over several years with the complexity and involvement of different disciplines to cover different perspectives. The European Commission (EC) High-Level Expert Group on AI developed the Ethics Guidelines for trustworthy AI 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 for Artificial Intelligence (CAHAI) and the Committee for Artificial Intelligence (CAI) at the Council of Europe, with the development of the draft AI Convention currently under discussion.

Established ethical principles in the AI space, promoted by frameworks like the IEEE's Ethically Aligned Design (IEEE 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 (see also IEEE 2022).

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 relevant 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 and virtual worlds. 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.

A few large companies and nation states are primarily responsible for the development of the metaverse.
If this trend persists, these players may have considerable power to control access, conduct and users' data globally. The fair and inclusive ownership, transparency, accountability, and control of the metaverse are pressing ethical concerns, and there are acute risks 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, and the expectations, roles and responsibilities of different stakeholders of the metaverse ecosystem in safeguarding human rights, the rule of law and democracy.

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 harms and the promotion of core ethical principles, including South Korea, the Agile Nations (an inter-governmental cooperation network of states committed to providing an innovative regulatory environment), the World Economic Forum (WEF) and the OECD, while Chile has incorporated neurorights 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 cooperative ethical analysis are likely to be key to harnessing the metaverse's benefits on a global scale.

Impact on human rights, the rule of law and democracy

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 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 relevant 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 provide a highly personalised and responsive user environment and experience. Metaverse-enabling hardware is equipped with sensors that collect, process, and create an unprecedented volume of data to drive key metaverse functionalities, including physiological, psychological, and biometrics data like pulse, breathing, temperature, eye movement, facial expressions, gait and gestures, voice, and brainwaves. In just 20 minutes of using a VR headset, roughly 2 million points of biometric data are collected (Bailenson 2018). This results in more **intrusive method of data collection** or what some call **requisite sensing** (O'Hagan et al. 2023). 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 protection (Article 8 the Convention) remains essential, especially considering potential issues related to the concept of anonymity.

The increased appetite for data collection and processing is increasingly tied to a lucrative data brokerage industry, generating billions in revenue for profiling, recommendations, and advertising; also, this could include the use of AI bots instead of human workers, with possible transparency issues vis-à-vis users, and uncertainties about ownership of this data and related access rights.

Privacy has been respected for thoughts and leisure, but new invasive biometric technologies might challenge this in the future. While a lot of attention goes to data and data protection (Renieris 2023), there are further concerns, tied to **freedom of thought** (Art. 9 the Convention), **mental privacy** and **autonomy/integrity**. Moreover, there is a higher risk of **discrimination or attacks to the dignity and identity** of users when sensitive data is made available, and a threat to access to information if they are deprived of certain information because of profiling and recommendation systems.

Informed consent for data collection, processing and use is a challenging area: this informed consent can happen in the form of a "blanket approval" through **active opt-in. Passive acceptance** of terms of service has been ruled out as an unlawful practice in the context of social media. It is not always a given that users will be aware and understand the extent and types of data collection involved, or the expected and authorised use of this data. This brings into question how informed even specific consent could be and opens opportunities for circumventing the laws to which data controllers and processors must adhere.

In particular, this is relevant to children. The Council of Europe made a call to step up the protection of **children's privacy** and data protection in the digital environment and has provided guidelines to respect, protect and fulfil the rights of the child in the digital environment (Decl(28/04/2021), CM/Rec(2018)7). Age-appropriate design principles should also be explored for the metaverse context, or even extended to a child-centric general design. 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. Relevant 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. This Recommendation poses 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 traditionally considered private spaces, like individual homes (O'Hagan et al., 2023). However, unintended access to information (location, standard of living, personal preferences, etc.) through sensors enabling immersive experience blurs the boundaries between private and public spaces, along with the meaning of consent for accessing and using related information. This raises concerns about **"reasonable privacy."** Privacy concerns in the metaverse extend to **professional, civic, and academic settings.** Without the appropriate safeguards in **place, the growing use of biometric data and lack of research standards exacerbates the risk of** biases, discrimination, and exploitative practices.

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 and **erosion of their reasonable expectation of privacy** (Franks 2017), supporting "cyborg stalkers" and creating a global panopticon society. This calls both for multidisciplinary dialogue to assess the technical feasibility of addressing this issue, and public awareness about privacy concerns and new connotations of privacy in the metaverse context.

A further perspective to consider is that of anonymity: it can protect privacy, for example, through an avatar which does not disclose certain aspects of an individual's identity, but 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.

Information and data 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 transfers, data sharing and portability across different applications. In addition, informed consent, a user-centric approach, strong cybersecurity measures, user agency and control of their personal information should be considered in the metaverse. A further issue for discussion would be the role of supervisory authorities and enforcement entities, 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**, and is customised to reflect physical features, personality, expression of social-cultural affiliation, and preferences. At the stage of design, developers should consider an **inclusive design** approach to ensure 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. This 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.

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. Equally important is the information about whether a presented identity-an avatar or a **digital human** (i.e., an advanced version of an avatar which reflects not only physical but also behavioural aspects of an individual) is

controlled by a human or is an AI agent. A **right to be informed,** recognised to date for user data held by public authorities, could come in question to provide transparency in the interaction.

A series of legal questions arise, including the **right to access** and **ownership** of one's own virtual representation/avatar and the right to **amend the view of others** without their consent (right to identity vs. free expression), and related platform accountability. **Personhood of digital humans,** an issue also found in the AI systems context, should be carefully considered as it could lead to complex and potentially dangerous conclusions, such as the recognition of human rights for AI agents. The often psychologically 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, as well as the relationship/treatment of multiple avatars and identities in the same or across platforms and the interplay between virtual and non-virtual identity.

