Background document

INPUT FOR THE GLOBAL MULTISTAKEHOLDER HIGH LEVEL CONFERENCE ON GOVERNANCE FOR WEB 4.0 AND VIRTUAL WORLDS, 31 MARCH – 1 APRIL 2025

WEB4HUB: 'A SPACE FOR THE METAVERSE –VIRTUAL WORLD AND THE TRANSITION TO WEB 4.0'

European Commission
PPMi
Part of the Verian Group
TNO
WEB4HUB

Authors: Egidijus Barcevičius (PPMI); Ekaterina Bobrovnikova (PPMI); Ming Chen (TNO); Laura Danielle (TNO); Oskar van Deventer (TNO); Simon Gunkel (TNO); Rūta Gabaliņa (PPMI); Barbora Kudzmanaitė (PPMI); Tom De Koninck (TNO); Aiym Sarmanova (PPMI); Teun van der Veen (TNO); Cristobal Vinagre (TNO); Aleksandra Wójtowicz (PPMI); Aida Zepcan (PPMI); Piotr Zuraniewski (TNO).

Language editor: James Nixon

TABLE OF CONTENTS

TABLE OF FIGURES

List of abbreviations

3D	three-dimensional
3GPP	3rd Generation Partnership Project
5G	fifth-generation mobile network technology
6G	sixth-generation mobile network technology
AGV	automated guided vehicle
AI	artificial intelligence
AIaaS	AI-as-a-Service
AINEMA	Artificial Intelligence Framework for Network Management
ALAC	At-Large Advisory Committee
APNIC	Asia Pacific Network Information Centre
AR	augmented reality
ARIN	American Registry for Internet Numbers
ASMR	autonomous sensory meridian response
ASO	Address Supporting Organisation
ATU	African Telecommunications Union
AWS	Amazon Web Services
BCI	brain–computer interface
CAGR	compound annual growth rate
CcNSO	Country code Names Supporting Organisation
CCPA	California Consumer Privacy Act
CoAP	Constrained Application Protocol
CSAM	child sexual abuse material
CSO	civil society organization
DID	decentralised identifier
DLSS	Deep Learning Super Sampling
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DPP	Digital Product Passport
DTI	digital trust infrastructure
dWeb	decentralised web
EDA	electrodermal activity
EEG	Electroencephalography
eMBB	enhanced mobile broadband

EPREL	European Product Registry for Energy Labelling
ESPR	Ecodesign for Sustainable Products Regulation
ETSI	European Telecommunications Standards Institute
EU	European Union
EUDI	European Digital Identity
EuroDIG	European Dialogue on Internet Governance
EuroQCI	European Quantum Communication Initiative
FG-MV	Focus Group on Metaverse
FMRI	functional magnetic resonance imaging
FNIRS	functional near-infrared spectroscopy
GAN	generative adversarial network
GDC	Global Digital Compact
GDPR	General Data Protection Regulation
genAI	generative artificial intelligence
GNSO	Generic Names Supporting Organisation
GPT	generative pre-trained transformer
HTTPS	Hypertext Transfer Protocol Secure
IAB	Internet Architecture Board
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	information and communications technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IERC	European Research Cluster on the Internet of Things
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IIoT	industrial Internet of Things
IMT	International Mobile Telecommunications
INTERPOL	International Criminal Police Organization
IoT	Internet of Things
IP	Internet Protocol
IPv6	Internet Protocol version 6
IRTF	Internet Research Task Force
ISAC	Integrated Sensing and Communication
ISO	International Organization for Standardisation
ITU	International Telecommunication Union

ITU-R	ITU Radiocommunication Sector
ITU-T	Telecommunication Standardisation Sector
LACNIC	Latin America and Caribbean Network Information Centre
LEO	low Earth orbit
LLM	large language model
MEG	magneto-encephalography
MICG	Multistakeholder Internet Cooperation Group
ML	machine learning
MLOps	machine learning operations
mMTC	Massive Machine-Type Communications
MQTT	Message Queuing Telemetry Transport
MR	mixed reality
MWh	megawatt hour
NFT	non-fungible token
NGO	non-governmental organization
NIST	National Institute of Standards and Technology
NLP	natural language processing
NTN	non-terrestrial networks
OECD	Organisation for Economic Co-operation and Development
OpenXR	open standard for accessing virtual and augmented reality platforms
OWL	Web Ontology Language
PET	privacy-enhancing technologies
PIPL	Personal Information Protection Law
PKI	Public Key Infrastructure
PNIF	Policy Network on Internet Fragmentation
PQC	post-quantum cryptography
QKD	quantum key distribution
RDF	Resource Description Framework
RFC	request for comments
RIPE NCC	Réseaux IP Européens Network Coordination Centre
RIR	regional internet registry
SAREF	Smart Applications REFerence ontology
SDO	standards development organization
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TSAG	Telecommunication Standardisation Advisory Group

UAV	unmanned aerial vehicle
UN	United Nations
VC	verifiable credentials
VR	virtual reality
W3C	World Wide Web Consortium
WSIS	World Summit on the Information Society
XR	extended reality

1. Introduction

This background document provides factual information and a detailed analysis of the technologies underpinning Web 4.0 and virtual worlds, along with the related challenges, needs and governance implications. The document supports the 'Input Document for the Conference based on Stakeholder consultation', which will be presented and discussed during the Global Multistakeholder High Level Conference on Governance for Web 4.0 and Virtual Worlds, hosted by the European Commission and the Polish Presidency of the Council of the European Union on 31 March–1 April 2025. The analysis presented in this document draws on extensive analysis of literature as well as expert interviews, workshops and online consultation (Annex 1).

In February and April 2023, the European Commission organised a "Citizens Panel on Virtual Worlds, which consisted of around 150 randomly selected citizens from all EU Member States. The panel formulated 23 specific recommendations on various aspects of virtual worlds[1]. Later in 2023, the European Commission published its **Strategy for Virtual Worlds and Web 4.0[2]**. The fourth pillar of this strategy focuses on the importance of promoting and facilitating open and robust global governance. This paper has been prepared as a follow-up to the recommendations of the Citizens' Panel and Action 9 of the Strategy for Virtual Worlds and Web 4.0, which foresees the engagement of "existing multi-stakeholder internet governance institutions to design open and interoperable virtual worlds" and support for the "creation of a technical multi-stakeholder forum to address certain aspects of virtual worlds and Web 4.0".

Aside from the work carried out by the European Commission, some countries have adopted **national strategies** that address Web 4.0 and virtual worlds. A notable example is Japan's 'Principles of the Metaverse', which describe the principles and elements for a metaverse that adheres to democratic values and ensures safety and security, self-motivated and autonomous development and trustworthiness[3]. South Korea's metaverse strategy focuses on developing the country's metaverse ecosystem, nurturing local talent, and establishing ethical principles for safe virtual environments[4]. Finland, a first mover in Europe, has collaborated with actors in its domestic ecosystem to create a metaverse strategy that emphasises good governance, predictability and continuity[5].

This paper reiterates the importance of the current internet governance framework and key declarations and initiatives, including:

- the **World Summit on the Information Society** (WSIS),[6] a United Nations (UN) summit on information, communication and the information society, which resulted in the adoption of the Declaration of Principles in 2003 in Geneva[7], and the **Tunis Agenda** for the Information Society in 2005[8];
- **NETmundial**, which took place in São Paulo, Brazil in April 2014 and resulted in a non-binding multistakeholder statement containing principles and a roadmap for cooperation and the governance of the internet. In a statement, NETmundial +10, held in 2024, reiterated the need to build an effective and functioning multistakeholder

1 Available at: https://citizens.ec.europa.eu/virtual-worlds-panel_en
2 European Commission (2023). An EU initiative on virtual worlds: a head start in the next technological transition. Available at: https://digital-strategy.ec.europa.eu/en/library/eu-initiative-virtual-worlds-head-start-next-technological-transition
3 More information is available at: https://www.soumu.go.jp/main_content/000975017.pdf
4 Ministry of Science and ICT (2021). *MSIT unveils strategies to lead the global metaverse market*. Available at: https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=621&searchOpt=ALL&searchTxt=
5 Business Finland (2023). *Metaverse Initiative by the Finnish Ecosystem*. Available at: https://www.digitalfinland.org/
6 By extension, also the 2015 WSIS+10 process, as well as the upcoming WSIS+20 review.
7 Available at: https://www.itu.int/net/wsis/docs/geneva/official/dop.html
8 Available at: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

governance architecture that facilitates informed, participatory and transparent engagement between sectors, through a multistakeholder approach[9];

- the **Global Digital Compact**[10] **(GDC),** adopted in September 2024 at the Summit of the Future, which contains principles for an "open, free and secure digital future for all" that build on consultations with governments.

Existing internet governance institutions and standards development organisations (SDOs) have already engaged with various aspects of Web 4.0 and virtual worlds. Several discussions have been held at the IGF, including on the protection of democratic values[11] and children in the metaverse[12] and on the governance of Web 4.0 and virtual worlds[13]. The 2023 edition of EuroDIG also included a focus on virtual worlds and their associated risks[14].

The Focus Group on metaverse (FG-MV) at the International Telecommunication Union (ITU) recently concluded its analysis of the technical requirements for the metaverse[15]. A joint ISO/ IEC working group[16] also explores the standardisation of and opportunities for the metaverse and related technologies. In 2021, the World Wide Web Consortium (W3C) established the MICG group, working on interoperability in the metaverse. The Institute of Electrical and Electronics Engineers (IEEE) Global Initiative on Ethics of Extended Reality has published a number of white papers, including a report, *Metaverse and Its Governance*[17]. Work carried out on standards and interoperability has included initiatives by SDOs (e.g. the Khronos Group, the W3C) as well as non-SDO initiatives such as the Metaverse Standards Forum and Open Metaverse Interoperability Group.

1.1. The evolution of the internet and the web

The **internet** serves as a global infrastructure that connects billions of devices with different technological capabilities, enabling the transfer of data and communication across diverse interconnected networks. It is the foundation for countless applications and services, including the World Wide Web (WWW), email, streaming, cloud storage and collaboration tools.

Since its commercialisation in the 1990s, the internet has increased in scale to include billions of connected devices, building on continuous advances in bandwidth, encryption protocols and network architecture. Fundamental building blocks of the internet such as the Transmission Control Protocol/Internet Protocol (TCP/IP) stack and the Domain Name System (DNS) have proven remarkably resilient and adaptable.

While the internet exists as a global system of networks, hardware, standards and protocols that enable global connectivity, **the web represents the content-rich, user-facing layer** on which people access information, communicate and interact. Together, the above elements form the backbone of modern digital life.

This section describes the evolution of the web from Web 1.0 to Web 4.0. It discusses the various definitions of Web 4.0, and presents the definition used in this paper. Lastly, it also discusses the relevance of Web 4.0 to the internet and its governance.

---

9 Available at https://netmundial.br/
10 Available at: https://www.un.org/techenvoy/global-digital-compact
11 IGF (2023). IGF 2023 Day 0 Event #207 Pursuing a metaverse based on democratic values. Available at: https://www.intgovforum.org/en/content/igf-2023-day-0-event-207-pursuing-a-metaverse-based-on-democratic-values
12 IGF (2024). IGF 2024 WS #14 Children in the Metaverse. Available at: https://intgovforum.org/en/content/igf-2024-ws-14-children-in-the-metaverse
13 In the context of the Global Multistakeholder High Level Conference on Governance for Web 4.0 and Virtual Worlds, hosted by the European Commission and the Polish Presidency of the Council on 31 March–1 April 2025, the IGF (2024) session, 'Governing the Future Internet The 2025 Web 4 0 Conference'
14 Key messages available at: https://comment.eurodig.org/eurodig-2023-messages/main-topic-3-digital-platforms/subtopic-1-virtual-worlds-but-real-risks-navigating-metaverses-as-a-next-generation-of-digital-platform
15 https://standict.eu/success-stories/accessibility-metaverse-itu-t-focus-group-metaverse-fg-mv
16 https://iec.ch/dyn/www/f?p=103:186:20055352492236 8::::FSP_ORG_ID,FSP_LANG_ID:43649
17 https://sagroups.ieee.org/ic20-016/

1.1.1. Evolution of the web

The web has evolved through distinct phases, each marked by technological breakthroughs that have paved the way for ever richer user experiences. The evolution from static hyperlinked pages to today's dynamic web applications has progressively enhanced interactivity and enabled intuitive and immersive experiences. Figure 1 presents a simplified definition of Web 1.0, 2.0, 3.0 and 4.0. It should be noted that these do not represent distinct 'versions' of the web, which is evolving continuously, but instead characterise broad trends in services[18]. Thus, when this paper refers to "version" numbers (i.e. Web x.0) it does not refer to versioning in the same sense that software is versioned.

Figure 1. Evolution of the web from Web 1.0 to Web 4.0

Source: European Commission (2023)[19], Hupont Torres et al (2023)[20].

In this simplified understanding of the evolution of the web, **Web 1.0** is typically presented as static and read-only, based on the HTML protocol that allowed documents to be linked. **Web 2.0** introduced two-way communication and enabled all users to become content and/or service providers. The key elements of **Web 3.0** are user control, user ownership, openness and decentralisation. Defined by the W3C as the "semantic web" or the "web of data"[21], Web 3.0 is based on linking data rather than whole documents and making web data machine-readable. Growing concerns about the apparent centralisation of the internet and platform control over user-generated content have catalysed the development of decentralised web architectures, known as Web3 or dWeb[22]. It envisions a web in which users have control over their own data, identities and online interactions, without relying on intermediaries. This decentralised web relies on blockchain technology and tokenisation[19].

Web 4.0 is seen by some authors as the likely future evolution of the web, whereby the digital and physical worlds merge seamlessly and in which advanced artificial intelligence (AI), the Internet of Things (IoT) and immersive technologies seamlessly integrate digital and physical environments. This will enable intuitive and immersive experiences in which real and virtual objects communicate and interact with each other in real time, forming a highly interconnected ecosystem. Web 4.0 goes beyond

---

18 W3C (2024). The web is unversioned, Available at: https://www.w3.org/2001/tag/doc/the-web-is-unversioned/

19 European Commission (2023). SWD (2023) 250 final: An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition. COM (2023) 442 final. Available at: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-information-insights-and-market-trends-web-40-and-virtual-worlds

20 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., & Vespe, M. (2023). Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU, Publications Office of the European Union, Luxembourg, doi:10.2760/51579, JRC133757. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC133757

21 World Wide Web Consortium (W3C) (no date). Semantic Web. W3C. Available at: https://www.w3.org/2001/sw/wiki/Main_Page

22 Zarrin, J., Wen Phang, H., Babu Saheer, L., & Zarrin, B. (2021, 15 May). Blockchain for decentralization of internet: prospects, trends, and challenges. *Cluster Computing*, 24 (4): 2841-2866.Available at: https://link.springer.com/article/10.1007/s10586-021-03301-8

current capabilities by seamlessly integrating the physical and digital worlds to deliver personalised, intuitive and immersive experiences[19,20]. The various definitions of Web 4.0 are discussed in more detail in the next section.

1.1.2. Defining Web 4.0

The concept of Web 4.0 **is still evolving**. Previously, the term "Web 4.0" has been used to describe development towards an "Ultra-Intelligent Electronic Agent", whereby the web would mirror human brain functions to facilitate highly intelligent interactions between humans and machines. The underlying idea behind this definition is that Web 4.0 would transcend the current capabilities of the internet by enabling machines to understand and anticipate users' needs using advanced artificial intelligence[23]. Alternative terms used for the future web include the "intelligent web", "symbiotic web" and "symbiotic interaction web", all of which highlight the immersive and interactive experiences that result from blending real and virtual worlds. In this understanding of Web 4.0, it comprises fully integrated and intelligent systems that form a symbiotic relationship between users, physical and digital objects. Thus, Web 4.0 would mark a major shift for users, extending beyond visual user interfaces to engage all human senses and communication methods. Gesture and voice control, tactile feedback and brain–computer interfaces (BCIs) redefine the ways in which users experience the web. Other scholars have characterised Web 4.0 as a pivotal advancement for industrial sectors in terms of automation, robotics, the integration of connectivity, and machine-to-machine communication, highlighting its capacity to enhance operational efficiency[24].

Similarly, in the stakeholder interviews conducted during the preparation of this paper, interviewees generally pointed out that Web 4.0 lacks a common definition. Nonetheless, most interviewees agreed that Web 4.0 technologies primarily represent the convergence of multiple emerging technologies, including virtual worlds and XR experiences, ambient intelligence, IoT and the seamless blending of the physical and digital worlds.

In this paper, we use the following definition from the European Commission, which integrates key elements of the various definitions outlined above[25]:

Using advanced artificial and ambient intelligence, the internet of things, trusted blockchain transactions, virtual worlds and XR capabilities, digital and real objects and environments are fully integrated and communicate with each other, enabling truly intuitive, immersive experiences, seamlessly blending the physical and digital worlds.

The technological building blocks underpinning Web 4.0 include AI; IoT; extended reality (XR); future communication networks (including 5G/6G); digital trust technologies such as blockchain, decentralised identity, privacy-enhancing technologies, and cybersecurity; BCIs and quantum technologies.

Moreover, the impact of these technologies extends beyond the application interface of the internet, influencing the fundamental networking systems and the internet architecture that underpins Web 4.0. Next-generation networks, boosted by non-terrestrial networks and AI-optimised resource management, promise enhanced resilience as well as readiness for high bandwidth and low latency –

[23] Choudhury, N. (2014). World Wide Web and its journey from Web 1.0 to Web 4.0. *International Journal of Computer Science and Information Technologies, 5*(6), 8096-8100. Available at: https://ijcsit.com/docs/Volume%205/vol5issue06/ijcsit20140506265.pdf

[24] Kollmann, T. (Ed.). (2020). Grundlagen des Web 1.0, Web 2.0, Web 3.0 und Web 4.0. *Handbuch Digitale Wirtschaft*, pp. 133-155. Available at: https://www.springerprofessional.de/grundlagen-des-web-1-0-web-2-0-web-3-0-und-web-4-0/18674050

[25] COM(2023) 442/final. Communication From the Commission to The European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition. Strasbourg, 11 July 2023. Available at : https://digital-strategy.ec.europa.eu/en/library/eu-initiative-virtual-worlds-head-start-next-technological-transition

requirements that are crucial for real-time XR applications. Quantum internet technologies are prompting discussions on ultra-secure communication, while AI-driven routing aims to optimise traffic via dynamic network responses. Blockchain-based identifiers are emerging as decentralised frameworks for new services. Meanwhile, the demand for immersive technologies is driving advances in edge computing and next-generation networks such as 6G.

These technologies, while distinct, are deeply interconnected, forming the foundation of an intelligent and immersive ecosystem. Their individual contributions and mutual dependencies are further explored in Chapter 2 of this paper, which details their role in shaping Web 4.0 It is also important to **distinguish Web 4.0 from virtual worlds and the metaverse.** While the latter contribute to immersive digital experiences, they represent specific environments and applications.

Virtual worlds are a significant part of the evolution to Web 4.0, providing a medium for personalised and immersive user experiences in 3D environments. In line with the European Commission's definition, virtual worlds are *"*persistent, immersive environments, based on technologies including 3D and extended reality (XR), which make it possible to blend physical and digital worlds in real time*"*[26]. These worlds offer opportunities for innovative applications in social interaction, commerce, education, entertainment and public services. The integration of AI and XR technologies within these virtual environments enables more dynamic and adaptive user experiences, blurring the lines between the physical and digital worlds[27,28]. It is worth noting that the European Commission's definition of virtual worlds is relatively broad, while some authors define them more narrowly. For example, an ongoing scoping review conducted by the JRC defines it as a 3D spatial environment in which users are represented and can interact with others and perform various activities in real time[29]. Nevertheless, whether based on narrow and broad definitions, virtual worlds will contribute to the immersive experiences envisioned in Web 4.0. However, these experiences are distinct as standalone, persistent environments that blend physical and digital realities without necessarily encompassing the full intelligent integration and interconnectedness that are characteristic of Web 4.0.

As an evolving vision for the future rather than an observable phenomenon[30,31], **the metaverse** has multiple definitions, but most of these share a common theme: the link between real and virtual worlds. The European Commission defines it as "interoperable network" of virtual worlds[27]. As such, like virtual worlds, the metaverse is a concept that is interrelated with but distinct from Web 4.0. The World Economic Forum describes the metaverse as a persistent and interconnected virtual environment in which social and economic elements mirror reality[32]. Similarly, the OECD defines the metaverse as immersive environments based on extended reality (XR) technologies, which enhance the realism of virtual experiences and blur the boundaries between the physical and digital worlds[33].

---

26 COM(2023) 442/final. Communication From the Commission to The European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition. Strasbourg, 11 July 2023. Available at: https://digital-strategy.ec.europa.eu/en/library/eu-initiative-virtual-worlds-head-start-next-technological-transition

27 European Commission (2023). SWD(2023) 250 final: An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition. COM (2023) 442 final. Available at: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-information-insights-and-market-trends-web-40-and-virtual-worlds

28 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., & Vespe, M. (2023). Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU, Publications Office of the European Union, Luxembourg, doi:10.2760/51579, JRC133757. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC133757

29 Barreda Angeles, M., Hupont Torres, I., Hartmann, T., Coecke, S., Panzarella, G., Villar Onrubia, D., Meier, A., & Mansfield, K. (2025). Scoping Review Protocol: Virtual Worlds and Mental Health, European Commission, Brussels, JRC140069. European Commission: Joint Research Centre.

30 Weinberger, M. (2022). What Is Metaverse? – A Definition Based on Qualitative Meta-Synthesis. *Future Internet*, 14(11), 310. Available at: https://doi.org/10.3390/fi14110310

31 Smethurst, R., Barbereau, T., & Nilsson, J. (2023). The Metaverse's Thirtieth Anniversary: From a Science-Fictional Concept to the "Connect Wallet" Prompt. *Philosophy & Technology*, 36(3). https://doi.org/10.1007/s13347-023-00612-z

32 World Economic Forum (2023, January). Defining and building the metaverse – Davos 2023. World Economic Forum. Available at: https://www.weforum.org/stories/2023/01/defining-and-building-the-metaverse-davos-2023/

33 Organisation for Economic Co-operation and Development (OECD) (2024). *Harnessing the power of AI and emerging technologies - background paper for the CDEP Ministerial meeting*. OECD Publishing. Available at: https://www.oecd.org/en/publications/harnessing-the-power-of-ai-and-emerging-technologies_f94df8ec-en.html

1.1.3. Relevance of Web 4.0 to the internet and its governance

The impact of these technologies extends beyond the application layer of the internet, potentially influencing the fundamental **networking systems and the architecture of the internet**. For example, next-generation networks, enhanced by technologies such as non-terrestrial networks and AI-optimised resource management, will make the internet more resilient, adaptive and ready for the high-bandwidth, low-latency transmission that is required for real-time, virtual or augmented reality applications. The potential of quantum internet technologies to enable ultra-secure communication through quantum key distribution (QKD) has triggered debates and research as well as the exploration of standards to adapt existing protocols to quantum-compatible data flows. Similarly, AI-driven routing is being discussed for its ability to optimise traffic management through dynamic, predictive responses to network conditions[34,35]. Blockchain-based identifiers are already being used as decentralised frameworks to power new applications and services[36,37]. Immersive technologies, with their demand for high-resolution graphics and real-time interactions, have prompted advances in edge computing and next-generation networks including 6G[38,39]. Together, these developments highlight the intricate relationship between Web 4.0 technologies and the internet's foundational architecture. These are just some examples of how Web 4.0 could influence the internet (for further details, see Chapter 2).

In order for Web 4.0 technologies to be acceptable to users and society in the long term, it is crucial to effectively address societal aspects such as inclusiveness, sustainability, human rights and trustworthiness in terms of privacy, the integrity of data, and security. In turn, the challenges and needs that emerge from the evolution of Web 4.0 and virtual worlds must be considered from a **technical** perspective, as well as from the perspectives of **end users and society**. For example, the continued existence of an open, distributed and interoperable Web 4.0 **could be put at risk** by the emergence of "splinternets", non-interoperable app ecosystems, a lack of interoperability between virtual worlds and threats to net neutrality, as further elaborated in Section 3.1. Moreover, the evolution of Web 4.0 and virtual worlds could also amplify digital divides: access to and the ability to benefit from advanced technologies such as quantum computing, AI and next-generation networks might be limited to those with the necessary infrastructure, technical expertise and financial resources. The consequent surge in generation of data and an expansion in the collection of highly sensitive data (such as neurological and behavioural data), amplifies concerns over the safeguarding of privacy, as well as ensuring the ethical use of data and the protection of human rights. The potential of quantum computing to break encryption makes it essential to develop new security standards. These and other challenges and needs are further elaborated in Chapter 3 of this document. Together, these **challenges** underscore the unprecedentedly complex relationship between Web 4.0 technologies and the internet's foundational architecture, spanning both technical frameworks and policy principles.

Lastly, Web 4.0 and virtual worlds are likely to introduce new challenges for **internet governance** itself. Global internet governance[40] is a fairly stable yet evolving environment, with established global

34 ITU-R M.2160-0 - Framework and overall objectives of the future development of IMT for 2030 and beyond. https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2160-0-202311-I%21%21PDF-E.pdf
35 Umoga, U.J., Sodiya, E.O., Ugwuanyi, E.D., Jacks, B.S., Lottu, O.A., Daraojimba, O.D., & Obaigbena, A. (2024). Exploring the potential of AI-driven optimization in enhancing network performance and efficiency. *Magna Scientia Advanced Research and Reviews*, 10(1), 368-378. https://magnascientiapub.com/journals/msarr/sites/default/files/MSARR-2024-0028.pdf
36 World Wide Web Consortium (2022). Decentralized identifiers (DIDs) v1.0 (W3C Recommendation). Available at: https://www.w3.org/TR/did-core/
37 International Organization for Standardization. (no date). ISO/TC 307 – Blockchain and distributed ledger technologies. Available at: https://www.iso.org/committee/6266604.html
38 Metaverse Standards Forum. (no date). Domain groups. Available at: https://metaverse-standards.org/domain-groups/
39 International Telecommunication Union. (2023). Towards a secure and inclusive Metaverse: Standardization challenges and opportunities. *ITU Journal on Future and Evolving Technologies*, 4(4), Article 43. Available at: https://www.itu.int/pub/S-JNL-VOL4.ISSUE4-2023-A43
40 Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet (Tunis Agenda for the Information Society).

institutions and a strong anchor in a multistakeholder approach. This approach will be central in responding to the new challenges raised by Web 4.0 and virtual worlds in terms of privacy, security, interoperability, ethical and geopolitical issues. Such issues that can sometimes span multiple layers of traditional governance and institutional mandates. Early efforts at research and standardisation have been undertaken to address some of these challenges[41]. However, it is also important to ensure that the evolution of Web 4.0 and virtual worlds does not create risks of the fragmentation of internet governance as a result of discussions and initiatives being siloed and responses to emerging issues being insufficient coordinated. The specific challenges to internet governance posed by the evolution of Web 4.0 and virtual worlds are discussed further in Chapter 4.

1.2. Structure of the present document

This document consists of the following chapters:

- **Chapter 2** presents the technology clusters that underpin the development of Web 4.0. These include AI, IoT, 5G/6G and future communication networks, immersive technologies, brain–computer interfaces, digital trust infrastructure and quantum computing.
- **Chapter 3** analyses the needs and challenges to internet governance in relation to the evolution towards Web 4.0 and virtual worlds. The topics covered include an open and distributed and interoperable Web 4.0; security; privacy and data protection; ethics; safety and respect for human rights; sustainability; economic challenges; and accessibility.
- **Chapter 4** discusses the implications for current internet governance of the evolution towards Web 4.0 and virtual worlds.
- The **Annex** to this paper describes the methodology used for the stakeholder consultation, and introduces the key insights.

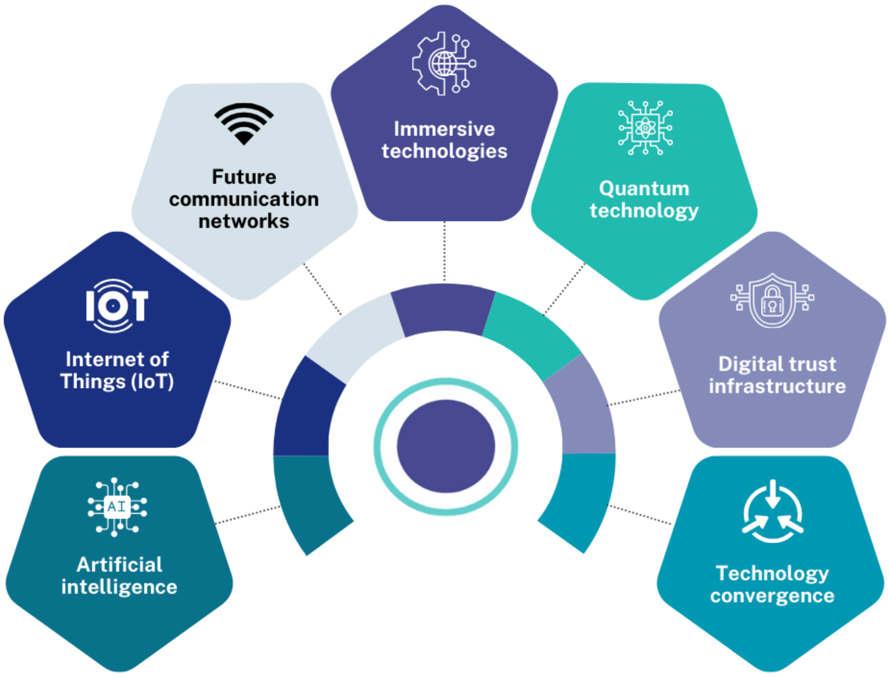
[41] For example, organisations such as the Internet Engineering Task Force (IETF), the International Telecommunications Union (ITU) and the World Wide Web Consortium (W3C) are exploring quantum-ready protocols, AI-enhanced networking standards and frameworks for integrating distributed systems. Discussions within global multistakeholder institutions such as the Internet Governance Forum reflect growing recognition of these issues.

2.Technology clusters

The evolution towards Web 4.0 is driven by the convergence of several digital technologies, each of which will play a crucial role in shaping the next generation of the internet and the web. This chapter explores the principal technology clusters that underpin Web 4.0, focusing on their characteristics, interdependencies and implications for governance.

These technology clusters include artificial intelligence (AI), the Internet of Things (IoT), immersive technologies (XR), future communication networks (including 5G/6G), digital trust technologies (such as blockchain, decentralised identity, privacy-enhancing technologies and cybersecurity), brain-computer interfaces and quantum technologies (see the figure below). These clusters have been identified on the basis of an assessment of emerging digital trends[42,43], as well as through consultations with experts and stakeholders[44] involved in this research.