Where **identity data ownership** is concerned, relevant legal and technological frameworks are not yet fully developed, depriving users of complete control over the flow and utilisation of their identity data, which may cause data and privacy disclosure, legacy issues, and putting identity security at risk.

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 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 world. 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 respectively, 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). Such 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 also 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 et al. 2016) and have the potential to incite hate or manipulate beliefs. Metaverse technologies can potentially alter individuals' perception of people, reality, and the world, based on user preferences, gatekeepers' interests, government mandates, and biometric psychography (Heller 2020; Bye 2021), allowing for **enhanced behavioural nudging** (Hummel and Maedche 2019; Schmidt and Engelen 2020). Different stakeholders may do that, including the headset wearer, owner, vendor, or governments, allowing for removal, obfuscation, or alteration of real-world content (diminished or altered reality). This manipulation, whether consensual or imperceptible to the user, could lead to change of attitude, biases, or political exploitation, affecting political participation and global citizenship

behaviours. Unlike digital disinformation limited to web-based social media, AR can embed such manipulation into everyday experiences on a much larger scale.

XR devices have the unique capability to **control users' perceptions of reality** through visual, auditory, and haptic stimuli, either filtering and augmenting their perceived reality or creating a distinct virtual environment (VR). XR integrates augmentations into the physical world, introduces imperceptible manipulations, and elicits physical and cognitive changes, making it more potent. While these manipulations are currently used to enhance XR experiences, they could potentially harm users and give rise to dark and deceptive design patterns in the future.

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, with a consideration of an opt-out option 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 on which metaverse software is built might further influence which data of users is collected, how it is processed and therefore exacerbate inequalities in experiences and the opportunities provided to users in their metaverse environment (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 to a de facto censorship and a threat to democracy.

Perceptual manipulation techniques require a fundamental **re-evaluation** by states/public authorities **of the permissible digital content** presented to users in XR to ensure **perceptual integrity**. Leveraging the benefits of perceptual manipulations while avoiding the creation of deceptive design patterns is crucial, and introduction of related limitations and rules could 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.

Lastly, if there is prevalence of misinformation and manipulation, the meaning of expression of thought (Art. 9 of the Convention) should be explored in the metaverse context, along with citizens' autonomy. The freedom from interference in citizens' thinking process and freedom of choice which may be at risk. To protect mental autonomy, some experts are discussing the need for "neurorights" (see more in the respective section), which are meant to safeguard clear-thinking processes and critical thinking, limiting external sources of manipulation and allow for critical thinking and autonomous decision-making.

Inclusion, diversity, and accessibility

The metaverse is not accessible by everyone either because of cost, internet access or skills (European Parliament 2022). As the metaverse becomes more prominent, special attention must be given to the experiences and challenges of marginalised and vulnerable populations, including persons with disabilities, the elderly, and all other groups at risk of discrimination or being targets of hate based on their personal characteristics and status. These groups face unique opportunities and risks in the virtual realm, requiring strategies to ensure inclusivity and safety within the metaverse. To promote the participation of persons with disabilities in the metaverse, their involvement in the

development process can lead to a more inclusive and accommodating virtual environment. Incorporating universal accessibility and inclusive design features by collaborating with disability advocacy organisations can be vital. To enhance the participation of the elderly in the metaverse, simplifying user interfaces and providing tailored support can overcome age-related and skill challenges. In addition, inclusivity should have a special focus on the impact of the metaverse offline, considering issues such as privacy, data protection, continuous digital literacy and social isolation. These issues are important as they affect well-being and engagement of this population in the virtual realm.

The immersiveness and location independence of the metaverse can support inclusion and enhance accessibility for remote and marginalised populations, allowing these groups to benefit from its potential. One example is virtual concerts which increase accessibility to those with disabilities. However, there's a risk that real-life venues may use virtual alternatives and virtual accessibility as an excuse to avoid accommodating people with functional limitations and other types of social, cultural, and economic barriers for participation in the physical world. This could lead to exclusion of some individuals who are left with only virtual options. Immersive inclusion should not lead to offline exclusion; both options should co-exist for a truly inclusive experience.

At the same time, lack of required infrastructure and cost of hardware pose the risk of an exacerbated digital divide, which could leave a significant part of the global population behind, out of and unrepresented in the metaverse, threatening the exercise of basic freedoms and rights and an inclusive and democratic metaverse. Furthermore, existing disparities (e.g., because of age, gender, functional limitations, language or other personal characteristics or statuses) will persist, are likely be perpetuated and amplified in the virtual world, leaving many experiences out of reach to those most in need of them.

Considering the private ownership of virtual spaces and the transition into digital “public spaces and services” will add further layers to the access issue and may require a global strategy to tackle. In terms of ability, the metaverse should be accessible to individuals with diverse capabilities, knowledge, expertise, physical and mental abilities, languages and social-economic status; VR/AR hardware is already considered emerging assistive technology for persons with functional limitations (WIPO 2021) and access to such devices could be considered a human right and state obligation as per the UN Convention on the Rights of Persons with Disabilities (UNCRPD 2008).

Moreover, the design of metaverse experiences should be inclusive and resonate with both online and offline communities to ensure representation of the diversity of individuals, groups and communities within society. A risk which could lead to the opposite result is bias in datasets affecting minority groups and under-represented individuals and communities based on their personal characteristic of status at the algorithmic level as outlined in the Council of Europe - “Study on the impact of artificial intelligence, its potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination”.

Such bias should be mitigated to avoid its permeation across the entire XR landscape. Addressing bias will yield a more inclusive and equitable metaverse as well as a more responsible and socially beneficial XR landscape. Responsible design should be responsive to the principle of fairness and inclusivity. Inclusive design in the metaverse can contribute to accessibility for diverse abilities, languages, and backgrounds, through customisation and individualisation, and by accommodating functional limitations, languages, social, cultural, and economic contexts, enabling representation and equal participation for all users and allowing for cultural heritage preservation. The latter will compete with virtual communities and their unique culture. Accountability and inclusive representation must robustly feature in the organisational governance of metaverse designers and deployers, allowing for adjustments and implementation of feedback to address related concerns.

Labour

The metaverse is expected to contribute significantly to the global GDP, with growth worth an estimated 800 billion Euros by 2030. The metaverse is also expected to transform the employment sector, with a 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, and reduced CO_2 emissions, and access to a global talent pool. 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 on issues such as wages and safety. However, enforcing an employer's duty to protect employees regarding occupational safety within the metaverse may present challenges. This can be advocated for by these aforementioned interest groups.

Working in the metaverse comes with some disadvantages, just as with digital work. It can blur the boundary between personal and professional life, making it challenging for caregivers, mostly women, to manage distractions and maintain work-life balance. Employers may not provide ergonomic working conditions or cover relevant costs, 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 potential monitoring. Employers will need to strike a balance between ensuring professional conduct and respecting employee privacy. Special data protection requirements have been established to address the legal concerns associated with data processing in employment relationships.

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 protect their right to disclose information about their disability and prevent discrimination. While employers may have limited influence over the avatar's design, they may request professional presentation to maintain uniformity and recognisability among colleagues and customers.

The European Social Charter acknowledges the right to work and fair conditions, including health and safety. With the metaverse, new challenges arise like global job losses and changing labour conditions, impacting well-being and society. This requires careful policy consideration.

The increased use of the metaverse, and the AI that drives the experiences and services, may lead to challenges such as perceived value for existing skill sets, making labour a commodity product and creating obstacles for maintaining livelihoods in the creator economy based on microtransactions. The metaverse, relying on AI, may lead to a significant increase in income inequality, impacting up to 50-70% of the wage structure (Acemoglu and Restrepo 2021). During the COVID-19 pandemic, four billion people were not adequately protected from job losses, highlighting the need to prepare the labour force for a changing landscape to avoid potential losses amounting to trillions of dollars (ILO 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 continuously evolving.

Due its borderless nature, determining the applicable law 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 policymakers.

Political and social participation

The metaverse offers **opportunities for increased political representation and the participation of marginalised communities in civic and political activities**, while **governments and politicians** follow popular platforms and **bring their messaging into virtual worlds**, crossing over from activity in online platforms into the metaverse. Governments are planning for the related changes and transitions, creating, among others, positions like a "Web3 minister." (Petkov 2023). However, increased use of the metaverse in political environments also comes with risks.

In virtual worlds, **political opponents** could be **visually, or audibly "blocked" or censored,** and **informational media** could be augmented, employing, for instance, **deep fakes to create confusion**. **Social augmentations** could be used to **spread political messages in targeted communities** or **suppress voter engagement** through obfuscations and alterations of voting stations (ACLU 2021). **Disinformation and conspiracy narratives** can result in or deepen **polarisation** or undermine inclusion and equality in a community, fuelling hate speech, bullying, harassment and exclusion. While the metaverse **can amplify grassroots voices**, it can also drown them out (Miazhevich 2015), presenting challenges in maintaining a fair and transparent political environment. **Countries with increased access rates to the metaverse** could also potentially have a **larger influence** over others in the virtual realm, while the dominance of a few languages may similarly lead to **limited language representation** and linguistic-based bias which should be addressed with proper governance. Representing **national culture** in virtual spaces of political participation can also be challenging, similar to new aspects of culture which can be formed within gaming and social networking communities with dynamics potentially not represented in the physical world. **Governments** are exploring how they want to be **represented in the metaverse**, with some, like Barbados (Wyss 2021), setting up consulates in virtual spaces or Tuvalu migrating its government to the metaverse.

The principles of citizen involvement could extend to virtual spaces, offering virtual avenues for **citizen participation** and dialogue between civil society and authorities, or even transforming traditional civic engagement. Co-management models involving youth, like Arnstein's ladder of participation (Arnstein 1969), 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 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 one.

In the metaverse, the concept of society may undergo redefinition and **virtual societies** may emerge, with opportunities to develop new relationships and a sense of belonging, collaborate on projects, and participate in shared experiences. These communities may create their codes of conduct, social norms, and even economies, and allow for **new expressions of social identity.** This is expected to influence young users, who are early adopters of the metaverse, and already consider online social interactions a meaningful replacement of in-person interactions (Deloitte 2023). Relationships with AI agents could become more prevalent, adding a **new layer to our traditional human interactions**,

blurring the lines between reality and virtuality, necessitating further long-term studies in terms of impact (Koike and Loughnan 2021). As society evolves, it is crucial to evaluate which changes are beneficial and which changes put our societal values, individual rights, freedoms, and humanity at risk. For this reason, safety needs to be considered more carefully at the design stage, as well as agency, choice, identity, and empowerment.

This could require the intervention of public authorities through the development of appropriate measures, including relevant legal frameworks. Co-operation with the virtual world and immersive experiences providers would be expected or recommended, as well as multidisciplinary teams for assessments before action. It is vital to develop guidelines and mechanisms to address harmful, offensive, or discriminatory content in virtual spaces, while balancing freedom of expression and preventing harm, hate speech, harassment and misinformation which could exacerbate known issues from social media (Frankel and Browning 2021) and lead to social exclusion. Responsible content creation, user empowerment, and dispute resolution mechanisms can foster a safe and inclusive metaverse environment.