Figure 2. Web 4.0 technology clusters



Rather than providing an exhaustive list of every relevant technology, this chapter highlights the major technological enablers that will define Web 4.0's structure and functionality. Given the rapid pace of digital innovation, new technologies will continue to emerge, and existing ones will evolve in

[42] European Commission (2023). Commission Staff Working Document accompanying the Communication on an EU initiative on Web 4.0 and virtual worlds: A head start in the next technological transition (SWD(2023) 250 final). Publications Office of the European Union, Luxembourg. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023DC0442

[43] ETSI (2021). ETSI Technology Radar (White Paper No. 45). European Telecommunications Standards Institute. Available at: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp45_ETSI_technology_radar.pdf

[44] Online consultation: when asked about the most critical technology clusters for Web 4.0 and virtual worlds, 42 out of 70 respondents (60.0 %) highlighted AI and natural language processing (NLP) as the most essential. Virtual reality (VR) and augmented reality (AR) were selected by 28 out of 70 respondents (40.0 %), while 26 out of 70 (37.1 %) pointed to the Internet of Things (IoT) and ambient intelligence. Next-generation networks (5G and 6G) and spatial computing were each identified by 17 out of 70 respondents (24.3 %). Meanwhile, multisensory modalities, including haptics, were considered critical by only 4 out of 70 respondents (5.7 %), and the same proportion selected other technology clusters such as digital twins and wallets

unpredictable ways. Furthermore, the boundaries between these clusters are fluid, as technologies within each category are deeply interconnected, reinforcing and amplifying one another's impact.

The sections that follow provide an overview of each cluster. Particular attention is given to their mutual dependencies, their potential to optimise the performance of the internet, and the societal challenges they introduce. The implications of convergence between these clusters are discussed in the final section of this chapter, as interactions between different technologies are likely to generate opportunities and challenges that extend beyond individual clusters.

2.1. Artificial intelligence

AI is a core enabler of **Web 4.0**, driving automation, personalisation, and real-time decision-making across decentralised and immersive digital ecosystems. AI technologies such as machine learning (ML), deep learning, natural language processing (NLP) and generative AI are redefining how users interact with digital services, information and infrastructure. The usage of AI extends beyond enhancing user experiences; it is also transforming the underlying architecture of the web, influencing network operations, cybersecurity, content generation and data-driven decision making.

AI **is an umbrella term** that covers a wide range of transformative technologies including different types of machine learning (ML). The overall rationale for AI is to simulate human-like intelligence, enabling functionalities such as NLP, speech recognition, decision-making and problem-solving. ML, a subset of AI, focuses on developing algorithms that allow systems to learn autonomously from data and to improve their performance iteratively. Together, these technologies are reshaping sectors ranging from healthcare to finance by powering recommendation systems, fraud detection mechanisms, and predictive analytics. Furthermore, while most currently available (gen)AI solutions focus on dedicated tasks or are best in class for a specific task, current efforts are also being made to develop general-purpose AI solutions[45].

Analysis by NASDAQ points out that "competition in the AI sector escalated dramatically in 2024, with major tech companies investing billions in a race to research and develop advanced AI technologies"[46]. Further, the global AI market is expected to grow significantly, with projections estimating a market size of up to USD 990 billion by 2027[47] [48].

Generative AI (genAI), a subset of AI, uses various techniques to produce human-like content. Most current genAI approaches rely on transformer-based deep neural networks technology, the roots of which can be traced back to early research in 1943[49]. Since then, the technology has advanced[50] into powerful prediction and "reasoning" models. Large language models (LLMs), trained on extensive datasets, are able to generate textual output of various types including fiction, poems or essays, as well as pieces of text that resemble news items or scientific articles in terms of style, but which may or may not be factually correct. LLMs are frequently used to power chatbot applications that allow users to engage in an interactive dialogue with machines. For instance, models such as OpenAI's GPT

45 Triguero, I., Molina, D., Poyatos, J., Del Ser, J., & Herrera, F. (2024). General Purpose Artificial Intelligence Systems (GPAIS): Properties, definition, taxonomy, societal implications and responsible governance. *Information Fusion*, 103, 102135. Available at: https://www.sciencedirect.com/science/article/pii/S1566253523004517

46 Nasdaq. (2024). *AI Market 2024 Year-End Review*, Nasdaq. Available at: https://www.nasdaq.com/articles/ai-market-2024-year-end-review

47 Bain & Company. (2024). AI's Trillion-Dollar Opportunity – Tech Report 2024. Bain & Company. Available at: https://www.bain.com/insights/ais-trillion-dollar-opportunity-tech-report-2024/

48 Grand View Research. (2024). Artificial Intelligence (AI) Market Analysis. Grand View Research. Available at: https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-ai-market

49 McCulloch, W.S., & Pitts, W. (1943). A Logical Calculus of the Ideas Immanent in Nervous Activity. *Bulletin of Mathematical Biophysics*, 5(4), 115–133. Available at : https://link.springer.com/article/10.1007/BF02478259

50 Maslej, N., et al. (2024). *Artificial Intelligence Index Report 2024*. arXiv preprint arXiv:2405.19522. Available at: https://arxiv.org/abs/2405.19522

family, Google's Gemini and Anthropic's Claude are advancing digital interactions by mimicking human conversation and creativity[51,52].

Aside from text, generative AI systems are able to produce images. These can range from imaginative "drawings" up to photorealistic images. Popular platforms such as DALL-E[53] and Midjourney[54] allow users to interact with the system by typing commands. While image generation systems can be coupled with a chatbot, the actual image generating technology is not based on an LLM but on other architecture such as generative adversarial networks (GANs) or variational autoencoders (VAEs). It is important to note that AI is also applicability more widely in computer processing (e.g. deep learning super sampling, DLSS, in gaming[55]), compression techniques and other technologies. Moreover, video generation (e.g. Sora[56] or Runway[57]) and audio generation (e.g. Suno[58]) are among the capabilities of the modern genAI platforms. This technology is a cornerstone of the shift towards multimodal, hyper-personalised user experiences and the automation of creative processes[59]. Such hyper-personalisation, which can include 3D assets, is directly related to new developments in immersive technology.

Presently, a **fragmentation in the AI landscape** can be observed, with many individual services being "best in class" for highly specific tasks, possibly trained and functioning in isolation. This fragmentation creates a strong need for interoperability. This can be achieved through decentralised frameworks, which enable dynamic interactions and personalised user experiences[60]. Different AI models are used together to enhance resilience and consistency, employing techniques such as automated machine learning (AutoML) and continuous retraining pipelines to maintain high-quality performance in the face of changing data patterns[61]. This collaborative approach not only improves the robustness of AI systems but also ensures their reliability and security in complex environments[62]. The **integration of AI agents**, and the establishment of hierarchies between them, are likely as part of the future Web 4.0. In this future, high-level agents would oversee strategic objectives, delegating tasks to lower-level agents, thereby ensuring efficient task management and adaptability[63].

The increasing use of AI is prominent at lower layers of the **internet and internet infrastructure** (cloud, 5G/6G), and the need for this technology will grow further as a result of the evolution towards Web 4.0. From the design phase onwards, chatbots can be used as "sparring partners" to refine ideas surrounding the business goals of a newly proposed network service[64] or a high-level deployment plan.

---

51 Brown, T., Mann, B., Ryder, N., Subbiah, M., Kaplan, J.D., Dhariwal, P., ... & Amodei, D. (2020). Language models are few-shot learners. *Advances in Neural Information Processing Systems*, 33, 1877-1901. Available at: https://proceedings.neurips.cc/paper/2020/hash/1457c0d6bfcb4967418bfb8ac142f64a-Abstract.html.https://proceedings.neurips.cc/paper/2020/hash/1457c0d6bfcb4967418bfb8ac142f64a-Abstract.html

52 Thoppilan, R., De Freitas, D., Hall, J., Shazeer, N., Kulshreshtha, A., Cheng, H.T., ... & Le, Q. (2022). *LaMDA: Language models for dialog applications*. arXiv preprint arXiv:2201.08239. Available at: https://arxiv.org/pdf/2201.08239.pdf

53 OpenAI (2024). *DALL·E 3 AI Image Generation*. Available at: https://openai.com/index/dall-e-3/

54 Midjourney (no date). Midjourney AI Image Generation. Available at: https://www.midjourney.com/home

55 Zhou, H. (2024, October). The role of AI in revolutionizing the gaming industry: A focus on DLSS and large language models. In 2024 2nd International Conference on Image, Algorithms and Artificial Intelligence (ICIAAI 2024), pp. 939-949. Atlantis Press. Available at: https://www.atlantis-press.com/proceedings/iciaai-24/126004170

56 OpenAI (2024). Sora: AI video generation. Available at: https://openai.com/sora/

57 Runway ML (2024). Runway: AI video generation. Available at: https://runwayml.com/

58 Suno (2024). Suno AI: AI music generation. Available at: https://suno.com/

59 Forbes Technology Council (2023, 27 December). Navigating the future: The dynamics of hyper-personalization and AI in customer experience. Forbes. Available at: https://www.forbes.com/councils/forbestechcouncil/2023/12/27/navigating-the-future-the-dynamics-of-hyper-personalization-and-ai-in-customer-experience/

60 Rafalski, K. (2024). *Understanding Web 4.0: The Future of an Intelligent Internet*. Netguru. Available at: https://www.netguru.com/blog/web-4-0

61 Forbes Technology Council (2024, 20 December). Building resilient AI systems in the cloud: Lessons from real-world deployments. Forbes. Available at: https://www.forbes.com/councils/forbestechcouncil/2024/12/20/building-resilient-ai-systems-in-the-cloud-lessons-from-real-world-deployments/

62 AI Models (no date). AI governance organizations: Safety and resilience in AI systems. Available at: https://aimodels.org/ai-governance-organizations/safety-resilience-ai-systems/

63 Andre, D. (2025). Hierarchical AI agents: Redefining Task Management in Artificial Intelligence. All About AI. Available at: https://www.allaboutai.com/ai-agents/hierarchical-agents/

64 Bizway (no date). Bizway: Automate & grow your business with a team of AI agents. Available at: https://www.bizway.io/

Code generators – whether generic ones such as Copilot[65], or ones such as Pulumi[66], that power specific Infrastructure such-as-code solutions – can produce software that creates (virtualised) network infrastructures that lay the foundations for advanced and resource-intensive services such as XR. In day-to-day operations, the monitoring of infrastructure and the detection of anomalies or attacks is of great importance[67,68]. Due to the sheer amount of data concerned (e.g. network links capable of transporting hundreds of gigabits per second), several layers of machine processing and intelligent, automatic selection of events are frequently employed before human operator attention is required. Specialists in network and security operation centres can also be assisted by genAI, which can summarise a situation and propose a solution based on collected logs, traces or events[69]. When action is needed – for example, a threat is identified and a new security policy must be created and executed – genAI tools can again offer assistance[70]. Due to the complexity and rapid evolution of threats to network infrastructures, AI can be a key driver for cybersecurity in the future[71]. In conclusion, new AI technologies can create significant impacts in improving the network and resources of Web 4.0, and will consequently also add new requirements for the network itself.

Standards are essential for building reliable AI systems, and will be fundamental to the development of Web 4.0. Efforts such as the W3C's semantic web standards have enabled seamless data sharing and machine understanding on the web. In addition, ethical frameworks such as the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems[72] emphasise fairness, accountability and transparency in the development of AI[73]. The Securing AI Technical Committee of ETSI addresses threats to AI systems and considers measures to mitigate them[74], while NIST promotes a systematic approach to AI risk management[75]. Furthermore, organisations such as the IEEE and NIST are at the forefront of developing standards for AI, focusing on aspects such as transparency, fairness and accountability[76,77]. These standards aim to create a framework that supports the responsible development and deployment of AI systems. Further standardisation work by the IETF has also begun on how AI can be concretely and successfully applied to network management in relation to different services, complex reasoning and event processing – namely, the Artificial Intelligence Framework for Network Management (AINEMA)[78].

Ultimately, AI will achieve widespread penetration into all digital products, thereby introducing new challenges and opportunities for future networks (see Section 2.3) and enabling enhanced, intuitive (more human-like) interactions between humans and machines (see Section 2.4). Moreover, the combination of expanded data collection (including highly sensitive biometric data, see Section 2.2) and AI creates a plethora of new challenges under Web 4.0. Some key concerns in the light of AI development include data control, privacy and ownership rights (see Sections 3.3 and 3.6.3). Moreover,

[65] GitHub (no date). GitHub Copilot: AI-powered code completion. Available at: https://github.com/features/copilot.

[66] Pulumi (no date). Pulumi: Cloud engineering for modern applications. Available at: https://www.pulumi.com/

[67] Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K.K.R. (2022). Artificial intelligence in cybersecurity: Research advances, challenges, and opportunities. *Artificial Intelligence Review*, 55, 1029–1053. Available at: https://link.springer.com/article/10.1007/S10462-021-09976-0

[68] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 97, 101804. Available at: https://doi.org/10.1016/j.inffus.2023.101804

[69] K8sGPT (no date). K8sGPT: AI-powered Kubernetes troubleshooting and optimization. Available at: https://k8sgpt.ai/

[70] Splunk, Inc. (no date). Splunk AI Assistant for SPL. Retrieved from https://www.splunk.com/en_us/products/splunk-ai-assistant-for-spl.html

[71] Sarker, I.H., Furhad, M.H., & Nowrozy, R. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. *SN Computer Science*, 2, 173. Available at: https://doi.org/10.1007/s42979-021-00557-0

[72] IEEE (no date). Ethics in Action: Advancing ethical AI and technology. IEEE. Available at: https://ethicsinaction.ieee.org/

[73] Leikas, J., Koivisto, R., & Gotcheva, N. (2019). Ethical framework for designing autonomous intelligent systems. *Journal of Open Innovation: Technology, Market, and Complexity*, 5(1), 18. Available at: https://www.mdpi.com/2199-8531/5/1/18/pdf

[74] ETSI. (2025, January). ETSI TR 104 221 V1.1.1 – Securing Artificial Intelligence (SAI): Problem Statement. ETSI. Available at: https://www.etsi.org/deliver/etsi_tr/104200_104299/104221/01.01.01_60/tr_104221v010101p.pdf.

[75] NIST (no date). AI Risk Management Framework (AI RMF). NIST. Available at: https://airc.nist.gov/AI_RMF_Knowledge_Base/AI_RMF

[76] IEEE Smart Cities Initiative (2021, August). Standardization of artificial intelligence. IEEE Smart Cities Newsletter. Available at: https://smartcities.ieee.org/newsletter/august-2021/standardization-of-artificial-intelligence

[77] NIST (2024). AI Test, Evaluation, Validation, and Verification (TEVV). NIST. Available at: https://www.nist.gov/ai-test-evaluation-validation-and-verification-tevv.

[78] Martinez-Julia, P., Homma, S., & Lopez, D.R. (2024, 21 October). Artificial Intelligence framework for network management. https://www.ietf.org/archive/id/draft-pedro-nmrg-ai-framework-05.html

the datasets used to train generative AI systems and LLMs are facing scrutiny over their implications for privacy and copyright[79]. AI system design can amplify issues that affect fairness and bias (see also subsection 3.4.63.4.6)[80]. These and other challenges that are relevant to the integration of AI into Web 4.0 are further explored in Chapter 3.

2.2. Internet of Things

The Internet of Things (IoT) **is a key enabler of Web 4.0**, facilitating seamless interaction between physical and digital environments. By connecting together billions of devices, sensors and systems, IoT enables real-time automation, intelligent decision-making and enhanced data exchange, driving innovation across sectors such as manufacturing, healthcare, smart cities and digital infrastructure. As IoT continues to expand, its integration with AI, edge computing and decentralised web architectures will accelerate, transforming the ways in which devices communicate, process data, and interact within complex ecosystems.

In the future Web 4.0, IoT devices **would form a unified network** that processes complex data streams from diverse connected devices[81]. The ITU defines IoT as “a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies”[82]. Recommendation ITU-T Y.2060[83] further clarifies that security and privacy requirements must be fulfilled when offering these services to all sorts of applications. A similar definition is provided by the European Research Cluster on the Internet of Things (IERC), which in addition highlights that physical and virtual things within the global infrastructure have “identities, physical attributes, and virtual personalities, and use intelligent interfaces”[84].

The above definitions highlight **the role of IoT in connecting multiple devices** and systems to provide advanced services. Such networks of interconnected devices and systems drives innovation across various domains, from smart homes to industrial automation, bringing about changes to daily life and business operations. IoT devices can form independent, self-sustaining networks, or may be connected via the internet. Different core networking strategies will merge alongside concepts in IoT technology[85].

By 2023, the number of IoT devices worldwide had reached 15.9 billion, and is expected to rise to more than 32.1 billion by 2030[86]. In Europe, the IoT market in 2023 recorded a revenue of more than USD 225 billion, expected to increase to USD 411 billion by 2028[87]. Worldwide, it has been estimated that by 2030, IoT could enable between USD 5.5 trillion and USD 12.6 trillion in value globally. The greatest potential for this economic value in 2030 is expected to be concentrated in factory settings that include standardised production environments (e.g. manufacturing, hospitals, precision farming), but also in

[79] Copyright Clearance Center (2024). *Heart of the Matter: Copyright & AI Training – LLMs Executive Summary*. Available at: https://www.copyright.com/blog/heart-of-the-matter-copyright-ai-training-llms-executive-summary/
[80] Ferrara, E. (2024). The butterfly effect in artificial intelligence systems: Implications for AI bias and fairness. *Machine Learning with Applications*, 15, 100525. Available at: https://www.sciencedirect.com/science/article/pii/S266682702400001X.
[81] European Commission (no date). Europe's Internet of Things Policy. Available at: https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy
[82] International Telecommunication Union (ITU) (2015). Global Standards Initiative on the Internet of Things (IoT). ITU-T. Available at: https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx
[83] International Telecommunication Union (ITU) (06/2012). ITU-T Recommendation Y.4000/Y.2060. ITU-T. Available at: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060
[84] IERC (2014). About IoT. Available at: https://internet-of-things-research.eu/about_iot.htm.
[85] Majid, M., Habib, S., Javed, A.R., Rizwan, M., Srivastava, G., Gadekallu, T.R., & Lin, J.C.W. (2022). Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. *Sensors*, 22(6), 2087. https://www.mdpi.com/1424-8220/22/6/2087/pdf
[86] Statista (2024). Number of IoT connections worldwide 2022-2033 Statista. Available at: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.
[87] Statista (2024). Internet of Things (IoT) in Europe – Statistics & Facts. Statista. Available at: https://www.statista.com/topics/4123/internet-of-things-iot-in-europe/

the setting of health and well-being (e.g. applications that are deployed in and affect the body, such as implants and brain–computer interfaces)[88].

The economic impact of the Industrial Internet of Things (IIoT)[89] will be especially significant in view of the evolution towards Web 4.0. IIoT refers to the network of interconnected devices, sensors, instruments and systems(-of-systems) used in industrial applications. IIoT enables the collection, exchange and analysis of data to improve: (1) operational efficiency and productivity, e.g. via real-time monitoring and predictive maintenance, reducing downtime and optimising operations; (2) decision-making, as data-driven insights can enable informed decision-making and strategic planning; and (3) safety, as the continuous monitoring of equipment and environments helps to prevent accidents and ensure compliance with safety regulations.

Successful applications of (I)IoT will become more far reaching and pervasive in the future. Pertinent examples include its use in manufacturing (real-time monitoring, predictive maintenance and quality control)[90], the domain of energy (real-time monitoring and control of smart grids, energy flexibility via renewable energy management)[91], transportation (fleet management, smart traffic systems and self-driving vehicles)[92], and agriculture (precision farming, smart irrigation, livestock monitoring)[93]. Many of these applications already exist in a pilot phase, but they are moving towards large scale adoption, which will be an important feature of Web 4.0[94].

A key challenge at present is the **lack of interoperability**, due to the large degree of fragmentation among existing protocols and standards, and the prevalence of proprietary solutions (leading to vendor lock-in)[95]. Such fragmentation can ultimately lead to isolated "islands" of connectivity, **increased complexity** and "data silos", resulting in products that are **costly** and **less accessible** and which **stifle innovation**. **Security** is another important risk resulting from this fragmentation, as an excessive number of protocols and standards leads to security measures being inconsistent and costly across IoT devices[96]. As well as interoperability being critical within a given vertical IoT domain, cross-domain interoperability will also be crucial for the future Web 4.0 to unlock the full potential of combining IoT data.

Standardisation has played a critical role in fostering interoperability. The adoption of IPv6 addressed the need for a vastly larger address space to accommodate billions of connected devices. Communication protocols such as MQTT[97] and CoAP[97] have ensured efficient data exchange, Semantic standards such as the ETSI SAREF framework of ontologies[98] have emerged as an enabler

---

88 McKinsey Global Institute (2021). The Internet of Things: Catching up to an accelerating opportunity. Available at: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/iot%20value%20set%20to%20accelerate%20through%202030%20where%20and%20how%20to%20capture%20it/the-internet-of-things-catching-up-to-an-accelerating-opportunity-final.pdf

89 Malik, P.K., Sharma, R., Singh, R., Gehlot, A., Satapathy, S.C., Alnumay, W.S., ... & Nayak, J. (2021). Industrial Internet of Things and its applications in industry 4.0: State of the art, *Computer Communications*, Available at: https://doi.org/10.1016/j.comcom.2020.11.016

90 Soori, M., Arezoo, B., & Dastres, R. (2023). Internet of things for smart factories in industry 4.0, a review. *Internet of Things and Cyber-Physical Systems*, 3, 192-204. Available at: https://www.sciencedirect.com/science/article/pii/S2667345223000275

91 Ahmad, T., & Zhang, D. (2021). Using the internet of things in smart energy systems and networks. Sustainable Cities and Society, 68, 102783. Available at: https://www.sciencedirect.com/science/article/pii/S2210670721000755

92 Wu, Y., Dai, H.N., Wang, H., Xiong, Z., & Guo, S. (2022). A survey of intelligent network slicing management for industrial IoT: Integrated approaches for smart transportation, smart energy, and smart factory. *IEEE Communications Surveys & Tutorials*, *24*(2), 1175-1211. Available at: https://ieeexplore.ieee.org/abstract/document/9732420/

93 Liang, C., & Shah, T. (2023). IoT in agriculture: The future of precision monitoring and data-driven farming. Eigenpub Review of Science and Technology, 7(1), 85-104. Available at: https://studies.eigenpub.com/index.php/erst/article/view/11

94 McKinsey & Company. (2021). IoT value set to accelerate through 2030: Where and how to capture it. McKinsey Digital. Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it#/

95 ETSI. (2016). TS 103 375: SmartM2M; IoT standards landscape and future evolutions. European Telecommunications Standards Institute. Available at: https://www.etsi.org/deliver/etsi_tr/103300_103399/103375/01.01.01_60/tr_103375v010101p.pdf

96 Dominioni, S. (2023). Internet fragmentation and cybersecurity. Available at: https://unidir.org/wp-content/uploads/2023/12/UNIDIR_internet_fragmentation_cybersecurity_primer.pdf

97 EMQX Team (no date). MQTT vs CoAP: Comparing Protocols for IoT Connectivity. www.emqx.com. Available at: https://www.emqx.com/en/blog/mqtt-vs-coap

98 ETSI (no date). SAREF: Smart Applications REFerence ontology. European Telecommunications Standards Institute. Available at: https://saref.etsi.org/

to interoperability between various IoT devices and systems from different vendors in an open, FAIR (i.e. findable, accessible, interoperable and re-usable)[99] and standardised way.

Energy consumption is a key challenge, and one that will become even more pressing in the future. Energy is needed to process and store this vast amount of IoT data. For this reason, edge computing increasingly relies on processing data closer to its source to avoid the transmission and processing of huge amounts of real-time data in the cloud. Edge computing also reduce latency and bandwidth usage, thereby supporting real-time applications. Challenges related to the sustainability of Web 4.0 and virtual worlds are further explored in Section 3.5.

Cybersecurity is a critical aspect, as billions of IoT devices connected to the internet represent points of vulnerability to cyber-attacks, creating serious problems for the Internet as a whole. Security standards have emerged to provide encryption and authentication mechanisms, along with cyber-security requirements for consumer IoT[100], IoT security guidelines[101,102] and certification initiatives[103]. The challenge is the multitude of different type of devices, systems and application domains (from consumer devices to expensive industrial IoT systems), as all of these present different risks and require diverse security solutions. For further details on security challenges, see also Section 3.2.

Privacy is another critical factor, as IoT devices often collect sensitive personal information, such as location data, health metrics and daily patterns of behaviour. These are typically stored on centralised servers, raising concerns about unauthorised access, data breaches and sharing with third parties without explicit consent from users. Some of these issues are further elaborated on in Section 3.3.

IoT systems will need to adopt semantic standards on a large scale and across domains to ensure seamless communication and data exchange between diverse platforms, fostering greater integration and scalability. For instance, consumers, public sector officials and businesses will be able to search for detailed information about the energy efficiency of IoT products sold in the EU. Such devices will have globally unique identifiers on the web, as well as rich metadata and clear provenance, and will carry a label indicating if they are "interoperability-ready" via standardised IoT ontologies[104]. Moreover, IoT – in combination with knowledge graphs (i.e. data structured in a named directed graph according to an ontology) – will be widely adopted to equip IoT systems with enhanced data integration, analysis and decision-making capabilities. For example, it could be used in smart homes to predict energy usage patterns and optimise the operations of IoT devices. Meanwhile, IoT systems could use digital twins in virtual environments to test and optimise product designs prior to physical prototypes being created.

Wider adoption of security standards for consumer IoT (such as ETSI EN 103 645) will ensure that the IoT devices entering the market and connected to the internet are more secure. Redefining the way in which IoT devices connect to the internet will also be important, as not every IoT device needs to communicate with all other devices connected to the internet. Security management systems will provide autonomous, adaptive security. With regard to privacy, the more widespread adoption of consumer IoT will reveal what data customers are willing to give up in return for benefits such as lower prices or special offers in a retail setting.

---

99 GO FAIR Initiative (no date). FAIR principles. Available at: https://www.go-fair.org/fair-principles/

100 ETSI (2021). ETSI EN 103 645: Cyber Security for Consumer Internet of Things – Baseline Requirements. European Telecommunications Standards Institute. Available at: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/03.01.01_60/ts_103645v030101p.pdf

101 Cloud Security Alliance (CSA) (2019). IoT Security Controls Framework. Cloud Security Alliance. Available at: https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework

102 IoT Security Foundation (2025). IoT best practices in IoT security. Available at: https://iotsecurityfoundation.org/

103 Eurosmart (2019). Eurosmart IoT Security Certification Scheme. Available at: https://www.eurosmart.com/eurosmart-iot-certification-scheme/

104 In an extension of the current initiative in the European Product Registry for Energy Labelling (EPREL) database, as of April 2024, manufacturers that sign the EU's Code of Conduct for Energy Smart Appliances will display a badge on compliant products to signify that they are "interoperable products". Ten manufacturers have already committed to this voluntary initiative and agreed to provide a mapping to the semantic standards SAREF and SAREF4ENER in their products.

2.3. Future communication networks

The evolution of communication networks **is central to the realisation of Web 4.0**. Such networks provide the foundation for high-speed, intelligent and seamless digital interactions. Future networks will bring unprecedented speed, ultra-low latency and enhanced connectivity, enabling immersive digital experiences, AI-driven automation and large-scale IoT deployments. Emerging technologies such as non-terrestrial networks, integrated sensing and AI-optimised resource management will play a key role in addressing these challenges, ensuring that next-generation networks are scalable, resilient and inclusive.

While the core infrastructure of the internet has followed a demand-driven development path, mobile networks have advanced through structured generational transitions, with each new generation (1G, 2G, 3G, 4G, 5G, etc.) introducing transformative capabilities. Such transitions have been driven by various factors including developments in technology, demand from businesses and consumers, spectrum availability and new applications.

The market for future communication networks, including 5G, 6G, core networks, fibre optics and satellites, is experiencing significant growth. In 2023, the global communication networks market was valued at approximately USD 94.1 billion, and is projected to reach USD 130.72 billion by 2030, growing at a compound annual growth rate (CAGR) of 6.7 % from 2024 to 2030[105]. Demand for high-speed internet and advanced communication technologies is driving this growth, with the global market for Industry 4.0, which includes Web 4.0 and future internet technologies, expected to expand from USD 166.1 billion in 2023 to USD 862.0 billion by 2032 – a CAGR of 20.1 %[106]. This will be fuelled by the increasing adoption of AI, IoT and other digital technologies, which are essential for the seamless integration and functionality of next-generation communication networks.

The fifth generation of mobile networks (5G) was introduced in the 2020s, and represents a paradigm shift in network capabilities. 5G is based on three main pillars[107]: delivering **enhanced mobile broadband** (eMBB), **ultra reliable and low latency communications** (uRLLC), and **connecting devices on a massive scale** (mMTC: massive machine-type communications). eMBB, with speeds up to 100 times faster than 4G, 5G supports high-definition video streaming, real-time gaming and seamless virtual and augmented reality experiences within widely available mobile networks. URLLC is crucial for applications requiring immediate feedback, such as autonomous vehicles and remote surgery[108]. Lastly, mMTC is key to enabling a massive number of devices to operate, supporting applications such as IoT.

The development of sixth-generation mobile networks (6G) has already begun, and these will be at the core of Web 4.0. It is expected that 6G will be commercially available by the 2030s. 6G expands beyond the three main pillars of 5G by further pushing the boundaries of connectivity[109]. First, it will deliver data rates of up to 1 terabit per second, enabling **immersive communication** that supports applications such as holographic communication or immersive XR environments, creating new possibilities in education, entertainment and remote collaboration. Second, it will deliver **hyper-reliable and low latency communications**, achieving latencies as low as 1 millisecond, enabling real-time applications such as autonomous vehicles, remote surgery, industrial automation and real time digital twins[110].

---

105 Verified Market Reports (2025). Communication networks market – Trends, growth, and forecast 2022-2032. Available at: https://www.verifiedmarketreports.com/product/communication-networks-market/

106 SNS Insider (2024). Industry 4.0 market report – Trends, analysis, and future outlook 2024-2032. Available at: https://www.snsinsider.com/reports/industry-4-0-market-1226

107 ITU Radiocommunication Sector (ITU-R). (2015, September). Recommendation ITU-R M.2083-0: IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond. Available at: https://www.itu.int/dms_pubrec/itu-r/rec/m/r-rec-m.2083-0-201509-i!!pdf-e.pdf

108 3GPP (2025). 3GPP Specifications and Technologies – Releases Overview. Available at: https://www.3gpp.org/specifications-technologies/releases

109 International Telecommunication Union (ITU) (2024). IMT towards 2030 and beyond (IMT-2030). ITU. Available at: https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2030/Pages/default.aspx

110 European Parliamentary Research Service (EPRS) (2024). The path to 6G: European Parliament briefing. European Parliament. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757633/EPRS_BRI(2024)757633_EN.pdf

Lastly, by enabling **massive communication**, 6G networks will deliver the ability to connect billions of devices and support IoT on an unprecedented scale, facilitating smart cities, intelligent transportation systems and advanced healthcare applications. However, in addition to the technical challenges presented by 6G[111], it is also part of geopolitical discussions involving national security and market protectionism, which introduces the risk of fragmentation of the network[112,113].