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 if there are 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.

Immersion in 3D environments within the metaverse can have both short-term and long-term physical negative physical health effects, including issues such as nausea, injuries from lack of awareness of surroundings, physical fatigue, eye strain, and potential risks from electromagnetic radiation. 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.

The metaverse offers the advantage of overcoming barriers to healthcare access, as telemedicine enables remote consultations and delivery of healthcare services, benefiting individuals in underserved areas, provided that the virtual consultations would not be inaccessible because of additional fees. Virtual reality and augmented reality technologies allow healthcare providers to remotely examine patients, provide diagnoses and deliver personalised care. This reduces travel burdens and can enhance access to medical professionals for those facing physical access challenges to healthcare facilities.

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 (PTSD), and anxiety disorders, as well as pain management. For treating conditions such as depression, some therapeutic uses of metaverse technologies can also involve brain stimulation, which directly stimulates the brain using sensors, affecting pulse rates and eye movements. This type of brain stimulation also occurs 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 the developing brains of children. As such, experts recommend prohibiting brain stimulation unless it is for limited amounts of time and for therapeutic purposes, until extensive studies give a better understanding of the effects. In recreational contexts like gaming, brain stimulation may not be necessary. 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 postoperative 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, among others. 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 advancements in the healthcare industry.

Existing studies on the metaverse's impact on mental health are limited and cannot 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 more extensive and diverse research to understand the full scope of the metaverse's effects on mental well-being. Further, the issues of latency (the lag in data transfer) can have significant consequences in health care procedures requiring precision. Similarly, cybersecurity may need to be enhanced given that healthcare is such a sensitive sector. 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.

As metaverse technologies advance and virtual experiences become more realistic, the ability to distinguish reality from fiction becomes distorted, which carries a risk of manipulation. Projected negative impacts of metaverse technologies on mental health are related to internet addiction and excessive online gaming, which were recognised in 2018 by the WHO as a psychiatric disorder and lead to disassociation and withdrawal from the physical world. Studies have shown that these behaviours often serve as coping strategies, and the tailored and immersive experiences of the metaverse can make them addictive. The growth of specialised treatment centres for this problem highlights the need for policy interventions. This is particularly the case for specific metaverse applications which will be recognised as mostly addictive, as a preventive mechanism. 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 negative life impacts, increased risks of injuries and diseases.

There is a need to fund research into the health implications of metaverse usage online and offline, at an individual and collective level, across generations. Further, in the area of health, governments may need to set up policy tools like RegLabs (when regulators enable new business activity based on agile regulations) or regulatory sandboxes to assess existing policies' robustness. Data trade deals are already happening for healthcare data and there may be a need for global consensus on best practices to ensure that the rights of the individual are safeguarded, as well as individual genetic markers that could be exploited for profit.

Environment

On 16 and 17 May 2023, the Heads of State and Government of the Council of Europe's 46 members met at the 4th Summit in Reykjavík 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" (Reykjavík 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 links 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 as human right and made sustainability a state obligation (OHCHR 2022). A sustainable planet is also a precondition for citizens to enjoy their fundamental freedoms and exercise their rights. The rapid growth of the metaverse and its potentially exponential adoption and use raise concerns about its environmental footprint linked to energy consumption due to reliance on massive data servers for cloud computing, resource extraction methods due to semiconductors, wearables and other hardware consumption, data transfers using land cables, marine cables or satellites and the poor recycling of e-waste, one of the fastest growing categories of waste.

The environmental impact and energy requirements of these technologies require careful oversight. As a response, discussions about the green digital transition and sustainable information and communication technologies (ICT) practices are starting to take place. For instance, initiatives like the IEEE Global Initiative on Sustainable Metaverse and the IEEE Planet Positive aim to address these environmental issues, such as a need for technical standards, including common language, and metrics, and indicators on how to develop, deploy sustainable technology and measure their environmental footprint.

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

Education

The right to education is recognised by Article 2 of Protocol No.1 to the Convention. Immersive learning offers a unique approach to education. However, in an exclusively virtual environment ensuring access to education would require providing access to enabling hardware or specific software applications to avoid discrimination and access issues. This is especially so for underprivileged populations or persons with functional limitations without appropriate assistive technology or accessibility software.

Metaverse applications in educational environments can offer valuable opportunities for skill practice, risk-free learning 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.

During the Covid-19 pandemic, the education sector has embraced the metaverse for STEM classrooms, history teaching, medical training and research and military simulations. However, challenges like privacy, age-appropriate content, and resource trust need to be addressed. Ideally, metaverse content development for the purposes of education should be done by a multidisciplinary team to ensure the experience and skills are appropriate and can translate into the real world (for example, surgery techniques learned online versus offline).

Moreover, there is limited research on the metaverse's long-term impact, especially on children's development, physical, cognitive, emotional, and psychological capacities, making it a concern for organisations like UNICEF (see also the section on health). The use of virtual companions (which will get increasingly personalised) to teach children is a growing trend, with studies showing increased engagement. Either parents provide consent, or consent requirements are not clearly specified.

Online gaming platforms with AR and VR elements that are aimed at children have the potential to offer experiential learning. However, children need metacognition - awareness and understanding of one's own thought processes - to fully benefit from these immersive environments. Traditionally, metacognition has been taught by human instructors, but in online games, children lack such guidance. Moreover, studies show that children's brains are not developed enough to perceive all aspects of 3D environments, with unknown effects in case of long exposure. There is a need for teaching programmes for educators, parents and guardians to embrace new digital literacies, and for understanding required protections for consent, security, and privacy.

Children's rights

As children grow up in an increasingly connected world, VR is 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. 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 2022-2027and 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 safeguard children from potential harms related to content, contact, conduct, and contracts and to protect their right to childhood.

The increasing use of social VR by children and adolescents has raised concerns about their exposure to inappropriate content, harassment or bullying, as well as the potential risk of interaction with offenders. Grooming and sexual harassment are some of the dangers that children face in virtual environments, and which 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 importance of a human in the loop is also discussed. Another potential solution that prioritises safety, security and privacy for children includes building in age-verification processes and safety measures, similar to real-world scenarios, or more systematically and holistically incorporation and use of age-appropriate design principles (ICO 2020) and related technical standards like the IEEE 2019-2021 to address age-appropriate design for children's digital services (IEEE SA 2021), already from the very early design stages of the metaverse.

The challenge lies in protecting confidentiality and children's privacy and data when intervening to ensure children's safety in online spaces. It is key to ensure that their protection is non-negotiable,

considering how vulnerable they are to have their perception of reality and beliefs altered by the (manipulative) capacities of the technology. 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 also requires thoughtful examination, as immersive virtual experiences may blur the lines between virtual and physical worlds, and impact identity and social interactions. Overreliance 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).

In the metaverse, where much of life may be online and gamified, introducing virtual learning and education for children raises some concerns, especially regarding mental health and addiction risks. Children's exposure to technology and internet access at an early age should be done thoughtfully, with robust safety measures in place, accompanied by adult and parental supervision to address potential online risks effectively.

The metaverse's potential to intensify cyberbullying issues for children highlights the need for safeguarding measures to protect their mental well-being. Cyberbullying can have severe consequences, including increased suicide risk and negative psychological outcomes such as depression and anxiety. Addressing online bullying and promoting a safe environment within the metaverse is crucial to ensure children's mental health.

Trade, property, IP and competition in the metaverse

The metaverse presents diverse economic opportunities, including the sale of 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 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 -enabled creations raise the question of application of 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" 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 is crucial in the metaverse, as brands face various risks like malicious registration and counterfeiting.

In the virtual context, **copyright** protection applies to works created both outside and within the metaverse. Copyright infringement occurs when copyrighted works are reproduced or made available to the public without the owner's permission. The anonymity of the metaverse poses challenges in identifying the author and owner of copyrighted digital works. Avatars and AI cannot be authors under EU copyright law, 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 (IP) rights** in the metaverse faces challenges due to territorial limitations and difficulties in identifying infringers, especially in decentralised collaborative processes or when users are anonymous behind their avatars. Moreover, portability of virtual identities and assets can create issues of interoperability and application of IP rights across jurisdictions and virtual worlds. 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 computing power and storage capacity). IP right owners must adapt to virtual environments, meet additional requirements, and implement effective monitoring measures for successful enforcement.

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, such as the European Commission, 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 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 acquisition of technologies, data and users.

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 which can facilitate civic engagement in the virtual world. However, these same technologies 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 Court’s case law, 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 the exercise of human rights and for pluralistic and participatory democracy. Moreover, the rule of law 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 due to their personal characteristics or status.

Public authorities are expected to face significant challenges in transitioning and adapting to metaverse technologies. However, they 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 the ecosystem's stakeholders. Specific challenges relate to digital territoriality, metaverse-related crime, 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 and accountability, access to information and enforceability while still safeguarding equality and non-discrimination remain.

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 across various fields of the digital realm. Similar discussions are now occurring concerning the metaverse, particularly regarding jurisdiction. This involves considering different types of relationships, including those between platform providers and users, supply chain providers/intermediaries and users, government and other authorities, and platform/technology developers and providers, states and other authorities and users, and between users themselves. 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.

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 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 rules and terms of service violations 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 "griefing" (i.e., 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, with possible impact in and from the offline world, while some new types or variations of crime may emerge in immersive environments. 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.

Policing, law enforcement and justice in the metaverse area

Combating virtual crime in the metaverse involves technology, community efforts and legal measures. Reporting systems, user guidelines, and coordination 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 in the metaverse era can adapt through virtual policing units, AI and machine learning, virtual forensics, collaboration in cross-border investigations or extradition for cross-border possibly backed by mutual legal assistance treaties and international law enforcement agencies, blockchain analysis, proactive monitoring, and ethical considerations to effectively combat virtual crimes while safeguarding user privacy. It is important that all stakeholders involved have a technical understanding and awareness of the nature and variations of misconduct and crime in the virtual

realm. This understanding and awareness are necessary for effective protection of the rule of law and human rights. Implementing means of grievance and redress is vital to ensure crimes are regulated and punished appropriately. In this context, tools will be needed for digital forensics, enforcement and effective justice in general.

Here, it is worth mentioning the Council of Europe Convention on Cybercrime and its two additional protocols as an example of how the Council has responded in a timely manner to the evolution of cybercrime, taking into consideration the growing importance of digital evidence in traditional crime. Moreover, case law on virtual crime has provided that criminal activities in online and virtual environments do have an impact in the physical world and confirms that such case law are not new to the judicial system. Accordingly, online violations must not be normalised or tolerated. There is a much thinner line than 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*). Nevertheless, 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.