The development of future communication networks is being driven by rapid advancements in AI, cloud computing, and edge processing, along with increasing demands for real-time data exchange and global connectivity. These networks **will reshape connection quality**. They will also draw upon an integrated network approach to data processing and storage via cloud and edge computing. Cloud infrastructure provides the scalable computing power needed to handle massive datasets, while edge computing enables data to be processed closer to its source, minimising delays and network congestion. Edge computing has already evolved to bring previously centralised storage and computing power closer to both source and end devices[114]. We anticipate that this trend will offer edge-based data/processing with low delay, which will increase its potential to significantly impact future network architectures, potentially leading to a redefinition of how data is processed and transmitted[114]. Lastly, the development of demanding new Web 4.0 services (such as AI, XR, spatial computing and others) may be inextricably linked to advances in edge computing, as both emphasise the need for integration, real-time processing and adaptation[114].

One important function of next-gen mobile networks (i.e. from 5G-Advance/6G) that should be highlighted is **Integrated Sensing and Communication (ISAC)**, as outlined in the 3GPP TS 22.137 specification[115]. ISAC[116] enables the simultaneous use of radio signals for both communication and sensing, allowing networks to detect and track objects such as UAVs, humans, AGVs, vehicles and animals in both outdoor and indoor environments. This capability is crucial for applications such as environmental monitoring, enabling real-time data on environmental conditions to be collected and analysed[117]. In addition, ISAC supports motion monitoring, enhancing the ability to track and analyse movements for various applications, from security to smart city management[118].

Enhancing many network functions and capabilities, AI/ML will be deeply embedded into next-generation network architectures, creating an **'AI-native' environment**. This integration will make AI a pervasive functionality, seamlessly embedded across all network layers to optimise performance and enhance user experiences[119]. Closed control loops will enable real-time automation and adaptability, ensuring efficient network management and minimal downtime[120]. MLOps pipelines will streamline the lifecycle management of AI/ML models, facilitating continuous integration, deployment and

111 Press release. ITU advances the development of IMT-2030 for 6G mobile technologies. ITU. Available at: https://www.itu.int/en/mediacentre/Pages/PR-2023-12-01-IMT-2030-for-6G-mobile-technologies.aspx

112 Majithia, K. (2023, 24 April). Standards body issues warning on 6G fragmentation. Mobile World Live. Available at: https://www.mobileworldlive.com/regulation/standards-body-issues-warning-on-6g-fragmentation/

113 MERICS (2023, 22 February). Fragmenting technology – 6G mobile could divide the world. MERICS. Available at: https://merics.org/en/comment/fragmenting-technology-6g-mobile-could-divide-world

114 Kolkman, O., Robachevsky, A., Gahnberg, C., & Badran, H. (2022). Evolution of the edge, what about the internet? In: *Proceedings of the ACM SIGCOMM Workshop on Future of Internet Routing & Addressing (FIRA '22)*. Association for Computing Machinery, New York, NY, USA, 1-5. https://doi.org/10.1145/3527974.3546975

115 3GPP, Service requirements for integrated sensing and communication, Tech. Rep. TS 22.137 version 19.1.0, Apr. 2024. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4198

116 Ramos, A., Inca, S., Ferrer, M., Calabuig, D., Roger, S., & Monserrat, J.F. (2025). Simulation framework for detection and localization in integrated sensing and communication systems. *Telecom*, 6(1), 4. https://doi.org/10.3390/telecom6010004

117 Johnston, J. (2024, 12 February). Guest Post: Why Integrated Sensing and Communications Will be the Killer App for 6G. Welcome to 6GWorld. https://www.6gworld.com/exclusives/guest-post-why-integrated-sensing-and-communications-will-be-the-killer-app-for-6g/

118 Ghadialy, Z. (2024, 21 September). Integrating Sensing And Communications (ISAC) for Enhanced System Efficiencies and New User Experiences. Free 6G Training, https://www.free6gtraining.com/2024/09/integrating-sensing-and-communications.html

119 You, X., Huang, Y., Zhang, C., Wang, J., Yin, H., & Wu, H. (2024). When AI meets sustainable 6G. Science China Information Sciences, 68(1). https://doi.org/10.1007/s11432-024-4257-6

120 R. Pires et al. (2024, 3 June). Closed-Loop Automation in 6G for Minimum Downtime Task Continuity in Surveillance Cobots. *024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Antwerp, Belgium, 2024, pp. 860-865* https://ieeexplore.ieee.org/document/10597048

monitoring[121]. In addition, AI-as-a-Service (AIaaS) will utilise the capabilities of AI via APIs, allowing external consumers to leverage advanced AI functionalities for various applications[122]. Together, these elements will create a robust, intelligent and highly adaptive 6G network, driving the evolution of the Web 4.0.

Going beyond the concept of 6G in the context of Web 4.0, future communications will feature the seamless integration of various network types to provide high-speed, reliable and **ubiquitous connectivity**[123]. This includes **satellite networks**[124], which offer global coverage and low latency through constellations of low Earth orbit (LEO) satellites, **terrestrial networks** that provide high-speed connectivity through ground-based infrastructure, and **airborne networks** that utilise aerial vehicles and drones to extend coverage and enhance communication capabilities. Furthermore, **non-terrestrial networks (NTN)**[125] will integrate and "glue together" different elements to ensure resilient and ubiquitous connectivity and, as such, form the backbone of the web 4.0[126].

2.4. Immersive technologies

Immersive technologies are transforming the way users interact with digital environments, enabling the seamless integration of virtual and physical spaces. As **a key component of the future Web 4.0**, immersive technologies are linked to extended reality (XR), which encompasses augmented reality (AR), virtual reality (VR), and mixed reality (MR). These technologies leverage advances in AI, IoT and next-generation networks (5G/6G) to deliver intelligent, real-time and hyper-personalised digital experiences.

3D virtual worlds have long been a feature of computer gaming. In the evolution towards Web 4.0, immersive technologies will **introduce a multitude of new use cases** for 3D virtual worlds in entertainment, education and training, healthcare and real estate, as well as retail and e-commerce[127]. Immersive technologies require ultra-low latency, higher bandwidth and accelerated processing power. The consequent surge in data traffic demands a resilient infrastructure capable of supporting these high-performance applications[128].

The immersive technology market is expected to grow significantly in the coming years, from USD 40.88 billion in 2024 to USD 173.99 billion by 2032[129], reflecting a compound annual growth rate (CAGR) of 27.9 %[130,131].

A key feature of the 3D digital transformation, virtual worlds[132] integrate **AI and XR** technology to enable unparalleled realism in rendering (by leveraging 3D assets, holograms and Gaussian splats) while seamlessly merging real-world and virtual interactions. Furthermore, AI-driven personalisation

---

[121] Singla, A. (2023). Machine Learning Operations (MLOPs): Challenges and strategies. *Journal of Knowledge Learning and Science Technology* 2(3), 333–340, ISSN 2959-6386 (Online). https://doi.org/10.60087/jklst.vol2.n3.p340

[122] S. Kerboeuf et al. (2024). Design Methodology for 6G End-to-End System: HeXa-X-II Perspective. *in IEEE Open Journal of the Communications Society, vol. 5, pp. 3368-3394,*. https://ieeexplore.ieee.org/abstract/document/10525242/

[123] Boubendir, A. & Airbus Defence and Space SAS (2024). Enabling the 6G use cases. https://hexa-x-ii.eu/wp-content/uploads/2024/10/Airbus_HexaX-WS_VTC-Conf_Enabling-6G-Use-Cases_07102024.pdf

[124] MediaTek, Inc. (2024). White paper: 6G Satellite and Terrestrial Network Convergence. MediaTek. https://www.mediatek.com/tek-talk-blogs/white-paper-6g-satellite-and-terrestrial-network-convergence

[125] https://www.etsi.org/images/Events/2024/NTN_CONFERENCE/6G_NTN_White_Paper_Vision-on-NTN-in-6G_r01_v04.pdf

[126] 6G-NTN project (2024, 20 November). 6G-NTN. https://6g-ntn.eu/

[127] EMB Global (2024). What is immersive technology: a deep dive into virtual reality. Available at: https://blog.emb.global/immersive-technology-explained/

[128] Joint Research Centre (JRC) (2023, 3 July). Next-generation virtual worlds: Opportunities, challenges, and policy implications. European Commission. Available at: https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/next-generation-virtual-worlds-opportunities-challenges-and-policy-implications-2023-07-03_en

[129] Credence Research (2024). Immersive technology market report 2024-2032. Credence Research. Available at: https://www.credenceresearch.com/report/immersive-technology-market

[130] Grand View Research (2024). Immersive technology market analysis & forecasts 2025-2030. Grand View Research. Available at: https://www.grandviewresearch.com/industry-analysis/immersive-technology-market-report

[131] Skillnet Ireland (2024). Irish immersive technology strategy for growth. Available at: https://www.skillnetireland.ie/insights/irish-immersive-technology-strategy-for-growth

[132] Kayakoku, H. (2023). History and development of virtual worlds and the metaverse. In: F.S. Esen, H. Tinmaz, H., & M. Singh (eds). *Metaverse. Studies in Big Data, vol 133*. Springer, Singapore. Available at: https://doi.org/10.1007/978-981-99-4641-9_2

will tailor virtual environments to the preferences and behaviours of individual users. Such hyper-personalisation will leverage personal user data at an even more granular level than social networks, amplifying both the benefits and concerns associated with such data. This poses challenges in the handling of sensitive user information, including haptics, gaze tracking and digital avatar identities[133].

Building on virtual worlds technology, **digital twins** are another key part of the evolution towards Web 4.0. Digital twins are highly accurate virtual replicas of real-world entities and systems. These virtual counterparts (combined with AI) are already extensively used in sectors such as the automotive industry (where they enhance vehicle design and testing), as well as urban city planning (where they help to optimise infrastructure and resource management)[134]. The development and further enhancement of digital twins will mostly be driven by the need to optimise manufacturing processes (e.g. in terms of worker safety and cost competitiveness)[135]. Digital twins are closely linked to the Internet of Things (IoT)[136], leveraging real-time data from connected devices to monitor, simulate and optimise physical systems[137]. However, the implementation of digital twins also poses certain challenges. These include cybersecurity risks, high costs, infrastructure development, and the need for interoperability between diverse systems[138,139].

Along with advances in IoT and wide-scale sensor networks, **spatial computing** is set to profoundly impact the future Web 4.0 by seamlessly integrating the physical and digital worlds. Spatial computing[140] refers to technology that allows computers to understand and interact with the physical world in a spatial context. It involves the use of sensors, cameras and other devices to collect real-time data about the environment, which is then processed to create a digital representation of the physical space. This digital representation can be used to overlay information, create virtual objects and enable interactions that feel natural and intuitive. Thus, spatial computing leverages real-time data from a wide range of sensing devices to create immersive, interactive environments that enhance user experiences and operational efficiencies[141]. It is a key building block in allowing complex interaction between the real world and (3D) digital worlds, and in enabling user interaction built around haptics and gaze[142,143]. However, data privacy, high implementation costs and the need for robust infrastructure remain a significant concern[144].

Brain–computer interfaces (BCIs), a type of neurotechnology, are emerging as the next frontier in the evolution towards Web 4.0. BCIs enable direct communication between the human brain and digital

---

133 Jain, A.K., Sahoo, S.R., & Kaubiyal, J. (2021). Online social networks security and privacy: Comprehensive review and analysis. *Complex & Intelligent Systems*, 7, 2157–2177. Available at: https://doi.org/10.1007/s40747-021-00409-7

134 Forbes & Dell Technologies. (2024, 26 June). Urban digital twins: AI comes to city planning. Dell Technologies. Available at: https://www.forbes.com/sites/delltechnologies/2024/06/26/urban-digital-twins-ai-comes-to-city-planning/

135 Sharma N. (2025). Blog: 10 Use cases and Benefits of how Digital twin Technology is revolutionizing automotive Design and manufacturing. Appinventiv. Available at: https://appinventiv.com/blog/digital-twin-in-automotive-industry/

136 Akbar F. (2024). How Digital Twins and IoT Work Together. Toobler. Available at: https://www.toobler.com/blog/digital-twin-iot.

137 Hananto, A.L., Tirta, A., Herawan, S.G., Idris, M., Soudagar, M.E.M., Djamari, D.W., & Veza, I. (2024). Digital Twin and 3D Digital Twin: Concepts, Applications, and Challenges in Industry 4.0 for Digital Twin. *Computers*, 13(4), 100. https://doi.org/10.3390/computers13040100

138 Boreham J. (2024, 13 June). Three digital twin challenges and how they affect the industry. *Digital Twin Insider*. Available at: https://digitaltwininsider.com/2024/06/13/3-digital-twin-challenges-and-how-they-affect-the-industry/.

139 Park, S., Maliphol, S., Woo, J., & Fan, L. (2024). Digital Twins in Industry 4.0. *Electronics*, 13(12), 2258. https://doi.org/10.3390/electronics13122258

140 Yenduri, G., Ramalingam, M., Maddikunta, P.K.R., Gadekallu, T.R., Jhaveri, R.H., Bandi, A., Chen, J., Wang, W., Shirawalmath, A.A., Ravishankar, R., & Wang, W. (2024, 30 January). Spatial Computing: concept, applications, challenges and future directions. arXiv.org. https://arxiv.org/abs/2402.07912

141 Altaweel M. (2020). The spatial Internet of Things. Geography Realm. Available at: https://www.geographyrealm.com/the-spatial-internet-of-things/

142 Jacucci, G., Bellucci, A., Ahmed, I. et al. (2024) Haptics in social interaction with agents and avatars in virtual reality: a systematic review. *Virtual Reality*, 28, 170. Available at: https://doi.org/10.1007/s10055-024-01060-6

143 Zheleva, A., Hardeman, J., Durnez, W., Vanroelen, C., De Bruyne, J., Osei Tutu, D., … & Bombeke, K. (2023). The impact of eye gaze on social interactions of females in social virtual reality : the mediating role of the uncanniness of avatars and the moderating role of task type. *Heliyon*, 9(10). Available at: https://doi.org/10.1016/j.heliyon.2023.e20165

144 Yenduri, G., Ramalingam, M., Maddikunta, P.K.R., Gadekallu, T.R., Jhaveri, R.H., Bandi, A., Chen, J., Wang, W., Shirawalmath, A.A., Ravishankar, R., & Wang, W. (2024). Spatial computing: Concept, applications, challenges, and future directions. arXiv preprint arXiv:2402.07912. Available at: https://arxiv.org/pdf/2402.07912

systems[145]. In this context, it is useful to differentiate between two types of BCIs: (1) external sensors attached to the head to measure brain activity (i.e. EEG, MEG, fNIRS, and fMRI)[146] and (2) sensors implanted into the brain of the user. While all BCI techniques are advancing, they are currently still in an initial phase of research and development. The current focus of BCI technology is on interaction and interactivity (both human-to-machine and human-to-human): decoding speech, measuring attention, controlling devices, enabling collaboration and immersive virtual reality. Market ready devices (beyond very specific devices such as those designed for the medical domain) are not expected on a mass scale within the coming 5-10 years. Furthermore, if such devices do appear in this timeframe, it is expected that they will reproduce similar interaction paradigms to those that currently exist (e.g. in terms of texting and navigating user devices). This said, the number of EEG-based BCI devices in use is increasing rapidly in both medical and non-medical domains[147]. While the future impact of such devices on existing networks and infrastructure is still unclear, the biggest concerns lie in the protection of the sensitive data utilised by BCI devices – namely, aspects of security, privacy, trust and other ethical considerations. Many questions remain with regard to the technical capabilities of BCIs in the coming years, as well as their potential impact on Web 4.0 and the handling of any associated data[148].

Rendering in XR, as well as spatial computing and new interaction paradigms, are driving a significant increase in **compute power requirements**. The aforementioned technologies demand high-performance computing in order to process and render complex 3D environments, real-time simulations and interactive experiences[149]. This surge in compute power is closely tied to the evolution of future networks, including 5G and 6G, which provide the necessary bandwidth and low latency to support such data-intensive applications[150]. In addition, the integration of cloud and edge[151] computing enables the distribution of computational tasks, optimising performance and reducing latency by processing data closer to the source. These developments necessitate robust infrastructure and advanced computing capabilities to ensure seamless and efficient operation, ultimately transforming how we interact with digital content and services, as well as the real world.

However, advances in XR technologies create the risk of fragmentation and disconnection in the digital ecosystem by fostering the development of incompatible platforms, proprietary standards and isolated virtual environments (see also Sections 3.1 and 4.3). Therefore, clear and enforceable standards are needed[152,153,154]. Key standardisation initiatives currently underway include **OpenXR**, an open standard by the Khronos Group, which provides a unified interface for AR and VR applications across various hardware platforms[155]; **WebXR Device API**, developed by W3C, which enables web applications to interact with XR devices, thereby supporting consistent user experiences across

145 IEEE (2020). Standards roadmap: Neurotechnologies for brain-machine interfacing. IEEE Standards Association. Available at: https://standards.ieee.org/wp-content/uploads/import/documents/presentations/ieee-neurotech-for-bmi-standards-roadmap.pdf

146 SURF (2024). Introducing Brain-Computer Interfaces for Education and Research. Available at: https://www.surf.nl/files/2024-10/en-whitepaper-intro-to-bci-1.0.pdf

147 Vărbu, K., Muhammad, N., & Muhammad, Y. (2022). Past, present, and future of EEG-based BCI applications. *Sensors*, 22(9), 3331. Available at: https://www.mdpi.com/1424-8220/22/9/3331/pdf

148 Radu, R. (2024). Neurotechnologies and the future of internet governance. European University Institute. Available at: https://cadmus.eui.eu/bitstream/handle/1814/77410/RSC_IB_2024_Radu.pdf

149 Lee, E.-S., & Shin, B.-S. (2023). Enhancing the Performance of XR Environments Using Fog and Cloud Computing. *Applied Sciences*, 13(22), 12477. Available at: https://doi.org/10.3390/app132212477

150 Theodoropoulos, T., Makris, A., Boudi, A., Taleb, T., Herzog, U., Rosa, L., Cordeiro, L., Tserpes, K., Spatafora, E., Romussi, A., Zschau, E., Kamarianakis, M., Protopsaltis, A., Papagiannakis, G., & Dazzi, P. (2022). Cloud-based XR services: A survey on relevant challenges and enabling technologies. *Journal of Networking and Network Applications*, 2(1), 1–22. Available at: https://doi.org/10.33969/J-NaNA.2022.020101

151 M. Satyanarayanan (2017, January). The Emergence of Edge Computing. *Computer*, 50(1), pp. 30-39, Available at: https://ieeexplore.ieee.org/document/7807196

152 APDC Portugal (2024). Portugal XR Report 2024. APDC Communications. Available at: https://comunicacoes.apdc.pt/portugal-xr-report-2024/69324122

153 Cosgrove J., Kilkelly F. (2024, May). Irish Immersive Technology Strategy for Growth. Skillnet & Eirmersive. Available at: https://www.skillnetireland.ie/uploads/attachments/Report-GrowthIndustriesForImmersiveTech_.pdf

154 Bennett M., Cornwall A., Cser A. Miller P., Gownder J. P., Liu M., Ask J., Pilecki M., Wang X., Truog D. et al. (2024). *The state of the metaverse 2024*. Forrester Trends Report. Available at: https://www.forrester.com/report/the-state-of-the-metaverse-2024/RES180414

155 Khronos Group. (no date). OpenXR: Empowering Portable Immersive Experiences. Available at: https://www.khronos.org/openxr/.

browsers[156]; and **GeoPose**, a standard created by the Open Geospatial Consortium that ensures accurate positioning and orientation data for AR applications[157].

2.5. Quantum technology

As the web evolves towards a more immersive, intelligent and interconnected digital ecosystem, the underlying infrastructure will need to adapt to evolving computational and security demands. **Quantum technology represents a fundamental shift** in the way data is processed, transmitted and secured. It has the potential to both enhance and challenge the foundations of the digital world. Quantum computing is likely to drive breakthroughs in computing, cryptography and sensing; however, it also presents disruptive risks, as it could be used to compromise traditional encryption methods.

Quantum computing has potential relevance to Web 4.0 in a number of ways. These include improving user experiences through its processing and modelling capabilities; securing and protecting private data in virtual environments (through the use of quantum key distribution); and securing network channels through the use of quantum random number generation[158]. Moreover, based on current estimates, the emergence of Web 4.0 and mature virtual worlds[159] and the global quantum internet (estimated to emerge in 10-15 years)[160,161] are likely to coincide.

Quantum technology has the **potential to disrupt** the way in which information is processed and communicated. Quantum computing offers solutions to problems that cannot be solved using classical computing[162]. Unlike classical computers, which use binary bits (0s and 1s), quantum computers use “qubits”, which can exist in the states ‘0’ and ‘1’, but also in the superposition of states. By exploiting quantum-mechanical phenomena such as superposition and entanglement, quantum computers will be able to perform certain calculations exponentially[163] faster than classical systems. Thus, quantum technology brings new possibilities in the field of computation, communication (the quantum internet) and sensing or metrology (ultra-small and accurate sensors).

The large-scale commercial adoption of quantum technologies currently remains constrained by challenges in hardware scalability, error correction and infrastructure integration[164]. However, the **global quantum computing market is experiencing rapid growth**, driven by investments from governments, research institutions and industry. The size of the global quantum computing market is projected to reach USD 1.51 billion in 2025[165]. Governments worldwide are investing heavily in quantum research. For example, in 2022, public funding for quantum computing in China amounted to USD 15.3 billion. In the same year, such funding amounted to USD 3.8 billion in the US, and EUR 7.2

[156] World Wide Web Consortium (W3C). (2024, October). WebXR device API: W3C Candidate Recommendations Draft. Available at: https://www.w3.org/TR/webxr/

[157] Open Geospatial Consortium (OGC) (2023). GeoPose standard for spatial positioning in the metaverse. Available at: https://www.ogc.org/publications/standard/geopose/

[158] European Commission (2023). Commission Staff Working Document accompanying the Communication on an EU initiative on Web 4.0 and virtual worlds: A head start in the next technological transition (SWD(2023) 250 final). Publications Office of the European Union, Luxembourg. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023DC0442

[159] Deloitte (2022). A whole new world? Exploring the metaverse and what it could mean for you. Deloitte Insights. Available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology/us-ai-institute-what-is-the-metaverse-new.pdf

[160] Nokia (no date). A clear road to the quantum internet. Available at: https://www.nokia.com/thought-leadership/articles/clear-road-to-quantum-internet/

[161] Vermeer, M.J.D., & Peet, E.D. (2023). Securing communications in the quantum computing age: Managing the risks to encryption. RAND Corporation. Available at: https://www.rand.org/pubs/research_reports/RR3102.html

[162] NASA (2024, July). Quantum Communication 101. NASA. Available at: https://www.nasa.gov/wp-content/uploads/2024/07/quantum-communication-101-final.pdf

[163] Delft University of Technology (TU Delft) (no date). Quantum computing: Basics of quantum mechanics. TU Delft. Available at: https://www.tudelft.nl/over-tu-delft/strategie/vision-teams/quantum-internet/basics-of-quantum-mechanics/quantum-computing

[164] Quantum Delta NL (2025). Infinite - Quantum Guide to Commercial Acceleration: Energy Industry. Insights contributed by Aramco, ENEOS, Stanford, E.ON, Alliander, Kvantify, Deloitte, Xanadu, Capgemini, SBQuantum, NTNU, Multiverse Computing, NAM, and TNO. Available at: https://docsend.com/view/449by4d5inkxyq3w

[165] Straits Research (2024). Quantum computing market: Size, share, and forecast to 2033. Straits Research. Available at: https://straitsresearch.com/report/quantum-computing-market

billion in the EU[166,167]. By 2040, the annual economic impact of quantum computing is expected to reach between USD 450 billion and USD 850 billion, with its primary applications being in pharmaceuticals, materials science, energy efficiency, finance and cybersecurity[168]. The global quantum communication market is forecasted to grow from USD 1.2 billion in 2024 to USD 3.6 billion in 2028, and USD 8.6 billion by 2032, as industries adopt quantum key distribution (QKD) to protect sensitive data from emerging cyber threats[169,170].

The integration of quantum technology into the future Web 4.0 or beyond **could bring about transformative capabilities**. Quantum computers may be able to process vast datasets with unprecedented speed, enabling real-time analytics and complex web applications[171]. Quantum algorithms may enhance routing and resource allocation, improving the efficiency and performance of global internet infrastructure. Quantum computing could accelerate machine learning tasks, enabling more accurate AI systems that improve predictive analytics, personalised experiences and intelligent automation[172]. This could drive advancements in fields such as materials science, drug discovery and climate modelling, surpassing the limitations of traditional computational methods[173].

The **primary risk of quantum computing** is its potential to break modern cryptographic protocols, rendering existing encryption methods obsolete (see also Section 3.2). Developments in quantum technologies have the potential to completely undermine the cryptography used in current protocols, such as digital signatures (DNSSEC) and TLS (privacy)[174]. Quantum attacks on critical infrastructure providers could have devastating effects[175]. Even cryptocurrencies such as Bitcoin and other blockchain systems might be vulnerable to quantum attacks[176].

Most vulnerable is asymmetric-key cryptography using common algorithms such as s RSA, ECDH, ECDSA, and EdDSA[177]. To mitigate the quantum threat, **post-quantum cryptography (PQC)** has been an active field of research, also supported by the European Commission under the Horizon 2020 framework: SAFEcrypto[178] and PQCrypto[179]. As a result, several algorithms are standardized by NIST: FIPS 203 intended for general encryption and FIPS 204 and 205 intended for digital signatures[180]. In case of symmetric-key cryptography, its key exchange is most vulnerable for the quantum threat. In

166 McKinsey & Company (2022, 13 September). Betting big on quantum. McKinsey & Company. Available at: https://www.mckinsey.com/featured-insights/sustainable-inclusive-growth/charts/betting-big-on-quantum

167 Shivakumar, S., Wessner, C., & Schumacher, A. (2025, 3 February). *Quick take: Quantum technology global competition*. Center for Strategic and International Studies. Available at: https://www.csis.org/blogs/perspectives-innovation/quick-take-quantum-technology-global-competition

168 Boston Consulting Group (2024, 18 July). Quantum computing on track to create up to USD 850 billion of economic value by 2040. Boston Consulting Group. Available at: https://www.bcg.com/press/18july2024-quantum-computing-create-up-to-850-billion-of-economic-value-2040

169 The Business Research Company (2024, 28 October). 2024-2033 quantum communication market: Key insights on growth opportunities. The Business Research Company. Available at: https://blog.tbrc.info/2024/10/quantum-communication-market-insights/

170 Business Research Insights (2025, 20 January). Quantum communication market size, share, growth, and industry analysis. Business Research Insights. Available at: https://www.businessresearchinsights.com/market-reports/quantum-communication-market-113933

171 AbuGhanem, M., & Eleuch, H. (2024). NISQ computers: A path to quantum supremacy. IEEE Access. Available at: https://doi.org/10.1109/ACCESS.2024.10606265

172 Forbes Technology Council (2024, 19 December). 20 tech-related threats we must not ignore (and solutions). Forbes. Available at: https://www.forbes.com/councils/forbestechcouncil/2024/12/19/20-tech-related-threats-we-must-not-ignore-and-solutions/

173 Altman, E., Brown, K.R., Carleo, G., Carr, L. D., Demler, E., Chin, C., ... & Zwierlein, M. (2021). Quantum simulators: Architectures and opportunities. *PRX Quantum*, 2(1), 017003. Available at: https://doi.org/10.1103/PRXQuantum.2.017003

174 ICANN. (2022, 17 February). ICANN publishes paper on how quantum computing will affect the DNS in the future. Internet Corporation for Assigned Names and Numbers (ICANN). Available at: https://www.icann.org/en/blogs/details/icann-publishes-paper-on-how-quantum-computing-will-affect-the-dns-in-the-future-17-2-2022-en

175 Weinberg, A. (2021, 2 June). Analysis of top 11 cyber attacks on critical infrastructure. FirstPoint Mobile Guard. Available at: https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure

176 Pont, J.J., Kearney, J. J., Moyler, J., & Perez-Delgado, C.A. (2024). Downtime required for Bitcoin quantum-safety. arXiv:2410.16965v1 [quant-ph]. Available at: https://arxiv.org/html/2410.16965v1

177 TNO (2024). Post-Quantum Cryptography: Challenges and Implementation Strategies. TNO. Available at: https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf

178 Horizon 2020 project SAFECrypto: https://www.qub.ac.uk/research-centres/csit/research/csit-research-projects/safecrypto/

179 Horizon 2020 project PQCrypto: https://www.pqcrypto.eu.org/

180 NIST (2024, August). NIST releases first 3 finalized post-quantum encryption standards. NIST. Available at: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

that case **quantum key distribution (QKD)**, which utilises quantum technology to create secure communication links, can be used. The development of QKD is being supported in many countries and regions. For instance, the European Quantum Communication Initiative (EuroQCI) is taking the first steps towards a secure quantum communications infrastructure using QKD[181]. Unlike PQC there are no standards yet for QKD.

Even though viable quantum computers are not yet available and the threat of a quantum computer able to break common cryptographic algorithms in the next decade is not likely[182], data could be stolen and stored for decryption at a later point in time when such computers are powerful enough to do so. This type of quantum attack is called a "**harvest now, decrypt later" attack** (or "store now, decrypt later"). Companies including Apple[183] Google[184] and Meta[185] have already begun migration to PQC in order to mitigate this risk.

Current advances in quantum technology suggest a gradual timeline for its integration with classical infrastructures. The classical internet could be enhanced with quantum information networks (QINs) that are capable of distributing and exploiting quantum entanglement. Initial deployment of quantum communication methods for security applications (QKD) on a local/national scale is currently underway, while international-scale (e.g. European) quantum infrastructures may become available within 5-10 years. Full-scale deployment of quantum-enhanced internet infrastructure that could eventually become the "quantum internet", is expected to become technically possible in 10 or more years[186,187,188,189]. However, acceleration or deceleration in this timeline cannot be ruled out, as breakthroughs or bottlenecks can occur unexpectedly.