Personhood and ownership in the metaverse

In the metaverse, the concept of personhood and individual rights becomes complex. This is especially so given the convergence of virtual and physical worlds, 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 ownership of digital assets like non-fungible tokens (NFTs) and avatars. Issues that arise concern their portability and safety in transactions, the protection of creations in the metaverse by intellectual property rights (IPRs), 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

The metaverse and its enabler, Web3, is decentralised by design: it 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 which enable transactions through smart contracts and bottom-up decision-making by their token holders. This form of decentralised governance is meant to remove intermediaries in the metaverse, bring transparency and reduce risks like fraud. However, despite the open, community-driven and streamlined rationale of DAOs, legal and governance challenges remain, such as power concentration by wealthy DAO members and token holders (WEF 2023(b)).

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 players 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 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 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 should get access for virtual forensics and effective functioning of the rule of law.

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**, **technical** and other **standards.** For instance, the recently adopted Recommendation CM/Rec(2023)5 of the Committee of Ministers to member States on the principles of good democratic governance 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. By collaborating and adhering to law and standards, and continuously re-assessing and evaluating these, we can create a fair and inclusive metaverse that addresses its unique challenges and upholds human rights, principles of democracy and the rule of law.

Regulation

Global discussions in the field of AI also raise the issue of whether we should be moving towards **international regulation** for the metaverse (for instance, see 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 to its specific implementation, a harmonised approach can help avoid the challenges of fragmented regulation or cross-border value chains, and address the limitations of stand-alone private sector self-governance, as witnessed recently in the case of generative AI. A further consideration is whether we should be moving towards **technology-specific, impact, outcome or principles-based regulation**. The answer may be a combination of several of these, 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 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.

Anticipatory regulation refers to a proactive approach to regulatory governance, aiming to address the 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 other principles in the form of internal governance and policy documents, adherence to charters or other principle-based frameworks, voluntary adoption of compliance with **technical standards,** certifications and **co-regulation**. The latter 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 2006). 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-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, codes of conduct, self-moderation**, etc. Another key issue about governance in the metaverse lies within its own regulations and related sanctions, their **adherence** to relevant national and international law, the necessary transparency around the system in place, and the availability of appeal mechanisms. Currently, content moderation in such worlds is carried out 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 sometimes clashes 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 while adhering to 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 and socio-technical standards

Technical standards are a means of self-regulation, and their **voluntary** adoption an indicator of uptake of agreed principles. Technical standards serve as the bridge between policies, principles and practice. They set technical ground rules for developer interactions, and some already provide essential technical guidance for the metaverse, while several of the issues addressed in the report are already under discussion in standards development (IEEE SA 2022(b)). They follow defined processes, are consensus-based and are voluntary, while public authorities, for instance, in a public procurement context, can make their adoption a requirement. These characteristics make standards generally more flexible and adaptable than policy or regulatory instruments.

Standards, including **socio-technical standards,** which embed ethical and societal considerations in and beyond technical specifications, can play an important role in the technical implementation of agreed-upon principles and ethical considerations which are the basis of legal frameworks and

regulation, including in socio-technical issues that emerging technologies bring. They can create a common language and set verifiable criteria for compliance. Similar to anticipatory regulation, standards development frameworks need to involve 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 providing a presumption of compliance and increase transparency, reliability and trust.

In the metaverse context, considering the different layers of enabling technologies, standards are useful and needed for core foundational technologies, their robustness, safety of technologies, data and different rights. Bearing in mind the above discussions, standards can help address portability and transferability issues, authenticate data and its source, introduce systems and design thinking in the development and deployment of the metaverse, embedding human rights and related issues as opposed to considering them separate to the technical requirements, or an afterthought to be addressed with different instruments. Ultimately, standards can be a useful tool for a responsible and human-centric metaverse, along with increased societal acceptance. Furthermore, standards can be supporting tools for the rule of law by providing factual evidence for the respect or violation of human rights, translating related requirements into technical specifications by taking into account the state of the art, best practices and feasibility and verifiability of certain aspects.

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 need collaborative efforts to address. The metaverse will constantly evolve and the technologies we associate with it today may not be relevant tomorrow. Hence, ongoing discussions need anticipatory and agile regulations for user rights, balancing regulation and self-regulation, and addressing the complexities of the metaverse supply chain, including responsibility and governance.

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. This 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, the technologies involved and possible adjacent innovations, interdependencies and gaps, with attribution of roles, responsibility and accountability across the different ecosystem participants 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 assessments (such as HUDERIA) and technology risk and environmental impact assessments. Furthermore, **awareness raising, training** and dialogue between policy makers with the 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 which may be addressed through the development of technology and standards. Given that there are often calls for regulation while 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 workshops with technologists, futurists, lawyers and policy makers could help in the thinking process and deciding upon on the most appropriate approach.

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

The responsibility and decisions around the values we want for our future society should involve everyone. **Participatory dialogue** and consultation with different stakeholders are needed to assess societal acceptance and concerns by 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. 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, as well as 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 programs 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. **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' **right 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, 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 curricula**. Metaverse ecosystem architects, with specialist knowledge in underlying technologies such as blockchain, artificial intelligence, computer vision, data analytics, quantum computing and high-speed networks and others with relevant profiles will be needed to lead virtual transformation programmes.

…and 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 policymakers 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 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. As the metaverse develops, prioritising children's interests and rights through **age-appropriate design** and a 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 space

Access to effective protection, supervision and enforcement of human rights is more challenging in a virtual space environment, which tends to be proprietary, as is the collected and processed data. This can be a challenge for law enforcement authorities. Concerned stakeholders should discuss their roles and responsibilities, as well as access and verifiability requirements Moreover, these environments create additional complexities for digital forensics - training and 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 and some new concepts arise. There is a **risk of underestimating** the **different scope and meaning** of these same 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 the 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.

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. It also important to assess whether there are provisions in place or whether these are needed for digital/virtual jurisdiction, redress, supervision authorities and enforcement mechanisms, along with the options for access to required information**.

For example, the metaverse presents us with the unchartered territory of brain stimulation and its impact on human bodies and brains, in particular in developing children's brains, and long-term implications. Indications from existing research are worrying as it suggests that it can change the perception of reality. This is especially concerning given the lower requirements for consumer goods than medical devices. Until this is better understood, a more restrictive use of brain stimulation should be encouraged, allowing brain stimulation only for specific applications and uses, and for shorter durations, while observing the effect of its use.

In the metaverse, next to the online platforms **content management** we need to also explore ways for potential **behaviour control**, and a **combination of agent behaviour with space managemen**t which bring up several governance discussions.

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

There is a known challenge associated with keeping pace and catching up with challenges posed by emerging technologies to regulation and standardisation. Disruptive technologies and accelerations in technology open the way for discussions about anticipatory or adaptive regulation and policymaking, as well as **timely**, if not agile, **standardisation processes**.

The assessments of whether existing frameworks are sufficient or new ones are needed will require an in-depth impact assessment. New questions and rights may arise, either due to the highly transformative potential of the metaverse or the new challenges posed.

Some considerations for new rights and regulation are linked to cases with increased risks and potential impact on human rights, the rule of law and democracy. These include the invasive potential of brain-computer/human-machine interface (BCI/HMI) and metaverse-supporting technologies, in particular for children's developing brains and the unchartered long-term impact of activities like brain stimulation; the risks of personhood of digital humans which are AI agents not controlled by humans - similar to AI personhood, which can lead to dangerous conclusions and open a new layer of threats to humans. Saving human rights for humans specifically may need to be explicitly stipulated. The potential for losing an aspect of self-determination by losing control over individuals' data which will be collected (and commoditised) in an unprecedented manner may lead to the need of a recognition of a right to access individual's own data independently from provision of consent for data collection (there is already provision for this in the GDPR). Chile was the first jurisdiction to introduce "neurorights" into its constitution and Spain has 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).
For the Council of Europe, the question will be whether an evolving interpretation of freedom of thought (Article18 of the International Covenant on Civil and Political Rights (ICCPR) 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 relevant guardrails.

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. Lastly, with the increased use of AI agents for avatars/digital humans, among others, a series of legal issues will arise, where previous experience from the AI context could be useful in relevant discussions.

Outlook

In conclusion, this abridged version of the upcoming 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 summary of the report reflect a range of subjective perspectives stemming from the different experiences, assumptions, or conclusions of the experts who contributed to the report. However, the range and the aggregation of these ideas provide useful insight into current metaverse environments and scenarios considering past technology rollouts, and how these rollouts have affected society.

It is not obvious how to addressing these issues in a way that safeguards human rights, the rule of law and democracy: the metaverse space is still under development, meaning there is a degree of approximation and uncertainty. There are also challenges in capturing all relevant risks. There is no clarity or alignment in the terminology and some challenges are familiar from previous technology advances and enablers of virtual worlds, yet their dimensions and meaning within the metaverse are diverse. Further to this, 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 at scale on individuals and societies is still unknown.

At this point of early consideration, a series of decisions need to be made and are linked to the following questions, 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 terms of the challenges it brings from other 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 it is so transformative, what are the societal values we want to use to design the metaverse? What can we learn from the way issues in these areas have been 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 or are regional or domestic regulation and approaches enough? Can the metaverse self-regulate and is hard law needed, and if the answer is positive for both, for which areas is each 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 infringe 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’’ *Nordic Human-Computer Interaction Conference*, NordiCHI ‘22, 2022. https://doi.org/10.1145/3546155.3546691

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

Arnstein S. (1969.), A Ladder of Citizen Participation. *Journal of the American Planning Association*, 35(4), 216-224. DOI: www.tandfonline.com/doi/abs/10.1080/01944366908977225

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

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: https://doi.org/10.1145/3264899

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

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

Bye K. (2021), "#988: Defining Biometric Psychography to Fill Gaps in Privacy Law to Cover XR Data: 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: 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: https://espanadigital.gob.es/en/measure/protection-digital-rights

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

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

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

European Parliament (2022), Metaverse Opportunities, risks and policy implications: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733557

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): https://doi.org/10.1093/poq/nfw006

Frankel S. and Browning K. (2021), *New York Times:* www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.html.

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

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: 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): 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:https://doi.org/10.1007/s12152-022-09511-0.

Hummel D and 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*: http://dx.doi.org/10.1016/j.socec.2019.03.005

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

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

Information Commissioner's Office (ICO) (2020), Age-appropriate Design Code: https://merlin.obs.coe.int/article/8978

International Labour Organization (ILO) (2021), World Social Protection Report: https://www.ilo.org/global/research/global-reports/world-social-security-report/2020-22/lang--en/index.htm

Joint Research Center(JRC)/Hupont Torres, I., Charisi, V., De Prato, G., Pogorzelska, K., Schade, S., Kotsev, A., Sobolewski, M., Duch Brown, N., Calza, E., Dunker, C., Di Girolamo, F., Bellia, M., Hledik, J., Nai Fovino, I. and Vespe, M., 2023, Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU: https://publications.jrc.ec.europa.eu/repository/handle/JRC133757

Koike M and Loughnan S. (2021) "Virtual relationships: Anthropomorphism in the digital age." *Social and Personality Psychology Compass*, 15(6), e12603: https://compass.onlinelibrary.wiley.com/doi/full/10.1111/spc3.12603

Lodder, A.R., (2013), Ten commandments of Internet law revisited: basic principles for Internet lawyers. *Information & Communications Technology Law*, *22*(3): https://www.tandfonline.com/doi/abs/10.1080/13600834.2013.852769

Maloney D, Freeman G and Robb A. (2020a), "A virtual space for all: Exploring children's experience in social virtual reality", pages 472- 483, *Association for Computing Machinery*: https://dl.acm.org/doi/10.1145/3410404.3414268.