Unlike the classical internet, which relies on the TCP/IP protocol stack to interconnect heterogeneous networks, the **quantum internet** will necessitate a new protocol stack tailored to the unique properties of quantum mechanics[190]. This shift raises the risk that quantum networks could operate in isolation, resulting in "quantum islands" that could struggle to interoperate with classical networks[191]. To mitigate this risk, it is crucial to develop new standards that ensure seamless integration and interoperability between quantum and classical systems[192]. Without such standards, the full potential of the quantum internet could be hindered by fragmented, non-cohesive networks with limited

181 European Commission (no date). The European Quantum Communication Infrastructure (EuroQCI) Initiative. European Commission – Shaping Europe's Digital Future. Available at: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

182 Global Risk Institute (2024, January). 2023 Quantum Threat Timeline Report. The Global Risk Institute. Available at: https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/

183 Apple (2024). Introducing PQ3: Advancing post-quantum cryptography for iMessage. Apple Security Research. Available at: https://security.apple.com/blog/imessage-pq3/

184 Google Cloud (no date). Post-quantum cryptography: Preparing for the future of security. Google Cloud Security. Available at: https://cloud.google.com/security/resources/post-quantum-cryptography

185 Lin, S., Tan, J., Asogamoorthy, A., Nekritz, K., Misoczki, R., & Delimanolis, S. (2024, 22 May). Post-quantum readiness for TLS at Meta. Engineering at Meta. Available at: https://engineering.fb.com/2024/05/22/security/post-quantum-readiness-tls-pqr-meta/

186 Illiano, J., Caleffi, M., Manzalini, A., & Cacciapuoti, A.S. (2022). Quantum internet protocol stack: A comprehensive survey. *Computer Networks*, 213, 109092. https://arxiv.org/pdf/2202.10894

187 Kozlowski, W., Dahlberg, A., & Wehner, S. (2020, November). Designing a quantum network protocol. In: *Proceedings of the 16th International Conference on Emerging Networking Experiments and Technologies*, pp. 1-16. Available at: https://doi.org/10.1145/3386367.3431293

188 European Commission (2024). Digital Decade 2024: International benchmarking of digital transformation. European Commission – Shaping Europe's Digital Future. Available at: https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-international-benchmarking-digital-transformation

189 Singh, A., Dev, K., Siljak, H., Joshi, H. D., & Magarini, M. (2021). Quantum internet—applications, functionalities, enabling technologies, challenges, and research directions. *IEEE Communications Surveys & Tutorials*, 23(4), 2218-2247. https://ieeexplore.ieee.org/iel7/9739/5451756/09528843.pdf

190 Luo, M.X. (2024). Quantum Internet. In: *Quantum Networks*. Springer, Singapore. https://doi.org/10.1007/978-981-97-6226-2_2

191 Illiano, J., Caleffi, M., Manzalini, A., & Cacciapuoti, A.S. (2022). Quantum internet protocol stack: A comprehensive survey. *Computer Networks*, 213, 109092. https://arxiv.org/pdf/2202.10894

192 Kleese Van Dam, K., Monga, I., Peters, N., Schenkel, T., & U.S. Department of Energy (2020). From long-distance entanglement to building a nationwide quantum internet. In: *Report of the DOE Quantum Internet Blueprint Workshop,* p. 10. https://www.energy.gov/sites/prod/files/2020/07/f76/QuantumWkshpRpt20FINAL_Nav_0.pdf

connectivity[193]. Therefore, establishing robust, universally accepted standards is essential for the successful deployment and scalability of the quantum internet within the framework of Web 4.0[194]. framework[195].

Standardisation efforts are critical to ensuring the interoperability and security of quantum computing. Organisations including ETSI and NIST, are leading initiatives to define quantum-safe cryptography[196]. In addition, entities including the Quantum Internet Alliance are paving the way, through global collaboration, for the deployment of protocols in relation to quantum network infrastructure.

2.6. Digital trust infrastructure

In the future Web 4.0, digital interactions will become increasingly complex, spanning immersive virtual environments, AI-driven decision-making and decentralised digital ecosystems. These new application scenarios and use cases give rise to significant challenges and new requirements for digital trust infrastructure (for examples, see Sections 2.1 and 2.7). **The evolution toward Web 4.0 relies on a structured digital trust infrastructure (DTI) to enable secure and trustworthy transactions** across physical and virtual domains. This includes robust identity authentication, the validation of digital transactions, and ensuring the integrity of shared information[197].

In this background paper, we define digital trust infrastructure as a **group of collaborating organisations** that manages a set of technologies and governance frameworks for the exchange of digital information. This infrastructure must support at least two core functionalities: (1) maintaining standardised syntax and semantics for digital information; and (2) providing verified identity information about the issuers who sign this digital information. The implementation of such infrastructure offers two primary benefits: cost reductions through the partial or full automation of digital information collection and processing, and increased productivity resulting from the enhanced assurance of trust between participating entities.

The **global digital trust market** is expanding rapidly, driven by the rising need for secure digital transactions, identity verification and data protection. This market was valued at USD 308.34 billion in 2023, and is expected to grow to USD 781.07 billion by 2030 – a compound annual growth rate (CAGR) of 14.2 %[198]. This growth reflects increased investments in authentication, encryption and fraud detection technologies across key sectors such as finance, insurance, e-commerce and digital identity management[199,200].

193 Martin, V. (2024, 25 November). MADQCI: Pioneering the integration of quantum and classical networks. Research Communities by Springer Nature. https://communities.springernature.com/posts/madqci-pioneering-the-integration-of-quantum-and-classical-networks

194 Choucair, C. (2024, 4 September). MADQCI: a scalable quantum key distribution network improving secure communications infrastructure. *The Quantum Insider*, https://thequantuminsider.com/2024/09/04/madqci-a-scalable-quantum-key-distribution-network-improving-secure-communications-infrastructure/

195 Choucair, C. (2024, 4 September). MADQCI: a scalable quantum key distribution network improving secure communications infrastructure. *The Quantum Insider*, https://thequantuminsider.com/2024/09/04/madqci-a-scalable-quantum-key-distribution-network-improving-secure-communications-infrastructure/

196 ETSI. (no date). Quantum-safe cryptography. European Telecommunications Standards Institute. Available at: https://www.etsi.org/technologies/quantum-safe-cryptography

197 World Economic Forum (2022). Earning digital trust: Decision-making for trustworthy technologies. World Economic Forum. Available at: https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf

198 Coherent Market Insights (2024). Digital Trust Market Size, Trends and Forecast to 2030. Coherent Market Insights. Available at: https://www.coherentmarketinsights.com/market-insight/digital-trust-market-6135

199 Mordor Intelligence (2024). Digital Trust Market Size & Share Analysis - Growth Trends & Forecasts (2025 - 2030). Mordor Intelligence. Available at: https://www.mordorintelligence.com/industry-reports/digital-trust-market

200 Precedence Research (2025). Digital Trust Market Size, Share and Trends 2025 to 2034. Precedence Research. Available at: https://www.precedenceresearch.com/digital-trust-market

At present, **digital trust infrastructures are typically based** on chains of X.509[201] certificates, known as public key infrastructure (PKI)[202]. Such chains are used for HTTPS, DNSSEC and other secure communication over the web. X.509 certificates can be traced to root certificates. Web applications – in particular, web browsers – are typically provided with pre-installed root certificates. Nowadays, web browsers provide a warning or aim to prevent users from visiting a website if there is an issue with a X.509 certificate. However, advanced users can add or remove root certificates and make these trust decisions themselves.

In the context of the evolution towards Web 4.0, the development of permissioned blockchains is emerging as a **technology for new digital trust infrastructures**. This shift introduces the concept of decentralisation through distributed ledger technologies (DLTs), in contrast to traditional centralised public key infrastructures (PKIs), which rely on root certificates. However, the key factor that determines trustworthiness (for example, clarity about which parties can be held liable when things go wrong) is not the underlying technology, but governance[203]. Once a group of organisations achieve sufficient mutual trust to run a digital trust infrastructure together, blockchain-technology becomes one of a number of options that can be used for the underlying infrastructure. One example is the European EBSI[204] infrastructure, which focuses on good governance as a key selling point, resulting from the European Blockchain Partnership[205].

One example of a transformative approach to digital trust infrastructure is the blockchain-based DNS Domain Name System (BDNS). BDNS aims to enhance the security, transparency and resilience of the internet. By decentralising the DNS, blockchain technology mitigates the risks associated with single points of failure and censorship, thereby fostering a more robust and trustworthy internet environment[206]. However, significant challenges exist to the adoption of blockchain-based DNS. Its decentralised nature could lead to governance issues, as there is no central authority to manage disputes or enforce regulations[207]. In addition, the scalability of blockchain technology remains a concern, potentially impacting the performance and efficiency of DNS resolution[207]. Thus, due to technical challenges and governance issues, BDNS remains in "in its infancy and cannot yet be seen as a serious rival to DNS"[208].

An upcoming application for digital trust infrastructure is the **automation of digital identity on persons**. Digitalisation promises to reduce costs for verifiers, as well as reducing effort for those users who feel confident using such digital technologies. The W3C has developed the Verifiable Credentials[209] (VC) standard, which supports unambiguous identification of both subject and issuer using decentralised identifiers[210] (DID). In parallel, the ISO has developed a standard for the mobile driver's licence

[201] International Telecommunication Union (ITU) (2025). Recommendation ITU-T X.509: Information technology - Open systems interconnection - The directory: Public-key and attribute certificate frameworks. ITU. Available at: https://www.itu.int/rec/T-REC-X.509/en

[202] Khan, S., Luo, F., Zhang, Z., Ullah, F., Amin, F., Qadri, S.F., ... & Wu, K. (2023). A survey on X. 509 public-key infrastructure, certificate revocation, and their modern implementation on blockchain and ledger technologies. IEEE Communications Surveys & Tutorials. https://ieeexplore.ieee.org/iel7/9739/5451756/10285344.pdf

[203] Barbereau, T., Smethurst, R., Papageorgiou, O., Sedlmeir, J., & Fridgen, G. (2023). Decentralised Finance's timocratic governance: The distribution and exercise of tokenised voting rights. *Technology in Society*, 73, 102251. Available at: https://doi.org/10.1016/j.techsoc.2023.102251

[204] European Commission & EBSI (2024). European Blockchain Services Infrastructure (EBSI). European Commission. Available at: https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home

[205] European Commission (2024). European Blockchain Partnership (EBP). European Commission. Available at: https://digital-strategy.ec.europa.eu/en/policies/blockchain-partnership

[206] Giamouridis, G., Kang, B., Aniello, L., & School of Electronics and Computer Science, University of Southampton, UK (2024). Blockchain-based DNS: current solutions and challenges to adoption. In: DLT2024: 6th Distributed Ledger Technologies Workshop, 14-15 May, 2024, Turin, Italy. https://ceur-ws.org/Vol-3791/paper16.pdf

[207] Osborn, G., & Alan, N. (2023). Web 3 disruption and the domain name system: understanding the trends of blockchain domain names and the policy implications. *Journal of Cyber Policy,* 8(2), 142 – 164. https://doi.org/10.1080/23738871.2023.2294759

[208] Afnic (Issue Paper). Could blockchain (really) replace DNS? https://www.afnic.fr/wp-media/uploads/2024/06/Could-Blockchain-really-replace-DNS-Afnic-Issue-Paper.pdf

[209] World Wide Web Consortium (W3C) (2023). Verifiable Credentials Data Model v2.0. W3C. Available at: https://www.w3.org/TR/vc-data-model-2.0/

[210] World Wide Web Consortium (W3C) (2022). Decentralized Identifiers (DIDs) v1.0. W3C. Available at: https://www.w3.org/TR/did-1.0/

(mDL)[211,212]. These two standards form the basis for the upcoming European Digital Identity Wallet[213] ("EUDI wallet"). The goal of this is to build a set of passport apps that citizens from one European country can use to access services both in their own country and in other European countries. Moreover, Canada[214], USA[215] and other countries are developing solutions for digital identity, as well as various actors in the private sector, in particular banks[216] and telecommunication operators[217].

Another important application of digital trust infrastructure that is connected to Web 4.0-related developments is the **automation of data sharing on "things" or physical objects**. For example, the EU has introduced regulations for Digital Product Passports (DPP), e.g. for (automotive) batteries[218]. A DPP is a standardised digital document that contains information about the composition, production, use and recycling of a product. The goal of DPPs is to improve the sustainability and transparency of products by providing detailed data throughout the entire lifecycle of a product. Under the Ecodesign for Sustainable Products Regulation (ESPR), DPPs are set to expand beyond batteries to textiles, construction and electronics. Most sectors of industry are now developing their data spaces to exchange digital data in secure and trustworthy ways. Relevant standards include Industrial Data Spaces[219 220], and again, W3C Verifiable Credentials. Semantic technologies such as RDF, OWL and Turtle play a key role in achieving semantic interoperability between different players in a data space.

Privacy-enhancing technologies (PETs) are a crucial component of modern digital trust infrastructure. These encompass multiple innovative approaches to data protection[221]. Core technologies include homomorphic encryption, which enables computations to be carried out on encrypted data; zero-knowledge proofs, which allow verification without revealing the underlying information; secure multi-party computation, which enables joint calculations while maintaining input privacy; federated learning, for distributed machine learning without data sharing; and differential privacy, for protecting individual privacy while preserving statistical utility.

These technologies have **diverse applications across multiple sectors**[222]. In financial services, they are used for private transaction processing and fraud detection; in healthcare, they are used for secure research collaboration and patient data protection. In enterprise environments, PETs ensure supply chain transparency and regulatory compliance, while in government services they are used to secure voting systems and protect census data. The technologies are often combined together to create comprehensive privacy solutions, such as using federated learning with homomorphic encryption for secure model training and aggregation, while adding differential privacy to protect outputs. As these

---

211 International Organization for Standardization (ISO). (2024). ISO/IEC 18013-5:2021 – Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application. ISO. Available at: https://www.iso.org/standard/69084.html

212 ISO's mDL standard is part of the broader mdoc framework (ISO/IEC 23220), which supports diverse credentials beyond driver's licencses.

213 European Commission (2024, February). EU Digital Identity Wallets. European Commission – Digital Building Blocks. Available at: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home

214 Government of Canada (2024, December). Trusted access to digital services. Government of Canada. Available at: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/digital-credentials.html

215 Fedscoop (2024, July). DHS invests in digital credential technology. Fedscoop. Available at: https://fedscoop.com/dhs-invests-in-digital-credential-technology/

216 iDIN (no date). Online identification via your bank. iDIN. Available at: https://www.idin.nl/en/

217 GSMA (no date). Mobile Connect. GSMA. Available at: https://www.gsma.com/solutions-and-impact/technologies/mobile-identity/mobile-connect/

218 European Parliament and Council (2023, 12 July). Regulation (EU) 2023/1542 concerning batteries and waste batteries, amending Directive 2008/98/EC and Regulation (EU) 2019/1020 and repealing Directive 2006/66/EC. Official Journal of the European Union, L 191/1. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1542

219 Braud, A., Fromentoux, G., Radier, B., & Le Grand, O. (2021). The road to European digital sovereignty with Gaia-X and IDSA. *IEEE Network*, 35(2), 4-5. https://ieeexplore.ieee.org/iel7/65/9387693/09387709.pdf

220 International Data Spaces Association (IDSA). (2017–present). Creating the future of the global digital economy. IDSA. Available at: https://internationaldataspaces.org/

221 One example of the use of PETs concerns the Monero cryptocurrency (https://www.getmonero.org/). Using this, Alice can send Monero to Bob. The public Monero blockchain prevents "double spending" (namely, when Bob has received the amount, Alice no longer has it). Alice cannot prove to anyone (not even law enforcement) that that the person to whom she sent the Monero was Bob. Bob cannot prove to anyone that he received it from Alice. Meanwhile, third parties cannot find identify parties between whom the transaction was carried out, nor the value in Monero of the transaction involved.

222 The Royal Society (2023). Privacy-enhancing technologies, https://royalsociety.org/news-resources/projects/privacy-enhancing-technologies/

technologies continue to evolve and become more efficient, their practical applications are becoming increasingly viable and widespread.

The future evolution of PETs is likely to be marked by further technical advances and expanding applications. On the technical side, we can expect quantum-resistant variants, significant improvements in computational efficiency, automated optimisation systems, and seamless hybrid approaches that combine multiple PETs. These advances will enable new applications in multiple sectors: privacy-preserving AI diagnostics in healthcare, "privacy by default" financial systems, smart city implementations that protect individual privacy, and Web3 applications with built-in privacy features[223,224].

The secondary effects of digital trust infrastructure give rise to **two key challenges**: digital coercion and digital exclusion. As digital trust infrastructure enables citizens and SMEs to have vast amounts of their personal and confidential data readily available in digital form, organisations (both businesses and public agencies) may be tempted to request more information than is strictly necessary. The verified nature of this data creates an additional incentive for organisations to store and analyse it beyond its original purpose. Conversely, digital exclusion represents an equally significant ethical concern. While DTI and its associated automation could reduce costs for data-collecting organisations and simplify processes for digitally adept citizens, a substantial portion of the global population faces barriers to participation (see also Section 3.7)[225]. The digital divide also extends to individuals who may not possess the physical or mental capabilities to navigate the complexities of digital systems, whether in responding to legitimate requests or protecting themselves against fraudulent ones.

2.7. Technology convergence

Technology convergence refers to the integration of multiple, previously distinct technological domains, leading to new capabilities and functionalities. In the evolution towards Web 4.0, such convergence is not only reshaping digital infrastructures but also creating unexpected effects across computing, networking, AI, immersive environments and decentralised systems[226,227,228]. Technology convergence can be regarded as an important source of potential changes towards Web 4.0[229].

As **AI matures and becomes deeply embedded in digital infrastructures**, it acts as a catalyst for convergence, enabling adaptive, intelligent and self-optimising networks[230]. These **developments lead to *emergence***, whereby interconnected systems exhibit new behaviours and functionalities that cannot be predicted from their individual components. A well-known example of *emergence* is the application of neural networks to LLMs. When these models were trained using large and diverse datasets, emergent properties appeared that had not been explicitly programmed or predicted. This surprised the researchers that had built them, as well as the users of the LLM/genAI applications[231]. However, while emergence brings significant opportunities for automation and real-time intelligence, it also introduces new risks such as unintended consequences, security vulnerabilities and ethical concerns.

223 Usercentrics (2025). Data privacy trends to watch in 2025, https://usercentrics.com/knowledge-hub/data-privacy-trends-for-2025/
224 Finextra (2024). https://www.finextra.com/blogposting/26348/privacy-enhancing-technologies-key-to-win-in-todays-evolving-world
225 Eurostat (2023, December). 56% of EU people have basic digital skills. European Commission – Eurostat. Available at: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20231215-3
226 European Commission. (2023). EU initiative on virtual worlds: A head start in the next technological transition. European Commission. Available at: https://digital-strategy.ec.europa.eu/en/library/eu-initiative-virtual-worlds-head-start-next-technological-transition
227 Anil, A. M. (2025, 13 January). Technology convergence is leading the way for the fifth industrial revolution. World Economic Forum. Available at: https://www.weforum.org/stories/2025/01/technology-convergence-is-leading-the-way-for-accelerated-innovation-in-emerging-technology-areas/
228 See Annex 2 on technical considerations, based on the results of the online consultation.
229 Sourced from the project stakeholder consultation.
230 Greverie, F. (2025, 20 January). There is now a business case for tech convergence. World Economic Forum. Available at: https://www.weforum.org/stories/2025/01/the-business-case-for-tech-convergence/
231 Ganguli, D., & Amodei, D. (2024). Emergent abilities in large language models: An explainer. Center for Security and Emerging Technology (CSET). Available at: https://cset.georgetown.edu/article/emergent-abilities-in-large-language-models-an-explainer/

The convergence of digital and physical realms further amplifies these effects, as AI-driven personalisation, digital twins and immersive environments blur the boundaries between online and offline experiences. The implications of this are profound: governance frameworks must adapt in order to ensure trust, accountability and resilience in an increasingly interconnected and intelligent digital ecosystem.

The above aspects are discussed in greater detail in the sections that follow. Subsection 2.7.1 describes how hybrid networks that integrate cloud, edge and AI technologies can support complex, data-intensive applications by enhancing scalability, real-time processing and security, thereby transforming the internet into an adaptive, intelligent network. Subsection 2.7.2 then outlines some of the cross-cutting consequences of merging physical and digital spaces, which are then further elaborated upon in the challenges described in Chapter 3.

2.7.1. Robust infrastructure and systems-level foundations

The seamless integration of technologies **relies on robust infrastructure** to enable increasingly complex and data-intensive applications (e.g. real-time data processing, decision-making, resource allocation), including within of our physical environments (e.g. smart cities, industrial IoT) as well as in immersive virtual worlds.

Currently, private networks are being developed alongside the public internet infrastructure, thus resulting in so-called **"hybrid networks"**. This evolution demands that existing internet protocols and frameworks are continuously improved to meet new needs (e.g. IPv6 offers an expanded address space and supports advanced the networking capabilities that are essential for IoT ecosystems and smart environments)[232].

Cloud computing platforms fulfil an important function in this process by providing the computational resources and scalability needed to manage the vast amounts of data generated by digital ecosystems. Cloud computing supports efficient storage, analytics and service delivery at scale[233]. At the same time, advances in **edge computing** enable the processing of data closer to the source, reducing latency and bandwidth usage. Edge computing is crucial for processing large amounts of generated data (e.g. from sensors and IoT) and real-time applications (e.g. XR experiences and industrial automation)[234] [235].

The convergence of cloud, edge and on-device computing creates **hybrid systems** that are capable of optimising performance and scalability. AI plays a pivotal role in predictive maintenance and anomaly detection, enabling networks to proactively identify and mitigate potential issues. For instance, AI-powered systems can monitor traffic patterns to detect unusual activity that could indicate cyberattacks or network disruptions, which may also occur for other reasons. AI-powered systems are also used for load balancing, to ensure that bandwidth and processing power are dynamically distributed to prioritise mission-critical tasks[236].

Zero-trust architectures are being developed to address the risk of unauthorised access[237]. Such technologies (based on blockchain or PETs) may be integrated to ensure data integrity and transparent

232 European Commission (no date). EU Internet Standards Deployment Monitoring Website. Available at: https://ec.europa.eu/internet-standards/

233 Prieto, J., & Durán Barroso, R.J. (2024). Emerging technologies in edge computing and networking. Sensors, 24(4), 1271. Available at: https://doi.org/10.3390/s24041271

234 IEEE (2024). IEEE VR 2024: Conference papers program. IEEE Virtual Reality Conference. Available at: https://ieeevr.org/2024/program/papers/

235 Kolkman, O., Robachevsky, A., Gahnberg, C., & Badran, H. (2022). Evolution of the edge, what about the internet? In: Proceedings of the ACM SIGCOMM Workshop on Future of Internet Routing & Addressing (FIRA '22). Association for Computing Machinery, New York, NY, USA, 1-5. https://doi.org/10.1145/3527974.3546975

236 International Telecommunication Union (ITU) (2023). Recommendation ITU-R M.2160-0: Framework for the integration of IMT-2020 and beyond into fixed-mobile hybrid networks. ITU. Available at: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2160-0-202311-I%21%21PDF-E.pdf

237 Ahmadi, S. (2024). Zero trust architecture in cloud networks: Application, challenges and future opportunities. *Journal of Engineering Research and Reports*, 26(2), 215-228. Available at: https://doi.org/10.9734/jerr/2024/v26i21083

record-keeping. This is key to the operation of decentralised systems in which multiple entities interact and where trust must be maintained without central oversight.

When intelligence (AI functionality) is added on a large scale to the network, **the internet turns from a passive infrastructure into an active, adaptive network** that can dynamically respond to changing circumstances. AI and IoT work together to collect, process and analyse vast datasets in real time, enabling predictive analytics and intelligent decision-making. For example, IoT sensors deployed in smart cities generate data that AI systems can use to optimise energy usage, traffic flow and public safety[238]. When individual nodes not only transmit data but also analyse and make decisions locally, **complex interactions arise that create value in unexpected ways.** If every node in the network uses AI to learn from incoming data, and shares these insights with other nodes, **the network as a whole becomes smarter and more effective**[239].

2.7.2. Likely consequences of merging physical and digital realities

When digital and physical interactions continuously shape each other, they create effects that go beyond mere immersion[240]. Unlike earlier applications of virtual worlds in gaming or entertainment, these environments will extend into all aspects of life. Thus, the convergence between Web 4.0 technology clusters leads to a series of cross-cutting consequences. Each of these has further implications on users and society, as elaborated in Chapter 3.

- ***User agency in intelligent environments***

AI-driven automation, real-time personalisation and predictive computing will be integrated into spaces that anticipate and react to user behaviour. Immersive interaction will not be limited to intentional user actions, but will extend to AI-mediated adaptation, in which environments dynamically adjust in real-time on the basis of physiological, behavioural, contextual and even neural data[241]. AI-driven ultra-personalisation in virtual environments enables spaces that can anticipate user needs, adjust emotional stimuli and even modulate experiences to achieve productivity, relaxation or engagement[242].

While this level of real-time environmental control enhances efficiency and user-centred design, it also raises profound ethical concerns (see Section 3.4). The shift from interaction to adaptation marks a turning point in digital agency, as AI's ability to influence perception, decision-making and engagement at a subconscious level moves far beyond the kind of personalisation seen in traditional social media or e-commerce. This transformation introduces challenges in relation to transparency, autonomy and manipulation[243,244,245].

- ***Perception, cognition and social interaction***

The blurring of boundaries between virtual and physical realities could fundamentally reshape human perception, cognition and social interaction. This raises concerns about cognitive confusion and trust in what is real. Ethical norms – traditionally well defined in physical spaces – may become fluid in AI-

[238] European Commission (2021). 2030 Digital Compass: The European way for the Digital Decade. European Commission. Available at: https://eufordigital.eu/wp-content/uploads/2021/03/2030-Digital-Compass-the-European-way-for-the-Digital-Decade.pdf

[239] Vani, G., Naveenkumar, R., Singha, R., Sharkar, R., & Kumar, N. (2024). Advancing predictive data analytics in IoT and AI: Leveraging real-time data for proactive operations and system resilience. *Nanotechnology Perceptions*, 20(S16), 568-582. Available at: https://nano-ntp.com/index.php/nano/article/download/3968/2998/7507

[240] PPMI & TNO (2025, forthcoming). Future of virtual worlds. Project 'Participatory Foresight for Next Generation Online Platforms'.

[241] UNESCO (2024). Unveiling the neurotechnology landscape: Scientific advancements, innovations, and major trends. United Nations Educational, Scientific and Cultural Organization. Available at: https://doi.org/10.54678/OCBM4164

[242] Partarakis, N., & Zabulis, X. (2024). A review of immersive technologies, knowledge representation, and AI for human-centered digital experiences. *Electronics*, 13(2), 269. Available at: https://doi.org/10.3390/electronics13020269

[243] Karami, A., Shemshaki, M., & Ghazanfar, M. (2025). Exploring the ethical implications of AI-powered personalization in digital marketing. *Data Intelligence*. Available at: https://doi.org/10.3724/2096-7004.di.2024.0055

[244] Tucker, I., Ellis, D., & Harper, D. (2012). Transformative processes of agency: Information technologies and the production of digitally mediated selves. *Kultūra ir visuomenė: Socialinių tyrimų žurnalas [Culture and Society: Journal of Social Research]*, 3(1), 9–24. Available at: https://repository.uel.ac.uk/item/8600v

[245] Radu, R. (2024). Neurotechnologies and the future of internet governance. European University Institute. Available at: https://cadmus.eui.eu/bitstream/handle/1814/77410/RSC_IB_2024_Radu.pdf

mediated interactions. Immersive digital environments can influence emotions through the use of biometric data and engagement algorithms, opening doors to emotional manipulation, cognitive dependence and identity fragmentation (see also subsections 3.4.1 and 3.4.4)[246].

This blurring of physical and digital realities could have psychological effects on users. Immersive environments may reinforce cognitive biases, creating self-reinforcing digital realities in which users become psychologically isolated within AI-generated responses and feedback loops (see also subsection 3.4.5). Over-reliance on AI-mediated social interactions could reshape social structures, potentially weakening real-world engagement and altering traditional mechanisms of emotional regulation and critical thinking.

- ***Risks posed by AI-integrated security and law enforcement***

Immersive technologies could reshape law enforcement and military operations, with digital twins, spatial computing and predictive analytics providing real-time situational awareness[247,248]. These advances could create significant value by improving risk assessment and crisis response. However, they also introduce ethical concerns concerning autonomous security systems, robotic patrols and AI-controlled surveillance.

The convergence of digital and physical interactions further contributes to these risks. Immersive environments, telepresence robotics and AI-assisted autonomous systems could lead to misjudgements in real-world navigation, increasing the likelihood of accidents, collisions and misinterpretations of physical surroundings. Autonomous systems that interact with humans may misinterpret behaviours, leading to unintended consequences.

As such, the expansion of AI-powered policing and military robotics raises concerns about autonomy, accountability and civil rights – particularly in contexts in which AI may make decisions over the use of force or monitoring public behaviour[249]. For more information, see Section 3.2 and subsection 3.4.4.

- ***Economic disruptions and transformation of the workforce***

Immersive workspaces, AI-driven decision-making, digital labour markets and decentralised virtual economies offer the potential to introduce fundamental shifts in employment structure and relationships. As well as creating new economic opportunities, this will put certain professions and jobs at risk[250]. When work increasingly takes place within hybrid digital-physical spaces, the relationships between employees and employers change. Societies might need to agree on new models for job security, taxation and legal protections for workers[251]. For more information, see subsections 3.7.2 and 3.7.3.

Web 4.0 and virtual worlds are set to disrupt traditional business models and sectors by enhancing efficiency, consumer engagement and operational processes via technologies such as digital twins, AI and spatial computing. However, companies that lack access to the necessary skills and digital infrastructure, or which are slow to adopt these technologies, risk falling behind – thereby deepening

---

246 Hariyady, H., Ibrahim, A.A., Teo, J., Suharso, W., Barlaman, M.B.F., Bitaqwa, M.A., Ahmad, A., Yassin, F.M., Salimun, C., & Weng, N.G. (2024). Virtual reality and emotional responses: A comprehensive literature review on theories, frameworks, and research gaps. *ITM Web of Conferences*, 63, 01022. Available at: https://doi.org/10.1051/itmconf/20246301022

247 National Security Technology Accelerator (NSTXL). (2023, 18 April). Immersive technologies in the US military. Available at: https://nstxl.org/immersive-tech-in-the-military/

248 V-Armed. (2025, 28 January). Virtual Reality Training for Law Enforcement: Enhancing Tactical and Decision-Making Skills. V-Armed. Available at: https://www.v-armed.com/2025/01/virtual-reality-training-for-law-enforcement-enhancing-tactical-and-decision-making-skills/

249 Morgan, F. E., Boudreaux, B., Lohn, A. J., Ashby, M., Curriden, C., Klima, K., & Grossman, D. (2020, 28 April). Military applications of artificial intelligence: Ethical concerns in an uncertain world. RAND Corporation. Available at: https://www.rand.org/pubs/research_reports/RR3139-1.html

250 World Economic Forum. (2025). The Future of Jobs Report 2025. World Economic Forum. Available at: https://reports.weforum.org/docs/WEF_Future_of_Jobs_Report_2025.pdf

251 Soueidan, M. H., & Shoghari, R. (2024). The impact of artificial intelligence on job loss: Risks for governments. Technium Social Sciences Journal, 57 :206-223, A New Decade for Social Change. Available at: https://www.researchgate.net/publication/380472833_The_Impact_of_Artificial_Intelligence_on_Job_Loss_Risks_for_Governments

digital divides and losing competitive advantage. This risk is further elaborated upon in subsection 3.6.23.6.4.

- ***Legal rights, AI liability and identity in hybrid worlds***

Digital-physical integration will demand fundamental adaptations in traditional legal systems, particularly with regard to digital identity and accountability in hybrid environments. Legal frameworks will need to establish clear protocols regarding users' ownership and control of their AI-generated identities, avatars and decentralised credentials across multiple digital and physical spaces. Accountability structures will need to be developed for AI-driven systems that make critical medical, legal and financial decisions. National legal systems will require new mechanisms to effectively govern automated financial transactions and decentralised digital property. These developments will necessitate comprehensive legal frameworks that explicitly determine responsibility, liability and enforcement methods for virtual and hybrid environments[252,253,254,255]. These aspects are also further described in Sections 3.6 and 4.4.

[252] Beckers, A., & Teubner, G. (2022). *Three liability regimes for artificial intelligence: Algorithmic actants, hybrids, crowds*. Bloomsbury. Available at: https://british-association-comparative-law.org/2022/06/17/three-liability-regimes-for-artificial-intelligence-algorithmic-actants-hybrids-crowds-bloomsbury-2022-by-anna-beckers-and-gunther-teubner/

[253] European Parliament (2020). Artificial Intelligence and Civil Liability. European Parliamentary Research Service. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf

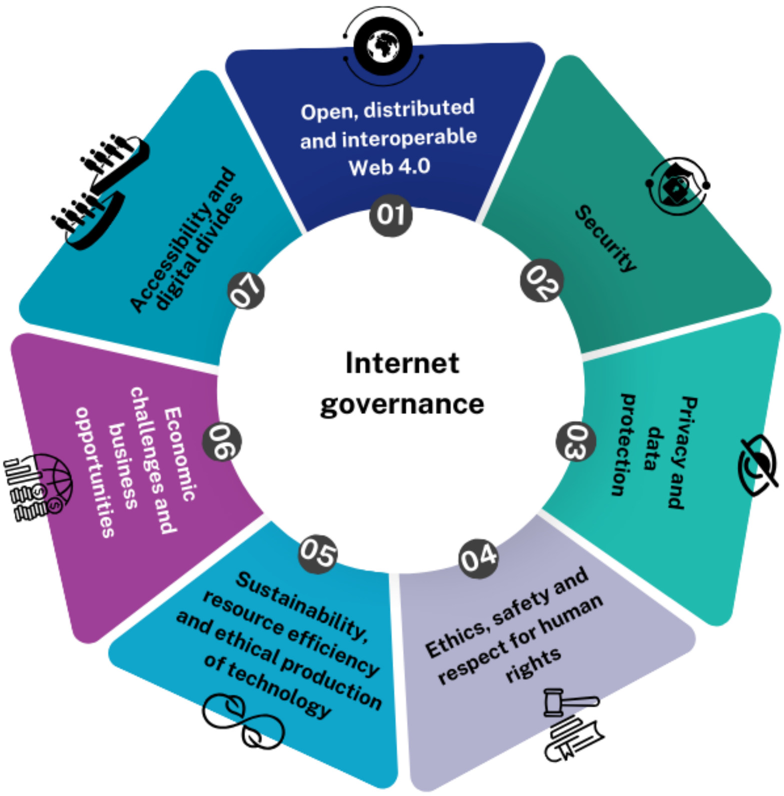
[254] European Commission (2020). White Paper: On Artificial Intelligence - A European approach to excellence and trust (COM(2020) 65 final). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0065

[255] European Parliament (2025). AI Liability Directive: draft proposal for the Artificial Intelligence Liability Directive (AILD. European Parliament Committees. Available at: https://www.europarl.europa.eu/committees/en/ai-liability-directive/product-details/20250130CDT14004

3. Web 4.0 and key internet governance challenges and needs

This chapter outlines the key challenges and needs resulting from the technological advances discussed in Chapter 2. These include the open, distributed and interoperable internet architecture that underpins Web 4.0, as well as security, privacy and data protection; ethics, safety and respect for human rights; sustainability and resource efficiency; economic challenges and business opportunities; and accessibility and digital divides.

Figure 3. Areas of challenges and needs with regard to the governance of Web 4.0 and virtual worlds, from the perspective of internet governance



3.1. An open, distributed and interoperable Web 4.0

While the internet and the web have gone through many evolutions (see Section 1.1), since the 1980s their main characteristics have been an open networking approach based on the TCP/IP protocol, distributed control and interoperability[256]. However, maintaining interoperability will be a key challenge

[256] Internet Society (2020). The Internet Way of Networking: Defining the critical properties of the Internet. Available at: https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/

on the future internet and in the evolution towards Web 4.0[257]. This challenge is identified by both commercial parties and standardisation bodies, as well as in the online consultation[258].

The key challenge is the potential **fragmentation of the future internet into different splinternets**. The IGF Policy Network on Internet Fragmentation (PNIF) differentiates between three types of fragmentation that are closely interrelated: fragmentation of the internet user experience; fragmentation of internet governance and coordination; and fragmentation of the internet's technical layer (see also Section 4.3)[259]. The term "splinternet" refers to the increasing fragmentation of the global internet into separate, nationally or regionally controlled networks. This includes the creation of national firewalls, content restrictions and the development of parallel digital ecosystems. It also encompasses divergence in technical standards and protocols between different countries or regions – for example, in mobile communications, encryption, data exchange and payments. Potential fragmentation of the future internet could have multiple causes, such as technical factors, a reduction in the flexibility of networks (or internet "ossification"), as well as pressure from state actors[260]. The technical factors that specifically impact the risk of fragmentation can be seen in the integration of AI in network management (see Section 2.3), interoperability issues among diverse IoT protocols (see Section 2.2), and the new network arising from the emergence of immersive technologies (see Section 2.4). Furthermore, the coexistence of advanced technologies such as non-terrestrial networks (NTN) alongside traditional mobile networks (see Section 2.32.3) further emphasises the need for unified, interoperable standards to prevent isolated, fragmented systems.

Organisations including the Internet Society are working to actively prevent fragmentation of the internet into splinternets[261,262]. In addition, the IGF PNIF serves as a platform for multistakeholder discussion surrounding the risks of internet fragmentation[263].

The third challenge is the **interoperability of virtual worlds**, which underpin the future Web 4.0**.** Multiple virtual worlds have already been developed, especially by the video game industry, in which assets, avatars and objects are not transferable to other worlds. Currently, virtual worlds are far from interoperable and remain immature (2 on a scale of 5, according to the Metaverse Maturity Model)[264]. Standardisation efforts are ongoing – for instance, through the ITU Metaverse Focus Group[265], and by the IETF, W3C[266] and Khronos[267]. The ITU also plays a role through its work on telecommunications standards; however the organisation has also been considering extending this work to adjacent areas, which may overlap with domains traditionally managed by the IETF, such as core internet architecture.

---

257 From the project stakeholder consultation.

258 In the online consultation, 16 out of 66 respondents (24 %) fully agreed that the TCP/IP stack and its underlying principles should be maintained to ensure continuity and stability, while 18 respondents (27 %) somewhat agreed with the statement. In contrast, 3 out of 66 respondents (5 %) expressed strong disagreement, whereas 4 people (6 %) partially disagreed. A total of 11 out of 66 respondents (17 %) were neutral on the topic (responding "neither agree nor disagree"), while 14 out of 66 (21 %) offered no opinion.

259 Internet Governance Forum (IGF) (2025, January). Policy Network on Internet Fragmentation – Output Report. IGF 2024. Available at: https://intgovforum.org/en/filedepot_download/256/28579

260 European Parliament: Directorate-General for Parliamentary Research Services, Perarnaud, C., Rossi, J., Musiani, F., & Castex, L. (2022). 'Splinternets' – Addressing the renewed debate on internet fragmentation. European Parliament. Available at: https://data.europa.eu/doi/10.2861/183513

261 Campbell N. (2022, May). Protecting the internet as we know it: Three things you can do today to stop the splinternet. Internet Society. Available at: https://www.internetsociety.org/blog/2022/05/protecting-the-internet-as-we-know-it-three-things-you-can-do-today-to-stop-the-splinternet/

262 Internet Society (2022, April). US, EU, and G7 commitment will slow the splinternet, but more work is needed. Internet Society. Available at: https://www.internetsociety.org/blog/2022/04/us-eu-and-g7-commitment-will-slow-the-splinternet-but-more-work-needed/

263 IGF (2024). Main Session Policy Network on Internet Fragmentation @IGF2024. Avoiding Internet Fragmentation: Understanding and Contributing to Operationalising the GDC Commitment Policy Network on Internet Fragmentation. Available at: https://www.intgovforum.org/en/content/policy-network-on-internet-fragmentation

264 Weinberger, M., & Gross, D. (2022). A Metaverse Maturity Model. *Global Journal of Computer Science and Technology*, 22(H2), 39–45. Available at: https://doi.org/10.34257/GJCSTHVOL22IS2PG39

265 ITU Focus Group on metaverse (FG-MV) (2023). Technical Specification ITU FGMV-19 - Service scenarios and high-level requirements for metaverse cross-platform interoperability. Available at: https://www.itu.int/en/ITU-T/focusgroups/mv/Documents/List%20of%20FG-MV%20deliverables/FGMV-19.pdf

266 World Wide Web Consortium (W3C) (2021). Metaverse Interoperability Community Group. Available at: https://www.w3.org/community/metaverse-interop/

267 Khronos Group (2025). The 3D Asset Delivery Format - glTF (Graphics Language Transmission Format). Khronos Group. Available at: https://www.khronos.org/gltf/

These overlaps, if not properly coordinated, could result in conflicting standards and contribute to fragmentation. Moreover, while global standards developed on a consensual basis aim to promote interoperability, they can inadvertently impose rigid frameworks that risk centralisation and may not adequately safeguard human rights. This observation aligns with the feedback received from the online consultation, in which respondents emphasised the importance of ensuring that interoperability is achieved without compromising the open, decentralised ethos of the internet. The Metaverse Standards Forum was established in 2022. Its main goal is to foster and accelerate the development of standards for open metaverse interoperability[268].

In the online consultation conducted during the preparation of this paper, interoperability between technologies and platforms emerged as the top challenge to achieving the evolution to Web 4.0, given the current internet architecture – chosen by 48 out of 68 respondents (70.6 %) (see Annex 2). When justifying their answers, several stakeholders stressed that Web 4.0 should not consist of isolated platforms, but should rather form an interconnected environment in which users and companies can seamlessly use their data, avatars and assets across platforms.

In addition to the challenges of interoperability and fragmentation, the evolution towards Web 4.0 raises significant concerns about **centralisation**. Since the 1980s, the open, distributed nature of the internet has been a cornerstone of its success. However, a gradual shift has occurred from the decentralised Web 1.0 and Web 3.0 towards more platform-driven services (see Chapter 1) and the convergence of technologies that increasingly rely on proprietary standards and infrastructures (see Chapter 2), as well as an ecosystem increasingly dominated by apps instead of web browsing[269]. This had led to a growing risk that control may be concentrated in the hands of a few dominant actors. For example, large technology companies, which control the dominant app stores, restrict interoperability by curating and limiting access to mobile apps. Similarly, proprietary ecosystems in which assets, avatars and digital economies are locked into closed platforms demonstrate how centralisation can hinder the open exchange of digital assets and user data. Furthermore, the consolidation of cloud services pose the risk of creating single points of failure and bottlenecks in digital trust infrastructure. Thus, these risks stemming from centralisation require robust governance frameworks to reduce the risk of power becoming concentrated, while maintaining a truly open, secure and interoperable Web 4.0 ecosystem.

Lastly, **the need to preserve net neutrality** has been questioned in view of evolution towards Web 4.0. The principle of net neutrality means that internet service providers (ISPs) are required to treat all internet traffic equally, without discrimination on the basis of content, user, platform, application or device. This is a foundational principle for an open internet[270]. Net neutrality prevents ISPs from creating "fast lanes" for preferred content providers or throttling access to competing services. This principle supports free speech, equal access and fair competition between internet applications and content providers. The evolution towards Web 4.0 builds on new technologies such as "network slicing" in mobile 5G networks, and the development of 6G networks and technologies such as edge computing and others[271]. These developments require significant investments, and stakeholders disagree over the extent to which net neutrality fosters such investment, or whether a reinterpretation of this principle is needed.

---

268 Metaverse Standards Forum (2024). Leading standards organizations and companies unite to drive open metaverse interoperability. Metaverse Standards Forum. Available at: https://metaverse-standards.org/news/press-releases/leading-standards-organizations-and-companies-unite-to-drive-open-metaverse-interoperability/

269 Sandvine (March 2024). Global Internet Phenomena Report 2024. Sandvine. Available at: https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/2024/GIPR/GIPR%202024.pdf

270 Lohninger, T., Gollatz, B., Hoffmann, C., Steinhammer, E.E., Deffaa, L.B., Al-Awadi, A., & Czá, A. (2019, 29 January). The net neutrality situation in the EU: Evaluation of the first two years of enforcement. Epicenter.works. Available at: https://cyberlaw.stanford.edu/content/files/sites/default/files/2019_netneutrality_in_eu-epicenter.works-r1.pdf

271 Netflix (no date). Netflix Open Connect Program. Available at: https://openconnect.netflix.com/en/

3.2. Security

Ensuring stability, security and safety has long been a priority in internet governance, with the WSIS Action Line C5 "Building confidence and security in the use ICTs" outlining specific areas for action in safeguarding security and countering cyber threats[272]. As Web 4.0 is characterised by the blurring of physical and virtual worlds, **security issues that exist in the physical world will therefore also exist in virtual worlds**.

Furthermore, the evolution towards Web 4.0 brings about **new vulnerabilities** that extend beyond traditional cyber threats. The International Criminal Police Organization (INTERPOL) has identified 10 potential areas of criminal activity "in and through the Metaverse"[273]. These include property crime, financial crime, terrorism, cybercrime, crimes against children, identity crime, crimes against public safety, intellectual property crime, acts intended to cause fear and emotional distress, and sexual offences and assault. Each of these areas is further divided into further potential sub-crimes[274]. Cyberattacks are increasingly targeting essential digital infrastructure and financial systems, as well as individual identities[275]. The blurring of physical and virtual environments introduces novel forms of identity theft, financial fraud and digital asset manipulation[276,277]. Other risks include social engineering attacks and the malicious misuse of advanced technologies[278], the exploitation of virtual marketplaces and smart contracts, threats to virtual assets (e.g. NFTs, digital currencies, tokenised virtual real estate, virtual goods sold in online marketplaces, reward tokens) as well as identity- and context-aware malware[279]. The growing interconnectedness of devices and digital services amplifies these risks, making security failures not only more disruptive, but also increasing their potential to have cascading impacts across multiple systems.

Virtual worlds represent **a new economy** in which virtual land, customised avatars and experiences are sold, owned and transferred. Blockchain technologies are used to make digital ownership more secure and decentralised, removing control from platform providers and social networks. Ownership of digital assets is stored on a blockchain, on which assets are identified through the use of non-fungible tokens (NFTs). While this approach addresses certain vulnerabilities, cybercriminals can still exploit weaknesses in the digital wallets and exchanges that interact with the blockchain[280]. Once stolen, these assets are very difficult to recover[281].

Internet security has relied heavily on **standardised encryption algorithms** to protect data and ensure secure communication. A new risk is now arising as a result of advances in quantum computing, which threatens to "crack" the encryption algorithms used by digital signatures (such as those used in

272 ITU (2003) WSIS Plan of Action. Available at: https://www.itu.int/net/wsis/docs/geneva/official/poa.html

273 INTERPOL. (2024). Metaverse: A law enforcement perspective: Use cases, crime, forensics, investigation, and governance [White paper].

274 Karapatakis, A. (2025), Metaverse crimes in virtual (Un)reality: Fraud and sexual offences under English law, *Journal of Economic Criminology*, Volume 7, 100118, ISSN 2949-7914, Available at: https://doi.org/10.1016/j.jeconc.2024.100118

275 Internet Governance Forum (IGF). (2024). Riyadh IGF Messages – Draft version. IGF 2024, Riyadh. Available at: https://intgovforum.org/en/filedepot_download/305/28526

276 IGF (2024). Main Session 2: Protecting Internet infrastructure and general access during times of crisis and conflict.

277 Shandler R., Canetti D., & Mimran T. (2024, 3 May). A look inside the cyberwar between Israel and Hamas reveals the civilian toll. The Conversation. Available at: https://theconversation.com/a-look-inside-the-cyberwar-between-israel-and-hamas-reveals-the-civilian-toll-228847

278 European Parliamentary Research Service (EPRS) (2024, July). The protection of mental privacy in the area of neuroscience - Societal, legal and ethical challenges. European Parliament. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2024/757807/EPRS_STU(2024)757807_EN.pdf

279 European Commission: Joint Research Centre, Hupont Torres, I., Charisi, V., De Prato, G., Pogorzelska, K. et al. (2023), Next generation virtual worlds – Societal, technological, economic and policy challenges for the EU, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2760/51579

280 The Science Times (2025, 19 January). Crypto security: Safeguarding digital assets. *The Science Times*. Available at: https://www.sciencetimes.com/articles/60235/20250119/crypto-security-safeguarding-digital-assets.htm

281 The Fintech Times (2025 March 15). Cybercriminals double down: Attacks on digital wallets, cryptocurrency exchanges, and BNPL companies. Available at: https://thefintechtimes.com/cybercriminals-double-down-attacks-on-digital-wallets-cryptocurrency-exchanges-and-bnpl-companies/

DNSSEC) and key exchanges for privacy (such as those used in TLS)[282,283]. To address this threat, work is already underway on post-quantum cryptography algorithms that can interoperate with existing communications protocols and networks[284 285]. Even if post-quantum cryptography standards become widely available before the technology becomes capable of cracking key encryption algorithms, a situation of "catch now, exploit later", whereby bad actors collect currently unreadable data in the hope of decrypting it later when technology allows, remains a threat[286].

Artificial intelligence provides a whole new toolkit[287] to enable cyber-attacks, automating their planning, intrusion and execution, while circumventing traditional cyber-security measures. For example, AI can provide new ways of orchestrating attack networks using botnets, typically employed in Denial-of-Service (DoS) attacks. While botnet attacks are already a critical challenge for organisations, AI-powered botnets can attack for a longer amount of time and can easily change their tactics from one type of DoS attack to another in real time. They can adapt and refine their attacks, executing changes without the need for human intervention. The speed at which AI-powered botnets are able to evolve also makes them harder to detect and mitigate than traditional botnets, which increases the pressure on security teams[288]. Moreover, the use of AI for cyberattacks is not limited to systems and software, but also to humans. Recent advances in generative AI have led to the phenomenon of AI impersonation. The copying of a voice or facial images allows real-time impersonation, enabling social engineering attacks aimed at online extortion or even the execution of offline attacks[289,290]. At the same time, security agencies and private companies are increasingly using AI to address new cyber-threats. Such applications of AI will only increase in the future.

The key initiatives to mitigate AI-related risks include the WEF (AI Governance Alliance), the Centre for International Governance Innovation (Global AI Risks Initiative) and NIST (AI Risk Management Framework) and the EU (AI Act), while SDOs such as the ISO and IEEE consider security in their AI standardisation working groups. The IEEE has even formed a specific working group dedicated to AI security[291,292].

The introduction of **brain–computer interfaces (BCIs)** for medical and non-medical applications is still in the early stages of development, but their potential application and impact is significant in relation to security risks[293]. Malicious actors could intercept, manipulate or steal brain signals, compromising user data integrity and confidentiality. AI-generated brain activity patterns could create convincing fake signals, allowing attackers to impersonate users or access sensitive information. BCI-enabled interfaces could manipulate users' thoughts, emotions or decisions, influencing their behaviour without them being aware of it. Brain signals contain highly personal information, necessitating robust data protection mechanisms to prevent unauthorised access or disclosure. Brain signals can also be

---

282 NIST (2025). Block cipher techniques project. NIST Computer Security Resource Center (CSRC). Available at: https://csrc.nist.gov/Projects/block-cipher-techniques

283 PPMI & TNO (2025, forthcoming). Future of the internet. Project 'Participatory Foresight for Next Generation Online Platforms'.

284 Hoffman, P. (2022, 11 February). The impact of quantum computing on cryptography and the DNS. ICANN Office of the Chief Technology Officer (OCTO-031). Available at: https://www.icann.org/en/system/files/files/octo-031-11feb22-en.pdf

285 NIST (2024, August). NIST releases first 3 finalized post-quantum encryption standards. NIST. Available at: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

286 Vermeer M.J.D., & Peet E.D. (2020). Securing communications in the quantum computing age: Managing the risks to encryption. RAND Corporation. Available at: https://www.rand.org/pubs/research_reports/RR3102.html

287 Kaloudi, N., & Li, J. (2020). The AI-based cyber threat landscape: A survey. *ACM Computing Surveys (CSUR),* 53(1), 1–34. Available at: https://doi.org/10.1145/3372823

288 IoT Insider (2024). Battling AI-powered botnets: Evolving challenges in mitigating non-human threats. IoT Insider. Available at: https://www.iotinsider.com/iot-insights/battling-ai-powered-botnets-evolving-challenges-in-mitigating-non-human-threats/

289 Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*. Available at: https://doi.org/10.1007/s10462-024-10973-2

290 CyberNews (2023, 9 May). Lessons learned from ChatGPT's Samsung leak. CyberNews. Available at: https://cybernews.com/security/chatgpt-samsung-leak-explained-lessons/

291 European Telecommunications Standards Institute (ETSI) (2025). Technical Committee on Securing Artificial Intelligence (TC SAI). Available at: https://www.etsi.org/committee/technical-committee-tc-securing-artificial-intelligence-sai

292 The Centre for Emerging Technology and Security (CETaS). (2024). Towards secure AI: How far can international standards take us? The Alan Turing Institute. Available at: https://cetas.turing.ac.uk/publications/towards-secure-ai

293 Radu, R. (2024). Neurotechnologies and the future of internet governance. European University Institute. Available at: https://cadmus.eui.eu/bitstream/handle/1814/77410/RSC_IB_2024_Radu.pdf

amplified or interfered with, potentially disrupting BCI systems or compromising their accuracy. As the use of BCIs becomes more prevalent, malicious code could target specific aspects of brain activity, exploiting vulnerabilities in BCI systems. Integrating BCIs into online interactions could lead to unintended consequences, such as brain signals being used against users' will or AI-generated content being perceived as realistic. Users may not fully understand the implications of BCI technology, leading to a lack of informed consent or insufficient awareness of the risks. The use of BCIs raises complex ethical questions, such as the potential for AI-generated content to manipulate users' beliefs, or the ethics of using brain signals to influence behaviour.

3.3. Privacy and data protection

When asked about the key governance and ethical challenges associated with virtual world**s,** respondents to the consultation carried out during the preparation of this paper ranked privacy and data security risks as the most significant concern, with 48 out of 58 respondents (86 %) identifying it as either "very" or "extremely" challenging (see Annex 2). The scale and complexity of the data collection, behavioural tracking and biometric analysis enabled by technologies related to Web 4.0 create significant risks for individuals and organisations[294,295,296]. Several interviewees pointed out that the potential for algorithmic manipulation, commercial exploitation and the misuse of biometric identifiers adds to these concerns, making data protection frameworks an issue that is central to governance.

A key feature of this trend is the **depth and granularity** of the data collected. Immersive technologies, IoT devices and AI analytics all generate vast amounts of biometric and behavioural data, including facial recognition, voice analysis, gaze tracking, haptics and real-time physiological responses[297,298]. Added to these is the ability to collect and process brain activity data through **neurotechnologies and BCIs**. Unlike health and wellness data currently collected through wearables, neuro-data has the potential to reveal subconscious thoughts, emotional states and cognitive processes – raising ethical concerns about personal autonomy[299,300]. Such data can be (mis)used for various purposes, including surveillance, manipulation and online harms, among others (further explained in Section 3.4).

294 World Economic Forum (2023). Metaverse: Privacy and safety. Available at: https://www3.weforum.org/docs/WEF_Metaverse_Privacy_and_Safety_2023.pdf

295 Ladikas, M., Madeira, O., Hahn, J., Correa Pérez, M., Caplice, G., & Gerasymenko, A. (2024). *D3.1: State-of-art in XR policy debates*. In M. Ladikas & M. Correa Pérez (Eds.), The Equitable, Inclusive, and Human-Centered XR Project (XR4Human) (Deliverable No. 3.1). Karlsruhe Institute of Technology (KIT). Grant Agreement No. 101070155 Available at: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5fb30fb9f&appId=PPGMS

296 Stakeholder interviews (see Annex 3).

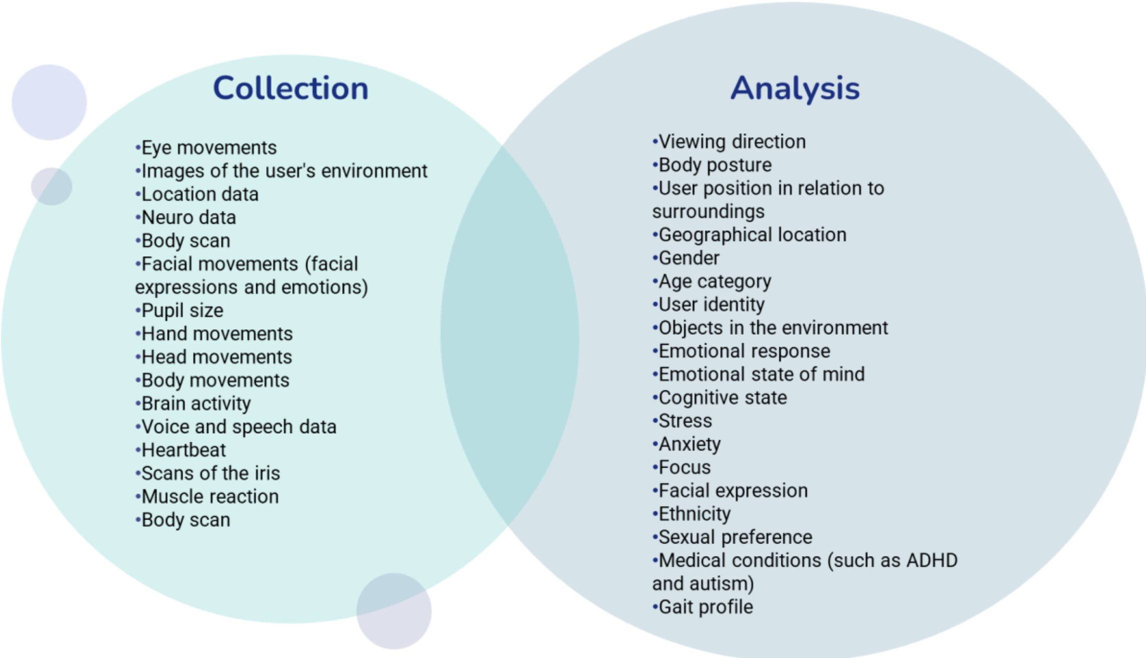
297 European Parliamentary Research Service (EPRS) (2024, July). The protection of mental privacy in the area of neuroscience - Societal, legal and ethical challenges. European Parliament. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2024/757807/EPRS_STU(2024)757807_EN.pdf

298 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., & Vespe, M. (2023), Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU, Publications Office of the European Union, Luxembourg, Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC133757

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

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

Figure 4. Examples of data collected and analysed in immersive environments



Source: European Commission (2023)[301].

The use of AI-driven personalisation and profiling in Web 4.0 environments amplifies concerns about discrimination, algorithmic bias and economic exploitation. AI-powered systems can segment users on the basis of behavioural data in order to optimise engagement, but they also enable new levels of consumer discrimination, such as individualised pricing models and hyper-targeted content manipulation[302].

The growing adoption of **digital fingerprinting** (as an alternative to cookies) further challenges existing privacy safeguards. Unlike cookies, which require user consent under regulations such as the GDPR, fingerprinting techniques track users without their explicit awareness, by analysing unique device and browsing characteristics[303]. The increasing use of AI-driven digital fingerprinting, which adapts in real time to changes in user behaviour, makes it harder to detect and regulate.

Moreover, some respondents to the online consultation suggested that under Web 4.0, users should have more granular control over personal data. This should be achieved by minimising the collection of personal data and through enhanced privacy settings and decentralised storage solutions, accompanied by stronger data protection standards and privacy-by-design principles embedded from the early stages of development (see Annex 2). Web 4.0 operates across **decentralised, globally distributed infrastructures**, making it more difficult to enforce privacy laws and users' rights. Differences in regional privacy frameworks (e.g. the GDPR in the EU, the CCPA in California, and China's PIPL) create fragmentation and uncertainty for businesses and users alike[304]. It is therefore relevant for privacy safeguards to consider the entire Web 4.0 technology stack, including AI models, XR systems, IoT networks and decentralised identity frameworks[305].

---

301 European Commission (2023). Shaping the Next Generation of Virtual Worlds – Science for Policy event. Available at: https://webcast.ec.europa.eu/shaping-the-next-generation-of-virtual-worlds-science-for-policy-event-23-11-08

302 World Bank (2024). Digital Progress and Trends Report 2023. World Bank Open Knowledge Repository. Available at: https://openknowledge.worldbank.org/server/api/core/bitstreams/95fe55e9-f110-4ba8-933f-e65572e05395/content

303 Information Commissioner's Office (ICO) (2024, December). Our response to Google's policy change on fingerprinting. ICO. Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/12/our-response-to-google-s-policy-change-on-fingerprinting/

304 Internet Governance Forum (IGF) (2024). Lightning Talk #136 – The Embodied Web: Rethinking Privacy in 3D Computing. IGF 2024. Available at: https://dig.watch/event/internet-governance-forum-2024/lightning-talk-136-the-embodied-web-rethinking-privacy-in-3d-computing.

305 TNO (no date). PET Lab – Secure multi-party computation and privacy-enhancing technologies. TNO. Available at: https://www.tno.nl/en/technology-science/technologies/secure-multi-party-computation/pet-lab/

Next to the data collected in immersive environments, there is also need to protect user created data, e.g. avatar or virtual world platform assets. This creative content needs protection against misuse and tampering: for instance avatars are a persistent representation of one's self, providing authentication and trust when engaging in an immersive experience with others. Some virtual world platforms also offer users the capability to create their own (public) space, to create games or artistic content. Intellectual property protection of these digital assets should follow the same rules as in the physical world. For the protection of intellectual property rights and industrial property rights, the existing legal framework in the EU (such as the Directive on Copyright in the Digital Single Market, the Regulation on the EU Trade Mark and the Directive on the Protection of Trade Secrets) applies generally to Web 4.0 and virtual worlds.

3.4. Ethics, safety and respect for human rights

The extension of **human rights** to online spaces has been a cornerstone of internet governance, at least in principle and in formal declarations. Recently, the Global Digital Compact introduced unprecedented language, underlining a renewed and heightened commitment to embedding these rights into the evolving digital landscape: "We commit to respect, protect and promote human rights in the digital space. We will uphold international human rights law throughout the life cycle of digital and emerging technologies so that users can safely benefit from digital technologies and are protected from violations, abuses and all forms of discrimination." Similar commitments to uphold the Universal Declaration of Human Rights are echoed in the Declaration for the Future of the Internet, the Tunis Agenda and NETmundial, among other declarations and discussion forums[306,307,308].

Questions about internet architecture have implications that are more than just technical. As the internet has become integral to our lives, technical standards and protocols have come to have a bearing on users' autonomy, privacy and safety online[309]. There is growing recognition within the internet governance community that decisions about protocols, domain names and algorithms have a significant impact on human rights[310]. In particular, recent challenges such as unauthorised data exposure and targeted behavioural advertising have underlined the impact infrastructure choices can have on individual rights and freedoms[311]. Open standards also help to ensure greater inclusivity by allowing marginalised groups the opportunity to access the internet, as well as helping to protect privacy and preventing monopolistic practices by tech companies[312].

Of course, the challenges to human rights, ethics and safety that could emerge as a result of advances towards Web 4.0 and virtual worlds are not restricted to the architecture of the internet. For instance, the advancement of neurotechnological devices will raise moral questions about mental integrity, which is closely interlinked with human dignity[313]. The use of behavioural data and advanced AI algorithms to personalise experiences can lead to hyper-targeted content and services tailored towards individuals and their specific emotional states, thereby potentially undermining freedom of thought and autonomy. The behavioural and movement data collected in virtual environments can allow individuals to be identified across multiple sessions, regardless of other identifiers (e.g.

306 High Level Multi-stakeholder event on the Future of the Internet (2022). Available at: https://www.youtube.com/watch?v=9aGsZLxLDOY
307 WSIS (2003). Declaration of Principles. Building the Information Society: a global challenge in the new Millennium. Available at: https://www.itu.int/net/wsis/docs/geneva/official/dop.html
308 NETmundial (2014). NETmundial Multistakeholder Statement. Available at: https://netmundial.br/2014/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf
309 Neyer, J. (2022). After global governance. *Z Politikwiss,* 32, 361–382 (2022). https://doi.org/10.1007/s41358-021-00290-3
310 Zalnieriute, M., & Milan, S. (2019). Internet architecture and human rights: Beyond the human rights gap. *Policy & Internet*, 11(1), 6-15.
311 Ibid.
312 IGF (2024). WS #75 An Open and Democratic Internet in the Digitization Era.
313 European Parliamentary Research Service (2024). Scientific Foresight Unit (STOA). The protection of mental privacy in the area of neuroscience. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2024/757807/EPRS_STU(2024)757807_EN.pdf

username, avatar). This creates new challenges for to the safeguarding of anonymity and privacy online[314,315].

Despite widespread agreement as to the importance of extending human rights to the digital realm, the reality of their implementation often diverges between countries and sectors. This divergence is likely to be further amplified as Web 4.0 and virtual world technologies become deployed. The rest of this section is divided into six subsections, each of which is dedicated to a specific challenge in ensuring a safe and ethical Web 4.0 and virtual worlds that respect human rights.

Figure 5. Dimensions of ethics, safety and human rights

3.4.1. *Manipulation and disinformation*

Advances in Web 4.0 and virtual worlds introduce risks **related to manipulation**, as well as the **spread of misinformation and disinformation**. The hyper-personalisation associated with virtual environments can be deliberately used to influence users' behaviour and preferences in both subtle and direct (i.e. coercive) ways. This can include, for example, the use of highly realistic stolen identities or fake, manipulative or coercive content highly tailored to users' preferences, behaviour and emotional states

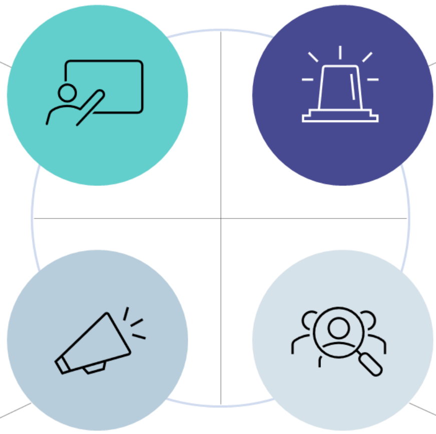
Manipulation in Web 4.0 comes from AI's symbiotic relationship with users, whereby intuitive systems influence decisions by exploiting behaviour and preferences in subtle ways. A few distinctive types of manipulation can be distinguished: persuasion, coercive threats, disinformation, deceit and subversion. These are presented in the figure below, and elaborated upon in the paragraphs that follow.

---

314 Nair, V., Guo, W., Mattern, J., Wang, R., O'Brien, J.F., Rosenberg, L., & Song, D. (2023). Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data. https://doi.org/10.48550/ARXIV.2302.08927

315 XR4Human (2023) D3.1: State-of-art in XR policy debates. Available at: https://xr4human.eu/wp-content/uploads/2024/10/XR4HUMAN_D3.1.pdf

Figure 6. Examples and types of interference in Web 4.0 and virtual worlds



Persuasion

Advertising that uses rational persuasion without false claims or concealed manipulation.
Social media influencers promoting products or ideas.
Educational and awareness raising campaigns in virtual environments.
Content recommendation systems transparently showing why specific content is being suggested based on past preferences.
Virtual assistants offering suggestions for improving productivity based on user input.

Coercive threats

Threats of account banning, legal action or penalties for undesirable behaviour.
Extortion or blackmail using sensitive user data.
Economic coercion, such as platform-specific penalties that discourage users leaving.
Virtual worlds may enable new forms of social coercion, such as locking users out of essential virtual environments or restricting access to digital assets.
Blocking or restricting access to specific websites, platforms, or content deemed undesirable.
The use of internet shutdowns or access restrictions as a form of punishment or suppression.

Disinformation & deceit

Disinformation campaigns spreading false news.
False advertising about digital products or platforms' terms of use.
Use of fake or stolen identities/ avatars or AI agents to deceive the user.

Subversion

Behavioural nudging through interface design (e.g. to promote engagement and addictive behaviours).
Targeted ads exploiting emotional vulnerabilities.
Recommendation systems suggesting content based on emotional or behavioural data.
Algorithms creating polarising or radicalising echo chambers.

Source: Sætra & Mills (2022)[316]; Council of Europe. (2024)[317]; IGF (2024)[318] authors' elaboration.

- **Persuasion**

Persuasion is an active attempt to change someone's attitudes, beliefs or emotions without using force or coercion. Unlike manipulation or pressure tactics, persuasion operates through communication and influence. It is thus different from the other types of interference mentioned below, as it is not covert. However, with the development of the Web 4.0 and virtual worlds, persuasion could evolve to include new, multimodal types of advertising, as well as more targeted content recommendation systems.

- **Coercive threats**

Virtual worlds could enable new forms of social coercion. Existing threats could further develop into new forms, posing a risk to the users of immersive environments. Currently, coercive threats include account banning, blackmail using sensitive user data, as well as blocking or restricting access. These threats could emerge under Web 4.0, and could include locking users out of essential virtual environments or restricting access to digital assets. Blackmail could exploit sensitive personal data. Moreover, virtual worlds may enable the confiscation or freezing of digital assets tied to user behaviour. Real-time monitoring of neurotechnological or biometric data could enable malicious actors to identify and oppress individuals who express dissenting thoughts or emotions.

- **Subversion**

In Web 4.0 and virtual worlds, **subversion** could become a sophisticated challenge that blurs the boundary between genuine influence and covert manipulation. As virtual worlds become highly realistic, the potential impact of subversion grows. Immersive environments could amplify this by

[316] Sætra, H.S., & Mills, S. (2022). Psychological interference, liberty and technology. *Technology in Society*, 69, 101973.

[317] Council of Europe (2024). *The metaverse and its impact* on human rights, the rule of law, and democracy. Retrieved from https://rm.coe.int/the-metaverse-and-its-impact-on-human-rights-the-rule-of-law-and-democ/1680b178b0

[318] IGF (2024). Lightning Talk #136 The Embodied Web: Rethinking Privacy in 3D Computing.

allowing more immersive interactions. Subversion can thus evolve into a sophisticated form of manipulation that subtly influences user behaviour across multiple digital channels[319]. Immersive experiences involve high sensory input, including vivid sights, dynamic sounds and tactile sensations delivered directly to the eyes, ears, hands and body. Behavioural nudging in Web 4.0 could thus become more intense and effective despite a lack of consent from users, as it could involve the ability to monitor of an individual's real-time actions, reactions and interactions. This could encompass every movement, gesture and response the body generates, all of which could be tracked and analysed by sensors[320]. This is especially pertinent in the case of neurotechnology, which could be used in the virtual worlds. The UN Human Rights Council Advisory Committee has emphasised the risks to human rights, particularly to freedom of thought, the right to privacy and the right to personal integrity, that arise from this technology[321].

- **Disinformation and deceit**

Existing internet governance initiatives have long emphasised the importance of a healthy infosphere. The Global Digital Compact calls for efforts aimed at "countering and addressing all forms of violence, [...] which occur through or [are] amplified by [...] misinformation and disinformation"[322]. This marks an important source of momentum for internet governance, as it highlights the threats related to disinformation and its potential impact on all internet users.

Abuse of the digital space for the purposes of electoral interference provides a stark example of how the internet can be weaponised to spread propaganda and disinformation, undermining democracy and putting lives at risk[323]. The immersive technologies associated with Web 4.0 expand the frontiers of free expression, yet simultaneously create fertile ground for deception and misinformation campaigns[324,325]. One of the reasons for this is that immersiveness is associated with the intensification of users' perceptions[326]. Moreover, the types of data that can be collected enable misinformation to be precisely targeted. Furthermore, AI enables the production of realistic fake content, which could later be amplified by algorithms.

At present, one of the most widely used methodologies to assess disinformation, as well as foreign information manipulation and interference, is the ABCDE framework[327]. This framework focuses on five key aspects of any information operation: actor, behaviour, content, degree and effect. Here, we employ ABCDE to examine the disinformation challenges associated with virtual worlds and Web 4.0:

- **Actor**

The notion of an "actor" raises the question of what types of actors are involved in disinformation activity. With the development of Web 4.0 and virtual worlds, this definition might become more difficult. In principle, disinformation actors are likely to remain the same, and include states, media,

---

319 Rosenberg, E. (2022). *The ultimate tool of persuasion*. Responsible Metaverse. https://responsiblemetaverse.org/wp-content/uploads/2022/10/The-Ultimate-Tool-of-Persuasion-FTC-Rosenberg-with-letter.pdf

320 Rosenberg, E. (2022). *The ultimate tool of persuasion*. Responsible Metaverse. https://responsiblemetaverse.org/wp-content/uploads/2022/10/The-Ultimate-Tool-of-Persuasion-FTC-Rosenberg-with-letter.pdf

321 United Nations Human Rights Council (2024). *Report on the impact of neurotechnologies on human rights* (A/HRC/57/61). United Nations.

322 United Nations (2024). *Global Digital Compact*. United Nations. https://www.un.org/techenvoy/global-digital-compact

323 Kubiecki, R., & Legucka, A. (Eds.). (2021). *Disinformation and the resilience of democratic societies*. The Polish Institute of International Affairs (PISM).

324 Centre for European Policy (CEP) (2023). *EU Metaverse strategy: Virtual worlds (COM(2023) 442) – Long version*. Centre for European Policy.

325 Council of Europe (2023). *The metaverse and its impact on human rights, the rule of law, and democracy*. Council of Europe.

326 Linares-Vargas, B.G.P., & Cieza-Mostacero, S.E. (2025). Interactive virtual reality environments and emotions: A systematic review. *Virtual Reality, 29*(3).

327 Pamment, J. (2020). *The EU's role in fighting disinformation: Crafting a disinformation framework* (Report part: The ABCDE Framework). Carnegie Endowment for International Peace.

politicians, etc. What will be different, however, is the variety of tools they will be able to harness through the use of avatars[328].

Disinformation authors may create fake identities (avatars), similar to the fake or "troll" accounts found on social media. In virtual worlds, however, these avatars could be far more personalised and human-like. This category could include newly created fake avatars, stolen avatars (belonging to people who have lost access or have ceased to use them), as well as entire groups of avatars designed to resemble genuine users[329]. Such practices pose several potential threats.

- First, avatars are highly personalised and potentially relatable, which can foster a strong sense of connection[330]. On social media, engagement with fake accounts is already high, but is limited to specific platforms. With Web 4.0, this engagement could occur across multiple virtual worlds, heightening the risk.
- Second, avatars are likely to bear a closer resemblance to actual humans. On social media, disinformation actors are merely represented by accounts, often without a real voice or face aside from a profile picture. In Web 4.0, fake avatars might look almost identical to real people, complete with unique voices and personal features, and potentially even realistic facial expressions[331]. This level of realism increases their relatability and amplifies their potential influence on other users.
- Third, disinformation actors often use troll and bot networks to sway public opinion, creating the appearance that many people share the same viewpoint. In virtual worlds, these possibilities could be even greater. A disinformation author might stage a scene depicting a conspiracy theory and populate it with other avatars or realistic avatar images—some possibly resembling the targeted user—who appear to endorse or act out a particular narrative. This synthetic social presence could have a profound impact on users[332].

- **Behaviour**

Web 4.0 could significantly influence the behaviour of online actors and change the spectrum of activities used to spread disinformation narratives, as these would become multimodal and could include sensory experiences.

There is growing concern that the properties of virtual worlds could bring to life persuasive experiences that could be used for manipulation[333]. This could include creating multi-stimuli harmful narratives that could potentially include fake avatars or voices and images of users whose identities have been stolen. And the risk goes even further – avatars' voices may closely resemble those of people that users regard as trustworthy or who are even known to them personally. Furthermore, the vast amounts of data that immersive environments allow to be collected about users can lead to detailed insights being gained regarding user behaviour and motivations, allowing content to be tailored to ensure maximum receptiveness of the target user[334].

- **Content**

---

[328] Kshetri, N. (2024). Disinformation and misinformation in the age of artificial intelligence and the metaverse. *IEEE Micro, 57*, 110–116. https://doi.org/10.1109/MC.2024.3461325

[329] Council of Europe (2023). *The metaverse and its impact on human rights, the rule of law, and democracy*. Council of Europe.

[330] Fox, J., & McEwan, B. (2017). Distinguishing technologies for social interaction: The perceived social affordances of communication channels scale. *Computers in Human Behavior, 72*, 298–318.

[331] Council of Europe (2023). *The metaverse and its impact on human rights, the rule of law, and democracy*. Council of Europe.

[332] Brown, J.G., Bailenson, J.N., & Hancock, J. (2023). Misinformation in virtual reality. *Journal of Online Trust and Safety*. https://vhil.stanford.edu/sites/g/files/sbiybj29011/files/media/file/brown_vr.pdf

[333] Ibid.

[334] Holt, R. (2023). Watching androids dream of electric sheep: Immersive technology, biometric psychography, and the law. *Journal of Entertainment & Technology Law, 23*(1).

The content of future disinformation may not differ significantly from that which exists currently; it is likely to build on narratives that have already been created and have proven effective. What would change, however, is its form. Disinformation narratives in Web 4.0 will be multimedia and multimodal. Content could thus be realistic and visualised in great detail, bringing users to a curated space that would represent the conspiracy theory. For example, one can imagine a visualised conspiracy narrative about the moon landing – a scene could be created that enforces the narrative that it was a hoax. This could take users to a fake meeting at which officials would allegedly be discussing the aforementioned hoax.

Nevertheless, creating such scenes is a challenge. Unlike other forms of online communication such as social media, VR experiences must be built specifically for the medium. This has two implications. First, the number of actors who can create such spaces is likely to be limited. Second, the number of disinformation narratives may also be limited to a few important (and thus convincing) ones.

- **Distribution**

Web 4.0 would significantly impact the distribution of disinformation. It creates an opportunity for very widespread distribution via new channels and new forms of interaction, including direct conversations with fake avatars or with whole groups of fake accounts, resembling large and active groups. Furthermore, with its seamless blend of the virtual and real, disinformation might be found anywhere – and could thus be visible in daily activities within virtual worlds. For example, virtual worlds might allow one to add one's own remarks on a variety of tools used there as well as on a number of surfaces, including virtual representations of companies or institutions. This, too, could significantly affect the reach of new narratives in virtual worlds.

Moreover, such distribution is currently mostly human-to-human or machine-to-human (i.e. via bot networks). With Web 4.0, human-machine and machine-machine distribution should also be considered, which could result in biased virtual worlds[335].

- **Effect**

Virtual worlds could lead to disinformation narratives having a potentially greater effect its users. With moderation becoming more difficult and a variety of new methods springing up to influence the users, new narratives may become both more convincing and more accessible. This could result in enhanced behavioural nudging[336] as well as in the manipulation users' actions in both the virtual and real worlds[337]. This could lead to changes in users' preferences, which creates risks for civic participation and electoral processes[338].

- **Countering disinformation**

Countering disinformation will become more challenging in Web 4.0 and virtual worlds. To be effective, it must operate in real time – which is already a significant hurdle on existing social media platforms. Content moderation is particularly complex in immersive 3D environments, where users can engage deeply with the virtual environment. Moderators must evaluate not only explicit content but also the context in which it appears, as well as non-verbal communication and interactions. These factors were less prominent in traditional media. Moreover, in virtual worlds, an immediate response is crucial; otherwise, it may become more difficult to reach those affected.

Furthermore, moderation in virtual worlds will need to address not just content but also behaviour. Current automated trust and safety mitigation techniques face significant challenges in VR environments, due to the ephemeral nature of real-time interactions and difficulties in monitoring

[335] Sipper, J.A. (2022). *The cyber meta-reality: Beyond the metaverse*. Rowman & Littlefield. https://www.amazon.com/Cyber-Meta-Reality-Beyond-Metaverse/dp/1666909254

[336] Hummel, D., & Maedche, A. (2019). How effective is nudging? A quantitative review on the effect sizes and limits of empirical nudging studies. *Journal of Behavioral and Experimental Economics, 80*, 47–58. https://doi.org/10.1016/j.socec.2019.03.004

[337] Council of Europe. (2023). *The metaverse and its impact on human rights, the rule of law, and democracy*. Council of Europe.

[338] Kulachai, U., Lerdtomornsakul, S., & Homyamyen, P. (2023). Factors influencing voting decision: A comprehensive literature review. *Social Sciences, 12*(9), 469.

multimodal communication, as well as complex behavioural patterns that are harder to detect than text-based violations. Such a situation poses a challenge when it comes to disinformation. The phenomenon of misinformation, however, is often linked to other online harms, as well as various types of cyberattacks. Meanwhile, the sense of physical presence in VR can magnify the impact of harassment, making it more intense. Moderators must reconsider how actions that might seem harmless in a 2D setting, such as invading someone's personal space or persistently following them, might feel threatening or intrusive in a 3D environment. Harmful narratives could be further spread through such behaviours.

However, new tools may help in countering these threats. AI technologies are key to addressing misleading content and disinformation within virtual worlds. Various tools and techniques have already been developed to detect and mitigate the spread of false information. These include fact-checking algorithms, image and video analysis, the detection of bots and fake avatars, as well as specialised content recommendation systems. In Web 4.0, different stakeholders could also offer personalised and immersive learning opportunities, including on topics such as immersive literacy and recognising disinformation[339]. Looking ahead, AI agents could be designed to identify potentially illegal behaviour or content, and could enforce regulations for resolving disputes in virtual environments[340].

3.4.2. Surveillance

Surveillance takes on novel dimensions as the digital and physical worlds merge, with constant data collection from interconnected devices raising concerns over privacy as well as increased potential for self-censorship. The immersive and interconnected nature of Web 4.0 means that both the quantity and the sensitivity of data collected may be much greater.

The potential for **surveillance by companies and platform providers**, typically carried out to increase engagement, advertising and ultimately profit, is heightened in Web 4.0. Immersive and interactive spaces will offer Big Tech companies and platform architects far greater involvement and control over user data, raising concerns and ethical questions about consent and exploitation. Datasets will be larger, not only terms of quantity but also quality and type, such as the biometric data of users of virtual worlds[341]. It is also important to mention the use of surveillance in third-party consumer settings – third parties will buy the data in order to better understand their consumers and to more effectively sell their products and services.

In addition, Web 4.0 technologies open up new possibilities for **surveillance by governments and law enforcement**. While many virtual platforms allow users to create avatars or pseudonymous identities, government agencies may be able to cross-reference biometric data, location tracking and interaction logs in order to uncover users' real-world identities. Facial recognition, voice analysis and even behavioural biometrics (such as the way a user moves or types) could also be used to match virtual personas to real individuals. If misused – for instance, to conduct surveillance at scale – this technology could be used to diminish individual liberties and strengthen state oversight[342]. This raises concerns about the erosion of online anonymity and the potential for increased political or social control.

Moreover, Web 4.0 and virtual worlds create room for increased **institutional surveillance within specific virtual environments** – for example, monitoring performance in workplaces or educational settings. Some companies are already deploying highly intrusive AI-driven surveillance tools to track and analyse their employees, often without their knowledge. A survey of 1,000 business leaders

[339] For example, the XR4HUMAN project, which produces videos on the responsible use and development of XR technologies. Available at: https://xr4human.eu/the-xr4human-educational-video-for-responsible-use-and-development-of-xr-technologies/

[340] Lou, Q., & Xu, W. (2025). Personality modeling for persuasion of misinformation using AI agent. *arXiv*. https://arxiv.org/abs/2501.08985

[341] Effing, R. (2024). Will the metaverse be out of control? Addressing the ethical and governance implications of a developing virtual society. *Digit. Gov. Res. Pract*. 5, 3, Article 29 (2024, September),

[342] Sherman, J. (2020), The Troubling Rise of Facial Recognition Technology in Democracies, *World Pol. Rev*., 23April 2020, https://www.worldpoliticsreview.com/the-troubling-rise-of-ai-facial-recognitiontechnology-in-democracies.

conducted in March 2023 revealed that 96 % of US firms with predominantly remote or hybrid workforces now use employee monitoring software[343].

By integrating virtual and physical worlds – including through brain–computer interfaces and other neural and biometric tracking tools; ubiquitous sensors and IoT; immersive virtual environments; facial and behavioural recognition; and real-time profiling technologies – **Web 4.0 enables powerful surveillance mechanisms**[344]. The table below outlines surveillance risks across features of various Web 4.0. These technologies could allow constant, real-time data gathering to monitor behaviour, restrict access, limit freedom of expression and potentially abuse labour rights[345].

Table 1. Potential surveillance risks under Web 4.0

Web 4.0 feature	Potential surveillance risks
Hyper-detailed behavioural tracking	In virtual worlds, every movement, interaction and even non-verbal cue (e.g. facial expressions, gestures) can be recorded. This results in the creation of extremely detailed user profiles, potentially revealing intimate personal habits and preferences. Such extensive tracking can erode privacy and be misused for targeted manipulation or discrimination.
Biometric data vulnerabilities	Many immersive devices (VR headsets, AR glasses, wearables) capture biometric data such as eye movement, heart rate, facial expressions and even voice patterns. Biometric data is inherently sensitive and difficult to change if compromised. Unauthorised access or misuse of this information could lead to identity theft, unauthorised profiling, or even health-related invasions of privacy.
The 'digital panopticon' effect	Continuous and pervasive monitoring in these environments can create an atmosphere in which users feel they are constantly being watched. This can alter behaviour – suppressing free expression, creativity or dissent – and can create an environment of self-censorship similar to the effects of a panopticon in the physical world.
Enhanced profiling	The detailed data harvested from virtual interactions can be used to build comprehensive profiles, which may feed into sophisticated AI algorithms. This opens the door to targeted advertising, behavioural nudging or even political and social manipulation. A risk also arises that such profiling could be used to discriminate against or marginalise certain groups.
Challenges in relation to consent	The complexity and opacity of data collection practices on immersive platforms often make it difficult for users to fully understand what data is being collected and how it is used. Without clear, informed consent, users may unwittingly agree to extensive surveillance practices, undermining their privacy and autonomy.

The potential side-effects of self-tracking in Web 4.0 environments will only become clear in the future. While tracing one's own behaviour and personal characteristics may become more popular in virtual worlds as more types of data become available, self-tracking technologies could pose a surveillance risk, as such data may be of interest to insurance companies, employers and retailers as well as other emerging actors[346]. It is worth noting, however, that technologies such as blockchain and quantum

[343] World Bank (2024). *Digital Progress and Trends Report 2023*. Washington, DC: World Bank. doi:10.1596/978-1-4648-2049-6.
[344] Radu. R. (2024) *Neurotechnologies and the future of internet governance*. Available at: https://cadmus.eui.eu/bitstream/handle/1814/77410/RSC_IB_2024_Radu.pdf?sequence=1&isAllowed=y
[345] Charamba, K. (2022). Beyond the corporate responsibility to respect human rights in the dawn of a metaverse. *U. Miami Int'l & Comp. L. Rev.*, 30, 110.
[346] Brubaker, R. (2020). Digital hyperconnectivity and the self, *Theory and Society*, vol.49, pp.771-801. Available at: https://link.springer.com/article/10.1007/s11186-020-09405-1

could potentially be used to address surveillance. For example, post-quantum cryptography and quantum key distribution could be explored as potential solutions for quantum-resistant encryption, potentially offering opportunities for enhanced security[347].

3.4.3. Control over, and interference with, access

Control over and interference in users' access represent significant challenges in the evolving landscape of Web 4.0 and virtual worlds. Immersive environments and increasingly interconnected experiences could amplify mechanisms of control. Such control potentially enables platforms, governments or other actors to **restrict access, limit individual freedoms and blur the boundaries between user autonomy and systemic control**. Reliance on AI-enabled technologies and associated real-time data gathering further exacerbates concerns over the possibility to influence user interactions and experiences.

Companies, as architects of these digital spaces, wield considerable influence over user experiences. Through algorithmic curation, content moderation and recommendation systems, companies can further restrict access, control narratives and limit freedom of expression[348,349] (see subsections 3.4.13.4.4 and 3.4.43.4.6 for more on algorithmic moderation and recommendation systems). Big tech companies and platform operators are increasingly serving as gatekeepers of digital access, whilst also playing a central role in algorithmic governance[350,351]. By harnessing machine learning and AI, companies have the capacity to infer user intent, preferences and vulnerabilities, potentially transforming virtual worlds into arenas of controlled interaction. Such granular insights can also allow companies to algorithmically curate experiences, suppress dissent and strategically restrict access to information or services, often prioritising commercial gain over user autonomy[352]. Furthermore, the predictive power of these systems poses systemic risks, including the potential to sway political outcomes, entrench data monopolies and legitimise policies that consolidate control over decentralised digital environments[353,354,355].

Governments could also leverage advanced technologies to reinforce state technological sovereignty and extend their control and authority into digital spaces. For example, facial recognition technology, widely adopted by governments for surveillance and policing (often without user consent or transparency) exemplifies how state control can be amplified in virtual environments if these technologies are misused. Governments likewise face a paradox: while regulating tech firms to ensure data privacy and online safety and to curb transnational dominance, **overly rigid or protectionist policies risk stifling innovation and fragmenting the digital ecosystem**[356,357]. For example, advances

347 Ajala, O.A., Arinze, C.A., Ofodile, O.C., Okoye, C.C., & Daraojimba, A.I. (2024). Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods. *Magna Sci. Adv. Res. Rev*, 10(1), 321-329.

348 Housego, R., & Farthing, R. (2022). Social grooming: Algorithms mis/shaping political discourse for young voters. *AQ - Australian Quarterly*, 93(4), 3–9.

349 Council of Europe. (2024). *The metaverse and its impact* on human rights, the rule of law, and democracy. Retrieved from https://rm.coe.int/the-metaverse-and-its-impact-on-human-rights-the-rule-of-law-and-democ/1680b178b0

350 Safadi, H., & Watson, R. T. (2023). Knowledge monopolies and the innovation divide: A governance perspective. *Information and Organization*, 33(2). https://doi.org/10.1016/j.infoandorg.2023.100466

351 Huang, K., & Krafft, P.M. (2024). Performing Platform Governance: Facebook and the Stage Management of Data Relations. *Sci Eng Ethics*, 2024 Apr 4;30(2):13. doi: 10.1007/s11948-024-00473-5. PMID: 38575812; PMCID: PMC10995037.

352 Chen, D., & Zhang, R. (2022). Exploring research trends of emerging technologies in health metaverse: A bibliometric analysis. Available at SSRN 3998068.

353 Housego, R., & Farthing, R. (2022). Social grooming: Algorithms mis/shaping political discourse for young voters. *AQ - Australian Quarterly*, 93(4), 3–9.

354 Brevini, B., Fubara-Manuel, I., Le Ludec, C., Jensen, J. L., Jimenez, A., & Bates, J. (2024). Critiques of data colonialism. In: J. Jarke & J. Bates (Eds.), *Dialogues in data power: Shifting response-abilities in a datafied world*. Bristol University Press. https://www.jstor.org/stable/jj.15617032.11

355 Plantin, J.C., & De Seta, G. (2019). WeChat as infrastructure: the techno-nationalist shaping of Chinese digital platforms. *Chinese Journal of Communication*, vol.12, no.3, pp.257-273.

356 van Lieshout, M. (2016). Privacy and Innovation: From Disruption to Opportunities. Data Protection on the Move: *Current Developments in ICT and Privacy/Data Protection*, 195-212.

357 Xie, Z., Qu, L., Lin, R., & Guo, Q. (2022). Relationships between fluctuations of environmental regulation, technological innovation, and economic growth: a multinational perspective. *Journal of Enterprise Information Management*, 35(4/5), 1267-1287. https://doi.org/10.1108/JEIM-02-2021-0104

in VR and gaming technologies have been used to support state-centric goals, such as to promote specific narratives, conduct information campaigns and influence global information standards[358]. These technologies can shape how individuals perceive and interact with reality, potentially affecting their ability to critically evaluate the information they encounter. By altering the way people engage with their environment, such tools can subtly influence their understanding of the world around them. The unintended consequences of restrictive digital governance are already evident. According to Freedom House, 65 % of people today live in countries where websites hosting political, social or religious content have been blocked; 48 % live in countries where authorities have disconnected internet or mobile networks, often for political reasons. More alarming still, 79 % of people live in countries where they could be arrested or imprisoned for posting content on political, social or religious issues[359].

Critically, **the extraction of value from user data is closely tied to control over the logistical infrastructure that underpins the digital economy**. For example, by owning vast networks of data centres, tech giants are able to not only dominate data storage and computing capabilities, but also to hold significant influence over smaller firms that rely on their services. This dynamic can create barriers to market access and competition[360]. When combined with corporate algorithmic and data-driven strategies, this infrastructural dominance can lead to **a self-reinforcing cycle of market power**. A key concern arises when market incentives are misaligned with the interests of users or society. For example, in the context of media convergence, control over infrastructure can extend to the level of content, meaning that platforms and entities shape the flow, distribution and even the framing of information[361]. This dual control over both the physical infrastructure and the content it carries poses the risk of amplifying the influence of certain actors over public discourse, cultural narratives and political agendas. Mitigating the potential risks associated with this concentration of power in the digital economy will therefore rely upon market structures and incentives aligning with broader societal goals and interests.

Aside from corporations and governments, **the extent to which users themselves can control and manage the acquisition, storage and sharing of their data under Web 4.0 remains a contentious topic.** While decentralised models such as blockchain-based systems offer a potential alternative by empowering users to retain control over their data[362], these remain niche[363]. Centralised control by private companies can enable developers to suspend or manipulate user accounts at will, raising concerns over accountability and fairness[364]. More recently, social media platforms have been moving away from third-party fact checking towards user- and AI-driven content moderation in an effort to more efficiently curb harmful content and promote free expression[365]. While notable, such efforts – which are designed to improve existing systems within centralised frameworks – further embed the shift away from alternative models that could empower users and reduce reliance on corporate intermediaries controlling digital spaces[366].

---

358 Hoffman, D.S., Hoja, T., Lau, Y., & Lee, L. M.C. (2024). Truth and reality with Chinese characteristics. Australian Strategic Policy Institute. Available at: https://www.aspi.org.au/report/truth-and-reality-chinese-characteristics

359 Freedom House (2024). *Freedom on the Net 2024: The global drive to control big tech and its impact on free expression*. Available at: https://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf

360 Brevini, B., Fubara-Manuel, I., Le Ludec, C., Jensen, J.L., Jimenez, A., & Bates, J. (2024). Critiques of data colonialism. In: J. Jarke & J. Bates (Eds.), *Dialogues in data power: Shifting response-abilities in a datafied world*. Bristol University Press. https://www.jstor.org/stable/jj.15617032.11

361 China Media Project (2021). 'CMP dictionary: media convergence', China Media Project, 16 April 2021. Available at: https://chinamediaproject.org/the_ccp_dictionary/media-convergence/

362 Zhang, C., Zhao, M., Zhang, W., Fan, Q., Ni, J., & Zhu, L. (2024). Privacy-Preserving Identity-Based Data Rights Governance for Blockchain-Empowered Human-Centric Metaverse Communications. *IEEE Journal on Selected Areas in Communications*, 42(4), 963-977. https://doi.org/10.1109/JSAC.2023.3345392

363 Effing, R. (2024). Will the metaverse be out of control? Addressing the ethical and governance implications of a developing virtual society. *Digital Government: Research and Practice*, 5(3). Available at: https://doi.org/10.1145/3674148

364 Travis, H. (2025). *Platform neutrality rights: AI censors and the future of freedom*. Routledge.

365 Meta (2025, January). Meta: More speech, fewer mistakes. In: Facebook Newsroom. Retrieved from https://about.fb.com/news/2025/01/meta-more-speech-fewer-mistakes/

366 Pentland, A., & Davis, P. (2021, October). How decentralized systems can help rebuild local communities. World Economic Forum. Retrieved from https://www.weforum.org/stories/2021/10/how-decentralized-systems-can-help-rebuild-local-communities/

The evolving landscape of Web 4.0, in which public infrastructure and private platforms increasingly intersect, **amplifies the risk of centralised control mechanisms that interfere with user access and autonomy.** These challenges underline the urgent need to address how data governance and advanced technologies can either restrict or empower users. Initiatives such as UNESCO's framework for equitable data governance, ethical data practices and inclusive policy design demonstrate the potential for collaborative approaches to mitigate these risks while fostering innovation and protecting fundamental freedoms in virtual environments. By prioritising transparency, accountability and participatory governance, stakeholders can reduce harmful interference with digital access and ensure that control mechanisms align with collective rights rather than consolidating power among dominant actors[367].

The ability of AI to monitor, moderate and manipulate behaviour in Web 4.0 also introduces **fundamental risks to freedom of speech and expression**. Combatting the other challenges described in this section (such as illegal and harmful content, as well as disinformation), while remaining consistent with freedom of expression, is also a key focus of WSIS Action Line 24 on media and promoting diversity of ownership in the Information Society[368]. While AI-driven content moderation is often a necessary safety measure, it also has the potential to suppress dissent, reinforce ideological biases and distort public discourse to instigate harm at both individual and collective levels. The risk of such AI-driven moderation extends beyond state control (see subsection 3.4.23.4.2 for more on surveillance). The vast amounts of personal data gathered in Web 4.0 environments could be leveraged by bad actors to silence dissent, amplify certain narratives over others, or create algorithmic echo chambers that distort public discourse and perpetuate harm[369]. This also raises the broader question of whether the increasingly hyper-personalised content each user would consume in such a scenario is desirable, or should common spaces exist in which individuals can access "the same truth" in digital environments? Already, recommendation systems in today's social media have been shown to affect users' information consumption by leading them to prioritise content that aligns with their existing views. This can gradually isolate users from diverse perspectives, reinforce shared opinions, increase polarisation and strengthen confirmation biases[370,371]. Lastly, the integration of AI-driven moderation and algorithmic bias could also disproportionately target certain groups, further entrenching existing inequalities and systemic discrimination[372] (see also subsection 3.4.6 for more on discrimination3.4.6).

3.4.4. Online harms

Web 4.0 and virtual worlds present unprecedented challenges to mitigating online harms within a new era of digital interactivity, powered by advanced technologies such as AI, extended reality (XR), haptics and brain-computer interfaces (see Section 2.4). While these innovations offer significant opportunities for enhanced engagement, personalised experiences and economic growth, they can also amplify existing online harms and facilitate novel forms of psychological, social and economic exploitation online. The blurred boundaries between the physical and digital worlds make these environments particularly vulnerable to exploitation, manipulation and abuse. The decentralised nature

367 Ndemo, B. (2024). Addressing digital colonialism: A path to equitable data governance. UNESCO Inclusive Policy Lab. Retrieved from https://en.unesco.org/inclusivepolicylab/analytics/addressing-digital-colonialism-path-equitable-data-governance

368 WSIS (2003). Declaration of Principles. Building the Information Society: a global challenge in the new Millennium. Available at: https://www.itu.int/net/wsis/docs/geneva/official/dop.html

369 Couldry, N., & Mejias, U.A. (2019). Data and the threat to human autonomy. In: *The costs of connection: How data is colonizing human life and appropriating it for capitalism,* Stanford University Press, pp.153-184.

370 Cinelli, M., De Francisci Morales, G., Galeazzi, A., Quattrociocchi, W., & Starnini, M. (2021). The echo chamber effect on social media. Proceedings of the National Academy of Sciences, 118(9). doi: 10.1073/pnas.2023301118

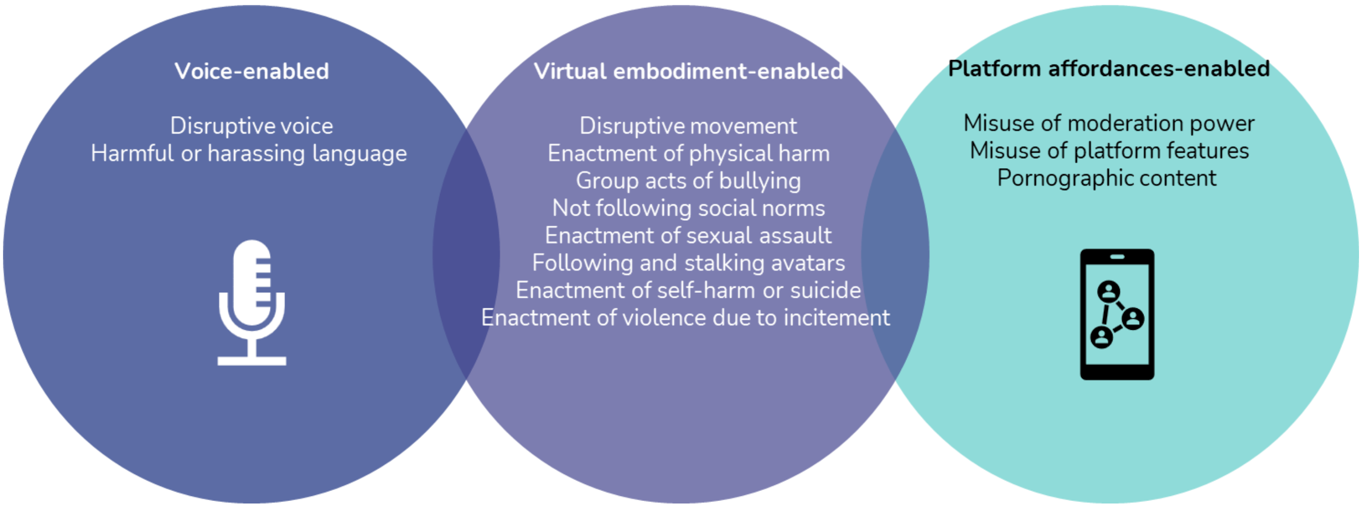
371 Reiter, F., Heiss, R., & Matthes, J. (2022). Explaining attitude-consistent exposure on social network sites: The role of ideology, political involvement, and network characteristics. *Social Science Computer Review*. Advance online publication. https://doi.org/10.1177/08944393211056224

372 Heller, B. (2021). Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law, *23 Vanderbilt Journal of Entertainment and Technology Law*, 1 (2021). Available at: https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss1/1

of Web 4.0 and the use of advanced AI systems introduces additional complexities, particularly in terms of content moderation, identity security and the protection of fundamental freedoms.

Web 4.0 and virtual worlds have the potential to **exacerbate existing online harms**, such as abuse and discrimination. Virtual spaces already demonstrate vulnerabilities to a spectrum of harms, ranging from privacy violations and surveillance to the spread of harmful content, as well as phishing scams, doxxing, ransomware and more[373,374,375]. INTERPOL has identified an additional wide range of potential harms "in and through the Metaverse"[376]. These include property crime, financial crime, terrorism, cybercrime, crimes against children, identity crime, crimes against public safety, intellectual property crime, acts intended to cause fear and emotional distress, sexual offences and assault. Each of these types of crime can be further divided into potential sub-crimes[377]. In one recent study that undertook virtual field research in three different VR environments, 13 types of harmful behaviours were identified as taking place across the online platforms (see figure below). In another study, within 11 hours and 30 minutes of recordings of user behaviour on a social media platform, researchers identified 100 potential violations of user policies, 51 of which met the platform's criteria for reporting. The platform did not respond to any of these reports, which included incidents of sexual harassment and the grooming of minors[378].

Figure 7. Types of harmful behaviours in virtual worlds



Source: Sabri, et al (2023).[379]

373 Sabri, N., Chen, B., Teoh, A., Dow, S.P., Vaccaro, K., & Elsherief, M. (2023). Challenges of moderating social virtual reality. In: *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (CHI '23) (Article 384, pp. 1–20). Association for Computing Machinery. https://doi.org/10.1145/3544548.3581329

374 ElSherief, M., Kulkarni, V., Nguyen, D., Yang Wang, W., & Belding, E. (2018). Hate Lingo: A Target-Based Linguistic Analysis of Hate Speech in Social Media. *Proceedings of the International AAAI Conference on Web and Social Media*, 12(1). https://doi.org/10.1609/icwsm.v12i1.15041

375 Dilla, W.N., Harrison, A.J., Mennecke, B.E., & Janvrin, D.J. (2013). The assets are virtual, but the behavior is real: An analysis of fraud in virtual worlds and its implications for the real world. *Journal of Information Systems*, 27(2), 131-158. https://doi.org/10.2308/isys-50571

376 INTERPOL. (2024). Metaverse: A law enforcement perspective: Use cases, crime, forensics, investigation, and governance [White paper].

377 Karapatakis, A. (2025). Metaverse crimes in virtual (un)reality: Fraud and sexual offences under English law. *Journal of Economic Criminology*, 7, 100118. https://doi.org/10.1016/j.jeconcrim.2025.100118.

378 Center for Countering Digital Hate (2021). New research shows Metaverse is not safe for kids. https://counterhate.com/blog/new-research-shows-metaverse-is-not-safe-for-kids

379 Sabri, N., Chen, B., Teoh, A., Dow, S. P., Vaccaro, K., & Elsherief, M. (2023). Challenges of moderating social virtual reality. In: *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pp. 1-20.

Meanwhile, the immersive and realistic nature of Web 4.0 and virtual worlds has the potential to **exacerbate harms associated with existing crimes,** such as sexual harassment and violence, online sex trafficking and grooming[380,381,382]. Since immersive technologies such as VR headsets and haptics can enhance the vividness and physical sensations felt during digital experiences, they can also invoke psychological and emotional responses akin to real "lived" experiences[383,384]. This heightened emotional engagement likewise means that users are more vulnerable to being affected by virtual harms, both online and offline[385]. Individuals can feel the physical and psychological impact of virtual harms or negative interactions in virtual worlds more intensely, given that the boundaries between digital and real-world experiences are increasingly blurred in virtual spaces. This can potentially intensify traumas associated with offences such as harassment, sexual violence and hate crimes[386]. Worryingly, this could result in marginalised groups, who are already susceptible to online abuse, experiencing **compound harms,** whereby multiple layers of vulnerability intersect, intensifying the severity and long-term consequences of virtual harms. AI-driven personalisation could further exacerbate this issue, as algorithms that learn from user preferences could inadvertently reinforce exposure to harmful environments and abusive interactions, or further entrench systemic biases, perpetuating discrimination and exclusion[387] (see subsection 3.4.63.4.6).

Since Web 4.0 depends upon vast amounts of user data, and as virtual worlds continue to integrate diverse types of data into disparate ecosystems, **new opportunities for exploitation and misuse will continue to arise**. For instance, when merging the demand of machine learning for behavioural data with addictive platform designs, platform engineers are able to (mis)use users' data to create cybernetic feedback loops to encourage constant user engagement. In turn, this normalises the collection of vast amounts of data[388]. The misuse of such data collected from wearable devices, haptic technologies and neural interfaces (not limited to biometric, neurological and behavioural data) also risks enabling other harms such as identity theft and emotional manipulation by bad actors. For instance, the availability of such diverse data might make it possible to conduct emotional exploitation (e.g. using a user's fears, anxiety or behaviours such as impulsivity or loneliness to drive specific actions or to boost engagement)[389,390].

While the immersive interfaces of Web 4.0 can amplify emotional responses, the absence of certain physical cues and asynchronous communication can also weaken emotional regulation. This could **make users more prone to engaging in impulsive or harmful online behaviours** such as trolling, if they

---

380 Sabri, N., Chen, B., Teoh, A., Dow, S. P., Vaccaro, K., & Elsherief, M. (2023). Challenges of moderating social virtual reality. In: *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pp. 1-20.

381 Europol (2022). Policing in the metaverse: what law enforcement needs to know. Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Policing%20in%20the%20metaverse%20-%20what%20law%20enforcement%20needs%20to%20know.pdf

382 Ladikas, M., Madeira, O., Hahn, J., Correa Pérez, M., Caplice, G., & Gerasymenko, A. (2024). D3.1: State-of-art in XR policy debates. In: M. Ladikas & M. Correa Pérez (Eds.), *The Equitable, Inclusive, and Human-Centered XR Project (XR4Human)* (Deliverable No. 3.1). Karlsruhe Institute of Technology (KIT). Grant Agreement No. 101070155.

383 Gray, J.E., Carter, M., & Egliston, B. (2024). Governing social virtual reality: Preparing for the content, conduct, and design challenges of immersive social media. Springer Nature, Switzerland. https://doi.org/10.1007/978-3-031-61831-4

384 Gray, J.E., Carter, M., & Egliston, B. (2024). Conduct Harms in Social VR: Embodied Harassment, Gender-Based Harm and Toxic Cultures. In: *Governing Social Virtual Reality*, Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-61831-4_3

385 Wolfendale, J. (2007). My avatar, my self: Virtual harm and attachment. *Ethics and Information Technology*, 9(2), 111–119. https://doi.org/10.1007/s10676-006-9125-z

386 Gómez-Quintero, J., Johnson, S.D., & Borrion, H. (2024). A scoping study of crime facilitated by the metaverse. *Futures*, 157, 103338. https://doi.org/10.1016/j.futures.2024.103338

387 Hanna, M.G., Pantanowitz, L., Jackson, B., Palmer, O., Visweswaran, S., Pantanowitz, J., Deebajah, M., & Rashidi, H.H. (2025). Ethical and bias considerations in artificial intelligence/machine learning. *Modern Pathology*, 38(3), 100686. https://doi.org/10.1016/j.modpat.2024.100686

388 Fourcade, M., & Fleur, J. (2020). Loops, ladders and links: the recursivity of social and machine learning. Available at: https://link.springer.com/content/pdf/10.1007/s11186-020-09409-x.pdf

389 Cheong, B. C. (2022). Avatars in the metaverse: Potential legal issues and remedies. *International Cybersecurity and Law Review*, 3(4), 467-494. https://doi.org/10.1365/s43439-022-00056-9

390 European Parliamentary Research Service (EPRS) (2024, July). The protection of mental privacy in the area of neuroscience - Societal, legal and ethical challenges. European Parliament. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2024/757807/EPRS_STU(2024)757807_EN.pdf

are struggling to manage potentially negative emotions online[391]. In parallel, "cloaking" – the practice of obscuring or regulating emotional expressions, voices, locations and other components of an individual's digital footprint – has been used to further personalise virtual experiences and enhance privacy[392]. However, it has also raised concerns about the potential for behavioural modification, manipulation and exploitation by bad actors. Emotional and behavioural recognition technologies are increasingly being used alongside algorithmic security, surveillance, predictive policing and smart city infrastructures, to enable the real-time quantification and analysis of a subject's mental and emotional state[393,394,395]. The risks associated with these technologies are amplified in virtual environments, where emotional and psychological influence can be more pervasive and difficult to regulate. In some countries, attempts have been made to restrict the use of emotional recognition technologies; however, continuous advances in areas that are not excluded continue to pose challenges for governance and policy frameworks[396].

The decentralised and anonymous nature of virtual environments creates a plethora of complications for user safety in Web 4.0. Pseudonymity, a common feature of these spaces, enables individuals to hide their true identities, which can facilitate harmful or criminal activities while reducing accountability[397,398]. Risks of identity theft, impersonation attacks and avatar authentication failures are also heightened[399]. Furthermore, governments are calling attention to the proliferation of deepfakes, misinformation and disinformation that can manipulate public opinion and trust, along with concerns regarding AI-generated content, cyberbullying and harassment[400]. For instance, in an XR environment, bad actors could create deepfake avatars of politicians to mislead users or manipulate discourse[401]. In Web 4.0, hackers could also potentially exploit authentication loopholes, phishing schemes and compromised wearable devices to steal sensitive personal information, digital assets and even assume control over avatars[402,403]. Virtual scams, which already pose significant challenges in Web 3.0 environments, are also likely to escalate in complexity with the increased integration of blockchain-based digital goods as well as virtual real estate among other digital assets, and

391 Syrjämäki, A.H., Ilves, M., Olsson, T., Kiskola, J., Isokoski, P., Rantasila, A., Bente, G., & Surakka, V. (2024). Online disinhibition mediates the relationship between emotion regulation difficulties and uncivil communication. *Scientific Reports*, 14, Article 30019. Available at: https://doi.org/10.1038/s41598-024-81086-7

392 Goethals, S., Matz, S., Provost, F., Martens, D., & Ramon, Y. (2025). The impact of cloaking digital footprints on user privacy and personalization. *Big Data*. Available at: https://www.liebertpub.com/doi/pdf/10.1089/big.2024.0036

393 Fontes, C., Hohma, E., Corrigan, C.C., & Lütge, C. (2022). AI-powered public surveillance systems: Why we (might) need them and how we want them. *Technology in Society*, 71, Article 102137. Available at: https://doi.org/10.1016/j.techsoc.2022.102137

394 Mantello, P., Ho, M.T., Nguyen, M.H. et al. (2023). Machines that feel: behavioral determinants of attitude towards affect recognition technology—upgrading technology acceptance theory with the mindsponge model. *Humanit. Soc. Sci. Commun.*, 10, 430 (2023). Available at: https://doi.org/10.1057/s41599-023-01837-1

395 Gandy, O.H., Jr. (2019, July). The algorithm made me do it! Predictive policing, cameras, social media, and affective assessment. Paper presented at the IAMCR 2019 conference, Madrid, Spain. Available at: https://www.asc.upenn.edu/sites/default/files/2021-03/%22The%20Algorithm%20Made%20Me%20Do%20It!%20Predictive%20Policing,%20Cameras,%20Social%20Media%20and%20Affective%20Assessment.%22%20IAMCR%202019..pdf

396 Fry, W. (no date). The time to AI Act is now: A practical guide to emotion recognition systems under the AI Act. Available at: https://www.williamfry.com/knowledge/the-time-to-ai-act-is-now-a-practical-guide-to-emotion-recognition-systems-under-the-ai-act/

397 Karapatakis, A. (2025). Metaverse crimes in virtual (un)reality: Fraud and sexual offences under English law. *Journal of Economic Criminology*, 7, 100118. Available at: https://doi.org/10.1016/j.jeconcrim.2025.100118

398 Gómez-Quintero, J., Johnson, S.D., & Borrion, H. (2024). A scoping study of crime facilitated by the metaverse. *Futures*, 157, 103338. Available at: https://doi.org/10.1016/j.futures.2024.103338attributes of the metaverse(s) have the potential to make these types of offenses worse than their online equivalents.

399 Jabar, B.A., Azmi, M., Hernando, G., Moniaga, J.V., & Alpaullivarez, A.A. (2022). The Social Impact of VR Technology on Society: A Systematic Literature Review. *Ultimatics: Jurnal Teknik Informatika*, 14(2), 57-62.

400 Department for Science, Innovation and Technology (2024). International scientific report on the safety of advanced AI (Interim report). UK Government. Available at: https://assets.publishing.service.gov.uk/media/6716673b96def6d27a4c9b24/international_scientific_report_on_the_safety_of_advanced_ai_interim_report.pdf

401 Kourtesis, P. (2024). A Comprehensive Review of Multimodal XR Applications, Risks, and Ethical Challenges in the Metaverse. *Interact*, 2024, 8, 98. https://doi.org/10.3390/mti8110098

402 Cheong, B.C. (2022). Avatars in the metaverse: Potential legal issues and remedies. *International Cybersecurity and Law Review*, 3(4), 467-494. https://doi.org/10.1365/s43439-022-00056-9

403 Vaishnavi, A.R, Sahana, G., Guruprasad, N. (2023). "Wearable Devices in the IoT: A Security and Privacy Perspective", 2023 International Conference on IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, pp. 1-4, doi: 10.1109/ICICAT57735.2023.10263654.

decentralised financial systems[404]. Law enforcement agencies are likewise raising alarm regarding the continuing pace and development of new technologies such as AI and the metaverse, warning of an inevitable change in the attack methodologies used by cyber criminals to commit fraud[405]. Meanwhile, other scholars warn that the proliferation of multi-user environments within Web 4.0 will also lead to an increase in opportunities for fraud and financial crime[406]. Importantly, the absence of centralised regulatory oversight in many Web 4.0 or virtual platforms further exacerbates these issues, as offenders perceive there to be a lower risk of detection and punishment in unregulated spaces[407]. Moreover, the increasing sophistication of generative AI systems poses unique challenges in the detection and mitigation of these harms.

Web 4.0 and virtual worlds will also make content moderation even more complex, as the amount of data and real-time interactions produced in immersive environments will far exceed those on today's platforms[408,409] (see figure below for more detail). Recently, Meta announced a "safe zone" feature for its VR platform, allowing users to instantly create a personal shield against uncomfortable proximity or unwelcome advances from other users[410]. Despite such efforts to ensure user safety when interacting with other individuals in immersive spaces, moderating diverse types of content in Web 4.0 still faces challenges. For example, while techniques to detect images of child sexual abuse material (CSAM) have been effective in traditional internet contexts, their application in Web 4.0 environments is complicated by the multidimensional nature of content, which can include 3D videos, gestures and physical interactions facilitated by haptic technologies[411]. Content moderation is already a significant challenge for existing social media platforms, with the number of moderators available often being insufficient. In the aforementioned study by Sabri et al. (2023), out of the 100 scheduled events observed, harmful behaviours were identified in 45, but only 24 % of these incidents were addressed by moderators[412].

The behaviours and criminal activity discussed above are expected to move between platforms in Web 4.0, meaning that **close collaboration between the private sector, governments and civil society to tackle these issues will be critical**[413]. Research has shown that robust oversight, safeguards for free expression, and information sharing between governments and technology companies can improve users' ability to access authoritative and reliable information[414]. While the use of AI agents is also poised to play a central role in managing and monitoring Web 4.0 environments in which human moderation alone is insufficient, government agencies could, for example, provide vital context to companies in order to help combat cyberattacks or coordinated misleading behaviour[415]. AI tools can

---

404 Couldry, N., & Mejias, U.A. (2019). Data and the threat to human autonomy. In The costs of connection: How data is colonizing human life and appropriating it for capitalism, Stanford University Press, pp.153-184.

405 City of London Police (no date). *National policing strategy*. Retrieved from: https://www.cityoflondon.police.uk/SysSiteAssets/media/downloads/city-of-london/about-us/colp_national-policing-strategy-document.pdf

406 Couldry, N., & Mejias, U.A. (2019). Data and the threat to human autonomy. In: *The costs of connection: How data is colonizing human life and appropriating it for capitalism*, Stanford University Press, pp.153-184.

407 Gómez-Quintero, J., Johnson, S.D., Borrion, H., & Lundrigan, S. (2024). A scoping study of crime facilitated by the metaverse. *Futures*, *157*. https://doi.org/10.1016/j.futures.2024.103338

408 Gray, J.E., Carter, M., & Egliston, B. (2024). Content harms in social VR: Abuse, misinformation, platform cultures, and moderation. In *Governing social virtual reality,* Palgrave Macmillan, pp. 25-42. https://doi.org/10.1007/978-3-031-61831-4_2

409 Castro, D. (2022, 28 February 28). Content moderation in multi-user immersive experiences: AR/VR and the future of online speech. Information Technology and Innovation Foundation. Available at: https://itif.org/publications/2022/02/28/content-moderation-multi-user-immersive-experiences-arvr-and-future-online/

410 Basu, T. (2021). The Metaverse has a groping problem already. MIT Technology Review. https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/

411 Gómez-Quintero, J., Johnson, S.D., & Borrion, H. (2024). A scoping study of crime facilitated by the metaverse. *Futures*, 157, 103338. https://doi.org/10.1016/j.futures.2024.103338

412 Sabri, N., Chen, B., Teoh, A., Dow, S.P., Vaccaro, K., & Elsherief, M. (2023). Challenges of moderating social virtual reality. In: *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pp. 1-20.

413 IGF (2024). High-Level Session 5: Protecting Children's Rights in Digital World.

414 Freedom House (2024). *Freedom on the Net 2024: The global drive to control big tech and its impact on free expression.* Available at: https://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf

415 Ibid.

also serve to enhance justice by providing AI-powered legal assistance or helping people to acquire the analytical skills and legal terminology needed to successfully negotiate a complex legal system[416].

Figure 8. "Algospeak" – navigating AI-driven content moderation and exploitation in Web 4.0

With the emergence of new digital spaces comes the adoption of new vocabularies and even languages by users. "Algospeak" – a combination of the words "algorithm" and "speak" – refers to the code words or euphemisms used to circumvent algorithmic content moderation filters built into platforms. Unlike internet slang, algospeak is a way for users to get around having content flagged by AI-assisted content moderation systems[417]. It can take many forms.

Often, words are deliberately misspelled or used out of context such as during the COVID-19 pandemic, when some social media users referred to the pandemic as the "panini" or "panda express" due to platforms working to combat misinformation by down-ranking videos that mentioned the pandemic[418]. Other ways to avoid automated moderation tools include replacing letters with numbers and symbols such as "!" or "1" for the letter "I", or "$" for the letter "s". This new lexicon of words includes examples such as "seggs" for sex, "corn" for porn, "unalive" for suicide, death or kill, and "yahtzee" for "nazi". In some instances, users also obfuscate text with the addition of emojis. For instance, videos referring to cannabis are associated with a variety of emojis such as the herb emoji (🌿), or the gust of wind emoji (💨) to indicate marijuana or smoke. Experts are also particularly concerned about the impacts of algospeak on child and human exploitation, where sentences with double meanings are frequently used online to sexualise children[419].

In some cases, viewers of videos and livestreams online encourage young children in the comments section to perform certain acts to receive monetary gifts as a reward. Using "Gen z" slang and euphemisms in the comments to evade automated moderation tools, phrases such as "outfit check" are used maliciously by some users to ask to see a child's stomach or chest, in order to sexualise children online, particularly young girls, in exchange for money. Other solicitation attempts are more explicit, such as asking children to kiss or to spread their legs. Law enforcement and experts warn that these activities could potentially lead predators to groom children on to other platforms for sexual abuse, or more concerningly, offline[420].

As new words are created and flagged over time, the examples listed above will change and new words will be created as substitutes. For example, "ouid" was once commonly used as algospeak for "weed". Now, however, searches for this term on social media platforms return no results, and a warning is given that states, "this phrase may be associated with behaviour or content that violates our guidelines". More recently, in an effort to promote freedom of speech, online users coined the term "cute winter boots" to allow open discussions of political concerns to continue, while also avoiding censorship and boosting related content, since the term heavily appeals to online advertisers looking to place product advertisements[421].

While AI and AI-assisted technologies in Web 4.0 offer benefits such as personalised content, seamless navigation of immersive digital spaces and the automated identification of harmful behaviours, **AI agents also pose significant risks and introduce new avenues for exploitation**. One critical concern is behavioural moderation, which becomes increasingly complex in real-time virtual environments due to the speed, scale and intricacy of interactions[422,423]. Unlike traditional platforms, which primarily regulate static content, Web 4.0 requires the increased monitoring of avatar behaviour,

---

416 Farook, A. M., Kingston, W., & Kannaiah, S. K. (2024). Enlightening Justice: Empowering Society Through AI-Driven Legal Assistance. In: *2024 Second International Conference on Advances in Information Technology (ICAIT)*. Vol. 1, pp. 1-7. doi: 10.1109/ICAIT61638.2024.10690793.

417 Ifeanyi, K.C. (2022). Decoding what algospeak really means for content creators. *Fast Company*. Available at: https://www.fastcompany.com/90802742/decoding-what-algospeak-really-means-for-content-creators

418 *Washington Post* (2022). Internet 'algospeak' is changing our language in real time, from 'nip nops' to 'le dollar bean'. Available at: https://www.washingtonpost.com/technology/2022/04/08/algospeak-tiktok-le-dollar-bean/

419 Levine, A.S. (2022). From Camping To Cheese Pizza, 'Algospeak' Is Taking Over Social Media'. *Forbes*. Available at: https://www.forbes.com/sites/alexandralevine/2022/09/16/algospeak-social-media-survey/?sh=36cd51955e10

420 Levine, A.S. (2022). How TikTok Live Became 'A Strip Club Filled with 15-Year-Olds'. *Forbes*. Available at: https://www.forbes.com/sites/alexandralevine/2022/04/27/how-tiktok-live-became-a-strip-club-filled-with-15-year-olds/?sh=5b4235c462d7

421 Di Placido, D. (2025, 29 January). TikTok's 'Cute Winter Boots' trend, explained. *Forbes*. Retrieved from https://www.forbes.com/sites/danidiplacido/2025/01/29/tiktoks-cute-winter-boots-trend-explained/

422 Sabri, N., Chen, B., Teoh, A., Dow, S. P., Vaccaro, K., & Elsherief, M. (2023). Challenges of moderating social virtual reality. In: *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pp. 1-20.

423 *Council of Europe (2024). The metaverse and its impact on human rights, the rule of law, and democracy. Retrieved from: https://rm.coe.int/the-metaverse-impact-on-and-its-impact-on-human-rights-the-rule-of-law/1680ae6bce*

necessitating more sophisticated moderation techniques[424]. However, AI agents themselves can be weaponised for malicious purposes – in particular, to facilitate fraud, scams and cyber attacks. More advanced AI systems can, for instance, be automated to complete complex end-to-end tasks such as generating highly convincing, personalised scam content at scale, bypassing security filters by correcting linguistic errors and improving message fluency, making phishing schemes and financial fraud more effective[425]. In addition, AI-powered automation lowers the technical barriers to executing cyberattacks, enabling individuals with little expertise to conduct and automate impersonation fraud and other online cyber attacks[426]. Impersonation attacks could become particularly insidious, as bad actors could create realistic digital clones of users in order to commit fraud or crimes against other metaverse participants[427]. Given the lack of comprehensive regulatory oversight in virtual worlds, these AI-driven harms could therefore proliferate unchecked, exacerbating mental distress, perpetuating digital abuse, and raising urgent concerns regarding power, control and online autonomy.

3.4.5. Health and well-being

Web 4.0 and virtual worlds **present significant opportunities to enhance health and well-being, but they also introduce new risks that must be carefully managed**. The immersive and hyperconnected nature of Web 4.0 technologies offers the potential to transform how we understand, monitor and regulate physical and mental health. However, the same features that enable these benefits (such as heightened realism, automated and personalised experiences and constant connectivity) also pose unique challenges to users' health and well-being.

Virtual worlds have shown significant promise in therapeutic and rehabilitation contexts. Encouraging the adoption of ICTs to improve and extend health care and health information to remote and under-served areas and vulnerable populations is also a key focus of WSIS Action Line 7[428]. In Web 4.0, immersive environments can be used for **physical rehabilitation, cognitive therapy and mental health interventions**[429], and exhibit great potential for improving overall well-being[430], reducing anxiety and depression[431], enhancing emotional regulation, relaxation[432], stress recovery, mindfulness[433], mood regulation[434], vitality, and overall cognitive performance in areas such as working memory, attention and concentration[435]. Studies have also demonstrated the effectiveness of VR technologies in treating

---

424 Department for Science, Innovation and Technology (2024). International *scientific report on the safety of advanced AI: Interim report*. Department for Science, Innovation and Technology, UK. https://assets.publishing.service.gov.uk/media/6716673b96def6d27a4c9b24/international_scientific_report_on_the_safety_of_advanced_ai_interim_report.pdf

425 Chan, A., Ezell, C., Kaufmann, M., Wei, K., Hammond, L., Bradley, H., Bluemke, E., Rajkumar, N., Krueger, D., Kolt, N., Heim, L., & Anderljung, M. (2024). *Visibility into AI agents*. arXiv. Available at: https://arxiv.org/abs/2401.13138

426 World Economic Forum & Capgemini (2024). *Navigating the AI frontier: A primer on the evolution and impact of AI agents.* World Economic Forum. https://reports.weforum.org/docs/WEF_Navigating_the_AI_Frontier_2024.pdf

427 Ali, M., Naeem, F., Kaddoum, G., & Hossain, E. (2022). Metaverse communications, networking, security, and applications: Research issues, state-of-the-art, and future directions. arXiv. Available at: https://arxiv.org/abs/2212.13993

428 WSIS (2003). Declaration of Principles. Building the Information Society: a global challenge in the new Millennium. Available at: https://www.itu.int/net/wsis/docs/geneva/official/dop.html

429 Zarei, T., Emery, M., Saredakis, D., Lee, G.A., Stubbs, B., Szpak, A., & Loetscher, T. (2024, 6 December). Being there together for health: A systematic review on the feasibility, effectiveness and design considerations of immersive collaborative virtual environments in health applications. arXiv. https://doi.org/10.48550/arXiv.2412.04760

430 Montana, J.I., Matamala-Gomez, M., Maisto, M., Mavrodiev, P.A., Cavalera, C. M., Diana, B., Mantovani, F., & Realdon, O. (2020). The benefits of emotion regulation interventions in virtual reality for the improvement of wellbeing in adults and older adults: a systematic review. *Journal of Clinical Medicine*, 9(2), 500.

431 Waqas, M., Gururaj, Y.P., Mitra, V.D., Karri, S.A., Reddy, R., & Azeemuddin, S. (2024). Using virtual reality for detection and intervention of depression: A systematic literature review. arXiv preprint arXiv:2403.01882.

432 Riches, S., Azevedo, L., Bird, L., Pisani, S., & Valmaggia, L. (2021). Virtual reality relaxation for the general population: A systematic review. *Social Psychiatry and Psychiatric Epidemiology*, 56.

433 Wang, X., Mo, X., Fan, M., Lee, L.H., Shi, B., & Hui, P. (2022, October). Reducing stress and anxiety in the metaverse: A systematic review of meditation, mindfulness and virtual reality. In: *Proceedings of the Tenth International Symposium of Chinese CHI*, pp. 170-180.

434 Diniz Bernardo, P., Bains, A., Westwood, S., & Mograbi, D.C. (2021). Mood induction using virtual reality: A systematic review of recent findings. *Journal of Technology in Behavioral Science*, 6, 3-24.

435 Yan, S., Shen, S., Lu, Q., Zhong, S., Lv, S., Lai, S., Luo, Y., Ran, H., Duan, M., Song, K., Ye, K., & Jia Y. (2024). Virtual reality working memory training improves cognitive performance of acute and remitted patients with major depressive disorder. *J. Affect. Disord.* 2024 Jan 1;344:267-276. doi: 10.1016/j.jad.2023.10.067. Epub 2023 Oct 12. PMID: 37838265.

conditions such as depression[436], anxiety[437], phobias and post-traumatic stress disorder (PTSD)[438]. For example, VR environments can simulate real-world scenarios to help individuals confront and manage their fears in a controlled setting using VR based exposure therapy techniques[439]. Research also highlights the potential of virtual worlds in detecting early signs of mental health issues such as depression, when combined with other advanced technologies in Web 4.0 such as eye tracking[440]. For older adults in particular, VR technologies have helped patients to remain motivated and engaged in rehabilitation following a stroke[441], with studies citing improved rehabilitation outcomes for people experiencing neurocognitive decline including dementia[442], as well as improved detection of the risk of Alzheimer's, when harnessing insights and data obtained from VR as a diagnostic tool[443].

The hyperconnected nature of Web 4.0 **enables the ability to affect emotional regulation and social interaction**. For instance, platforms already host communities centred around autonomous sensory meridian response (ASMR) videos that use soothing sounds and visuals to induce relaxation and alleviate stress. When combined with other emerging technologies, such as AI-driven emotion recognition systems, emotional regulation can be further enhanced by detecting physiological signals such as heart rate and electrodermal (EDA) activity. The box below provides further detail on the application and innovative use of ASMR alongside other advanced technologies in Web 4.0.

Figure 9. Applications of ASMR in Web 4.0 for emotional and psychological regulation

With the advent of digital and immersive technologies, **health and well-being has witnessed the emergence of innovative digital interventions including autonomous sensory meridian response (ASMR)**. ASMR refers to a pleasurable tingling sensation on the skin in response to a range of audio-visual triggers such as whispering, often accompanied by feelings of mild euphoria, relaxation and overall well-being[444]. ASMR has garnered a large and enthusiastic community online, in which creators produce and share videos and sounds to trigger an ASMR response among viewers. These videos typically feature whispered communication, quiet sounds and immersive audio recorded with microphones, often listened to with headphones to enhance the sense of proximity[445]. The visual component, while secondary, usually depicts a person in extreme close-up performing repetitive tasks or simulating personal care routines such as haircuts or medical check-ups, fostering a unique form of "distant intimacy"[446].

ASMR has likewise gained attention for its **potential therapeutic benefits**, demonstrating effectiveness in alleviating stress, anxiety, insomnia and even temporary relief from depression and chronic pain[447]. While empirical evidence remains limited, the growing interest in ASMR's therapeutic applications underpins its relevance in the context of digital health. Notably,

436 Waqas, M., Gururaj, Y. P., Mitra, V.D., Karri, S.A., Reddy, R., & Azeemuddin, S. (2024). Using virtual reality for detection and intervention of depression: A systematic literature review. arXiv preprint arXiv:2403.01882.

437 Boeldt, D., McMahon, E., McFaul, M., & Greenleaf, W. (2019) Using Virtual Reality Exposure Therapy to Enhance Treatment of Anxiety Disorders: Identifying Areas of Clinical Adoption and Potential Obstacles. *Front. Psychiatry*, 2019 Oct 25;10:773. doi: 10.3389/fpsyt.2019.00773. PMID: 31708821; PMCID: PMC6823515

438 Spytska, L. (2024). The use of virtual reality in the treatment of mental disorders such as phobias and post-traumatic stress disorder. *SSM - Mental Health*, 6, 100351. https://doi.org/10.1016/j.ssmmh.2024.100351

439 For an example, see oVRcome: https://www.ovrcome.io/

440 Zheng, Z., Liang, L., Luo, X., Chen, J., Lin, M., Wang, G., & Xue, C. (2024, 5 February). Diagnosing and tracking depression based on eye movement in response to virtual reality. *Front. Psychiatry*, 2024 Feb 5;15:1280935. doi: 10.3389/fpsyt.2024.1280935. PMID: 38374979; PMCID: PMC10875075.

441 Dixit, P., Phalswal, U., Kalal, N., & Srivastava, S.P. (2024). Effectiveness of virtual reality-supported exercise therapy in improving upper extremity function and activities of daily living among patients after stroke: A systematic review of randomized control trials. *Osong Public Health and Research Perspectives.* 15(3), pp. 189-200. doi: 10.24171/j.phrp.2023.0148.

442 Appel, L., Ali, S., Narag, T., Mozeson, K., Pasat, Z., Orchanian-Cheff, A., & Campos, J.L. (2021). Virtual reality to promote wellbeing in persons with dementia: A scoping review. *J. Rehabil. Assist. Technol. Eng.,* 2021 Dec 21;8:20556683211053952. doi: 10.1177/20556683211053952. PMID: 35024166; PMCID: PMC8743938.

443 Newton, C., Pope, M., Rua, C. et al. (2024). Entorhinal-based path integration selectively predicts midlife risk of Alzheimer's disease. *Alzheimer's Dement*., 2024; 20: 2779-2793. https://doi.org/10.1002/alz.13733

444 Poerio, G.L., Blakey, E., Hostler, T.J., & Veltri, T. (2018). More than a feeling: Autonomous sensory meridian response (ASMR) is characterized by reliable changes in affect and physiology. *Plos One*, 13(6), e0196645. https://doi.org/10.1371/journal.pone.0196645

445 Brubaker, R. (2020). Digital hyperconnectivity and the self, *Theory and Society*, vol.49, pp.771-801. Available at: https://link.springer.com/article/10.1007/s11186-020-09405-1

446 Andersen, J. (2015). Now You've Got the Shiveries: Affect, Intimacy, and the ASMR Whisper Community. *Television & New Media*, 16(8), 683-700. https://doi.org/10.1177/1527476414556184

447 Barratt, E.L., & Davis, N.J. (2015). Autonomous Sensory Meridian Response (ASMR): a flow-like mental state. *PeerJ.*, 2015 Mar 26;3:e851. doi: 10.7717/peerj.851. PMID: 25834771; PMCID: PMC4380153.

ASMR represents a novel form of self-regulation that contrasts sharply with the hyperconnected nature of modern digital life, while also offering a counterbalance to the stressors exacerbated by digital hyperconnectivity, such as heightened anxiety and sleep disturbances[448].

Advances in Web 4.0 technologies, particularly **wearable biosensors and AI-driven systems, have further expanded the potential of ASMR as a tool for emotional and physiological regulation**. For instance, ASMR's ability to modulate physiological signals such as heart rate and electrodermal activity (EDA) has also been documented[449]. Emotional arousal, which influences skin conductivity, is also reflected in EDA measurements, with ASMR often being associated with lower EDA values and a reduced heart rate, indicative of a relaxed state. Building on these findings, a novel AI-driven emotion recognition system has been proposed to classify arousal levels and differentiate between emotions such as happiness and calmness experienced with ASMR. This system has achieved an accuracy of 88.8 %[450]**.** This integration of ASMR with AI and biosensing technologies exemplifies the potential for Web 4.0 to enhance health and well-being through personalised, privacy-preserving interventions, while simultaneously introducing potential avenues for the exploitation of private, health related data.

While Web 4.0 and virtual worlds offer transformative possibilities, **their immersive nature also raises significant concerns for mental and physical well-being**. As explored earlier in this paper, virtual worlds and their related technologies have the capacity to evoke powerful emotions such as anxiety, relaxation, fear and joy within artificial environments[451]. The potential for these emotions to be manipulated therefore presents risks to users. These include the potential for escapism, cognitive overload and challenges in distinguishing between virtual and real-world experiences[452]. These issues are especially pronounced in virtual worlds, where the boundaries between reality and simulation can be blurred[453]. One of the most pressing concerns is the heightened risk of isolation and the displacement of real-world relationships and needs[454,455]. Immersion in virtual worlds can lead individuals to escape reality, resulting in various social consequences such as reduced real-world social interactions and increased social isolation[456,457]. Prolonged exposure to virtual environments has likewise been with the subject of concerns related to the exacerbation of more serious mental health issues, including depression, paranoid ideation and even severe psychiatric conditions[458,459].

Negative physical effects including dizziness, disorientation and headaches (often collectively referred to as "cybersickness") associated with virtual worlds technologies, particularly VR and head-mounted displays (HMDs), have also been well documented, with research pointing to prolonged use as a key

448 Brubaker, R. (2020). Digital hyperconnectivity and the self, *Theory and Society*, vol.49, pp.771-801. Available at: https://link.springer.com/article/10.1007/s11186-020-09405-1

449 Engelbregt, H.J., Brinkman, K., van Geest C.C.E., Irrmischer, M., & Deijen, J.B. (2022). The effects of autonomous sensory meridian response (ASMR) on mood, attention, heart rate, skin conductance and EEG in healthy young adults. *Exp. Brain Res.,* 2022 Jun;240(6):1727-1742. doi: 10.1007/s00221-022-06377-9. Epub 2022 May 5. PMID: 35511270; PMCID: PMC9142458.

450 Gahlan, N., Sethia, D., & Ray, S.B. (2024). Emotion Analysis Using Auditory ASMR via Physiological Signals and Federated Learning. 2024 IEEE 20th International Conference on Body Sensor Networks (BSN), Body Sensor Networks (BSN), 2024 IEEE 20th International Conference On, pp. 1-4. https://doi.org/10.1109/BSN63547.2024.10780682

451 Diniz Bernardo, P., Bains, A., Westwood, S., & Mograbi, D.C. (2021). Mood induction using virtual reality: A systematic review of recent findings. *Journal of Technology in Behavioral Science*, 6, 3-24.

452 Hadi, R., Melumad, S., & Park, E.S. (2024). The Metaverse: A new digital frontier for consumer behavior. *Journal of Consumer Psychology*, 34(1), 142-166.

453 Hadi, R., Melumad, S., & Park, E.S. (2024). The Metaverse: A new digital frontier for consumer behavior. *Journal of Consumer Psychology*, 34(1), 142-166

454 Chen, D., & Zhang, R. (2022). Exploring research trends of emerging technologies in health metaverse: A bibliometric analysis. Available at SSRN 3998068.

455 Jabar, B A., Azmi, M., Hernando, G., Moniaga, J.V., & Alpaullivarez, A.A. (2022). The Social Impact of VR Technology on Society: A Systematic Literature Review. *Ultimatics: Jurnal Teknik Informatika*, 14(2), 57-62.

456 Chen, D., & Zhang, R. (2022). Exploring research trends of emerging technologies in health metaverse: A bibliometric analysis. Available at SSRN 3998068.

457 Jabar, B.A., Azmi, M., Hernando, G., Moniaga, J.V., & Alpaullivarez, A.A. (2022). The Social Impact of VR Technology on Society: A Systematic Literature Review. *Ultimatics: Jurnal Teknik Informatika*, 14(2), 57-62.

458 Chen, D., & Zhang, R. (2022). Exploring research trends of emerging technologies in health metaverse: A bibliometric analysis. Available at SSRN 3998068.

459 Jabar, B.A., Azmi, M., Hernando, G., Moniaga, J.V., & Alpaullivarez, A.A. (2022). The Social Impact of VR Technology on Society: A Systematic Literature Review. *Ultimatics: Jurnal Teknik Informatika*, 14(2), 57-62.

determinant of such symptoms[460,461,462]. In addition, the frequently sedentary nature of extended virtual engagement can lead to physical health problems such as eye strain, musculoskeletal disorders and a general decline in physical fitness[463]. As immersive technologies become more pervasive, scholars are increasingly alarmed by the potential for these environments to further encourage sedentary lifestyles, which can worsen existing mental and physical health issues including social isolation[464]. This concern is amplified by society's growing reliance on mobile devices, which already limits opportunities for physical activity[465]. Several studies also cite the risks of addiction to or dependency on virtual world technologies that are used to reduce stress or for entertainment[466,467,468]. Without careful consideration and proactive measures, the health risks associated with Web 4.0 could outweigh benefits, particularly for vulnerable populations.

The immersive environments of Web 4.0 and virtual worlds **introduce profound ethical and psychological challenges to user health and well-being, particularly in relation to identity, social dynamics and the exploitation of data**. The ability to inhabit customisable avatars, for instance, can destabilise conventional notions of body image and gender identity, while amplifying risks of discrimination, harassment and social exclusion based on virtual appearances[469,470]. As noted previously, the heightened realism and sense of presence in these environments can render experiences of bias or marginalisation more psychologically visceral – mirroring, and at times exacerbating, real-world inequalities. For children, excessive immersion in virtual worlds may disrupt physical, cognitive and social development, necessitating a balanced approach to virtual and real-world interactions[471]. For already vulnerable individuals, the immersive allure of Web 4.0 environments can exacerbate addiction, mental health challenges and other unforeseen harms[472]. Exposure to hyper-realistic virtual content, such as targeted advertisements, gambling simulations or explicit material, risks further normalising harmful behaviours and altering the cognitive patterns of users who are already at risk[473]. Urgent questions are also raised about "neuroprivacy", or the protection of neural and biometric data that could expose intimate aspects of user thought, emotion and identity[474].

---

460 Souchet, A.D., Lourdeaux, D., Pagani, A., & Rebenitsch, L. (2023). A narrative review of immersive virtual reality's ergonomics and risks at the workplace: cybersickness, visual fatigue, muscular fatigue, acute stress, and mental overload. *Virtual Reality*, 27(1), 19-50.

461 Kuber, P.M., & Rashedi, E. (2023). Alterations in physical demands during virtual/augmented reality-based tasks: A systematic review. *Annals of Biomedical Engineering*, 51(9), 1910-1932.

462 Nesbitt, K., & Nalivaiko, E. (2018). Cybersickness. In: Lee, N. (Ed.) *Encyclopedia of Computer Graphics and Games*. Springer, Cham. Available at: https://doi.org/10.1007/978-3-319-08234-9_252-1

463 Chen, D., & Zhang, R. (2022). Exploring research trends of emerging technologies in health metaverse: A bibliometric analysis. Available at SSRN 3998068.

464 Jabar, B.A., Azmi, M., Hernando, G., Moniaga, J.V., & Alpaullivarez, A.A. (2022). The Social Impact of VR Technology on Society: A Systematic Literature Review. *Ultimatics: Jurnal Teknik Informatika*, 14(2), 57-62.

465 Chen, D., & Zhang, R. (2022). Exploring research trends of emerging technologies in health metaverse: A bibliometric analysis. Available at SSRN 3998068.

466 Han, D.I.D., Bergs, Y., & Moorhouse, N. (2022). Virtual reality consumer experience escapes: preparing for the metaverse. *Virtual Reality*, 26(4), 1443-1458.

467 Taylor, A., tom Dieck, M.C., Jung, T., Cho, J., & Kwon, O. (2024). XR and mental wellbeing: state of the art and future research directions for the Metaverse. *Frontiers in Psychology*, 15, 1360260.

468 Ladikas, M., Madeira, O., Hahn, J., Correa Pérez, M., Caplice, G., & Gerasymenko, A. (2024). D3.1: State-of-art in XR policy debates. In M. Ladikas & M. Correa Pérez (Eds.), *The Equitable, Inclusive, and Human-Centered XR Project (XR4Human)* (Deliverable No. 3.1). Karlsruhe Institute of Technology (KIT). Grant Agreement No. 101070155.

469 World Economic Forum (2023). Social implications of the metaverse. In collaboration with Accenture. Available at: https://www3.weforum.org/docs/WEF_Social_Implications_of_the_Metaverse%20_2023.pdf

470 World Economic Forum (2024). Metaverse identity: Defining the self in a blended reality (Insight Report). In collaboration with Accenture. Retrieved from: https://www3.weforum.org/docs/WEF_Metaverse_Identity_Defining_the_Self_in_a_Blended_Reality_2024.pdf

471 Council of Europe & IEEE (2024). The metaverse and its impact on human rights, the rule of law and democracy. Council of Europe Publishing. ISBN 978-92-871-9465-7. Available at: https://rm.coe.int/the-metaverse-and-its-impact-on-human-rights-the-rule-of-law-and-democ/1680b178b0

472 Kaimara, P., Oikonomou, A., & Deliyannis, I. (2022). Could virtual reality applications pose real risks to children and adolescents? A systematic review of ethical issues and concerns. *Virtual Reality*, 26(2), 697-735.

473 Chen, D., & Zhang, R. (2022). Exploring research trends of emerging technologies in health metaverse: A bibliometric analysis. Available at SSRN 3998068.

474 de Oliveira Wood, G.M., Berger, L., Jarke, J., Barnard, G., Gremsl, T., Dolezal, E., ... & Zandonella, P. (2024). The protection of mental privacy in the area of neuroscience. Societal, legal and ethical challenges. *Publications Office of the European Union. Belgium.* Available at: https://coilink.org/20.500.12592/65fxu33

The scale of data collection on health and well-being that is required to power Web 4.0 further escalates privacy risks, creating more opportunities for discrimination. Emerging technologies aggregate vast biometric and behavioural user data, including pulse, sleep patterns, speech frequency and even penile thrusts. This data is often shared with third parties, without robust consent frameworks being put in place[475]. For example, a 2016 study of health apps revealed that user data from just 12 platforms was disseminated to 76 external entities, highlighting systemic vulnerabilities to exploitation[476]. Furthermore, the automation of data collection and the measurement of user data such as data on eye gaze, can be used to infer information about users' well-being among a myriad of other identity markers such as literacy levels, vision impairments, political views and gender[477]. Health data collected for wellness or employment purposes could then be repurposed for commercial gain, discrimination over insurance, or workplace monitoring – possibly contributing to an erosion of user trust[478]. The adoption of XR tools in the workplace poses additional safety risks, ranging from physical injuries caused by obscured vision (e.g. collisions, muscle strain) to psychological stress due to constant surveillance via biometric sensors[479,480] (see subsection 3.4.2 3.4.2for more on surveillance). In healthcare contexts, the possibility of "gamifying" medical services, such as using virtual rewards to encourage adherence to treatment, also risks trivialising care, compromising patient safety, and exposing sensitive health data to commercial exploitation[481]. For example, wearable devices and AI-driven apps can automate mood detection, delivering personalised content (e.g. calming ASMR videos) to regulate stress or arousal. While such innovations promise tailored support for well-being, they are also dependent on opaque algorithms overseen by corporate platforms, and therefor pose the risk of neurophysiological manipulation. The potential effects of such manipulation are already evident with the wide-scale adoption of dopamine-driven notification and recommendation systems that hijack reward pathways to sustain engagement[482], as well as growing concerns around AI-driven technologies that can entrench existing inequalities and systemic discrimination[483].

3.4.6. Discrimination

While Web 4.0 and virtual worlds offer transformative opportunities for social inclusion and equity, they simultaneously introduce new risks of discrimination. On the one hand, **Web 4.0 has the potential to mitigate discrimination** through decentralised identity solutions that prioritise user privacy, AI-driven systems that are designed to detect and counteract bias, and adaptive interfaces that enhance accessibility for diverse users. These innovations promise to create more inclusive digital environments in which individuals can engage equitably. On the other hand, **the very features that define Web 4.0, including its decentralisation and reliance on AI, also create fertile ground for bias to thrive, whether implicit or algorithmic**. As digital interactions become increasingly mediated by AI systems, concerns over algorithmic discrimination, avatar-based bias and digital exclusion grow more

---

475 Brubaker, R. (2020). Digital hyperconnectivity and the self, *Theory and Society*, vol.49, pp.771-801.

476 Couldry, N., & Mejias, U. A. (2019). Data and the threat to human autonomy. In: The costs of connection: How data is colonizing human life and appropriating it for capitalism, (pp.153 - 184). Stanford University Press, pp.153-184.

477 Paneva, V., Strauss, M., Winterhalter, V., Schneegass, S., & Alt, F. (2024). Privacy in the Metaverse. *IEEE Pervasive Comput.*, 23(3), 73–78. https://doi.org/10.1109/MPRV.2024.3432953

478 Ali, M., Naeem, F., Kaddoum, G., & Hossain, E. (2024). Metaverse Communications, Networking, Security, and Applications: Research Issues, State-of-the-Art, and Future Directions. *IEEE Commun. Surv. Tutorials,* 26(2), 1238-1278. https://doi.org/10.1109/COMST.2023.3347172

479 Middleton, M. (2022). Business, finance, and economics: The IEEE global initiative on ethics of extended reality (XR) report. IEEE Standards Association.

480 Zhou, R. (2024). Understanding the Impact of TikTok's Recommendation Algorithm on User Engagement. *International Journal of Computer Science and Information Technology*, 3. 201-208. Available at: https://www.researchgate.net/publication/382423048_Understanding_the_Impact_of_TikTok%27s_Recommendation_Algorithm_on_User_Engagement

481 Ali, M., Naeem, F., Kaddoum, G., & Hossain, E. (2024). Metaverse Communications, Networking, Security, and Applications: Research Issues, State-of-the-Art, and Future Directions. *IEEE Commun. Surv. Tutorials*, 26(2), 1238–1278. https://doi.org/10.1109/COMST.2023.3347172

482 Fourcade, M, & Johns, F. (2020). Loops, ladders and links: the recursivity of social and machine learning. *Theory and Society*, 49: pp. 803-832. Available at: https://link.springer.com/content/pdf/10.1007/s11186-020-09409-x.pdf

483 Heller, B. (2021). Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law, *23 Vanderbilt Journal of Entertainment and Technology Law*, 1. Available at: https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss1/1

pressing – particularly with respect to marginalised communities who face compounded risks of exploitation and further disenfranchisement. In addition, the merging of physical and virtual identities in Web 4.0 has the potential to amplify existing societal inequalities and give rise to new forms of digital prejudice. Thus, while Web 4.0 holds immense promise in terms of fostering equity, its unchecked development could entrench discrimination in ways that are both subtle and systemic.

Algorithmic decision-making under **Web 4.0 relies heavily on AI models trained on vast datasets, which can inadvertently perpetuate and amplify existing biases, leading to unfair and discriminatory outcomes**[484]. Today, real-world inequities are already often being reproduced in or exacerbated by AI-driven algorithms[485]. Ultimately, minority groups and under-represented individuals and communities face the highest risk of discrimination in these contexts, due to bias in datasets and input at algorithmic level[486]. Even when AI decision-making is coupled with human oversight, the human actor can either conform to or introduce their own biases in the mix[487]. Moreover, given the potential for sensitive data to fall into the hands of bad actors, concerns have been raised in the literature over a higher risk of discriminatory attacks affecting the dignity and identity of users both online and offline[488], calling into question fundamental freedoms. Studies and research have demonstrated that machine learning models exhibit gender, racial and socio-economic biases. Such biases can influence hiring, lending and content recommendation systems in ways that disadvantage marginalised groups[489,490]. For example, LinkedIn's recruitment algorithm was found to prioritise male candidates over female candidates due to historical job-seeking behaviours[491]. Similarly, algorithms deployed in healthcare settings have assigned lower risk scores to poorer patients compared with wealthier ones, reflecting systemic inequalities in healthcare access and treatment[492]. Such biases can originate from unrepresentative training data, algorithmic design flaws, or institutional practices that mirror societal inequities[493]. In response to such risks, the adoption of ethical guidelines for algorithmic design and machine learning has helped in ameliorating