Maloney D., Freeman G and Robb A. (2020b), "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: https://doi.org/10.1109/VRW50115.2020.00075

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, Inc, 6 2021, pages 69-79: https://doi.org/10.1145/3459990.3460703.

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: https://games.jmir.org/2020/3/e14920.

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

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

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

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. https://doi.org/10.1098/rsta.2018.0089.

OECD. (2006), Alternatives to traditional regulation https://www.oecd.org/fr/gov/latestdocuments/92/

O'Hagan J (2023), "Privacy-Enhancing Technology and Everyday Augmented Reality: Understanding Bystanders' Varying Needs for Awareness and Consent". To appear in *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies:* https://doi.org/10.1145/3569501

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

Renieris E. (2023), *Beyond data: Reclaiming human rights at the dawn of the metaverse,* MIT Press: https://direct.mit.edu/books/monograph/5528/Beyond-DataReclaiming-Human-Rights-at-the-Dawn-of

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

Spano R. (2017), ‘’Intermediary liability for online users: comments under the European Convention on Human Rights”, *Human Rights Law Review*. https://academia.ilpp.ru/catalog/ij/ij-2-22-2017/intermediary-liability-for-online-users-comments-under-the-european-convention-on-human-rights/

Stephens M. (2022), Metaverse and its Governance, The IEEE Global Initiative On Ethics Of Extended Reality (XR) Report https://www.researchgate.net/publication/361362815_Metaverse_and_Its_Governance_-_The_IEEE_Global_Initiative_on_Ethics_of_Extended_Reality_XR_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, Portugal, pp. 546-554 https://doi.org/10.1109/VR50410.2021.00079

World Economic Forum (WEF) (2023b), Decentralised autonomous organisation toolkit: https://www.weforum.org/publications/decentralized-autonomous-organization-toolkit/

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

Council of Europe resources

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

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

Civil Participation in Decision-Making
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
https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108

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

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

Cybercrime Convention Committee (T-CY), Guidance note on identity theft and phishing in relation to fraud, 2013
https://rm.coe.int/16802e7132

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

Declaration by the Committee of Ministers on Internet Governance Principles, 2011 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
https://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
https://rm.coe.int/10-06-2022-digital-partnership-general-doc-updated/1680a6e634, 2022

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

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

European Court of Human Rights, Guide on Article 2 of the European Convention on Human Rights - Right to Life, 31 December 2020
https://www.refworld.org/docid/6048e29c2.html

European Court of Human Rights, Guide on Article 10 of the European Convention on Human Rights
www.echr.coe.int/documents/d/echr/guide_art_10_eng, 2002

European Social Charter, 1961 https://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 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
https://rm.coe.int/16806ebe7a

Guidelines for the co-operation between law enforcement and internet service providers against cybercrime 2008
https://rm.coe.int/2088-33-law-enforcement-isp-guidelines-2020/1680a091a7

Guidelines for the co-operation between LEAs and internet service providers against cybercrime. 2008
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3ba

Human rights guidelines for internet service providers 2008 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
https://rm.coe.int/16808ac918

Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech, 2022
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 2020
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, 2019
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, 2018
https://rm.coe.int/0900001680790e14

Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom 2016
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, 2016
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, 2015
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, 2014
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, 2013 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, 2012
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, 2012
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, 2011
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, 2010
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
https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d4a39

Reykjavík Declaration, United around our values, 2023
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
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
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
https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f

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

United Nations

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

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

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

FURTHER READIING

European Commission (2023), Virtual Worlds and Web 4.0 Factsheet:
https://digital-strategy.ec.europa.eu/en/library/virtual-worlds-and-web-40-factsheet

EUIPO (2022), “Virtual goods, non-fungible tokens and the metaverse”, 23 June 2022.
https://euipo.europa.eu/ohimportal/en/news-newsflash/-/asset_publisher/JLOyNNwVxGDF/content/pt-virtual-goods-non-fungible-tokens-and-the-metaverse

Brittan Heller's Human Rights Perspectives" Voices of VR Podcast. 8 April 2021: https://voicesofvr.com/988-defining-biometric-psychography-to-fill-gaps-in-privacy-law-to-cover-xr-data-brittan-hellers-human-rights-perspectives/.

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

IEEE SA IEEE P2048: Standard for Metaverse, Terminology, definitions and taxonomy: https://sagroups.ieee.org/2048/.

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

IEEE SA (2022a), Ethical considerations of Extended Reality (XR): https://standards.ieee.org/beyond-standards/industry/technology-industry/ethical-considerations-of-extended-reality-xr/.

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

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

The collaborative report by the Council of Europe and the IEEE Standards Association, aims at aiding 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 a human rights, rule of law and democracy driven approach to technology development, acknowledging the uncertainty of the metaverse's future evolution.

IEEE (Institute of Electrical and Electronics Engineers) and its members inspire a global community to innovate for a better tomorrow through highly cited publications, conferences, technology standards, and professional and educational activities. IEEE is the trusted "voice" for engineering, computing, and technology information around the globe.

www.ieee.org

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.

www.coe.int

IEEE
Advancing Technology for Humanity

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE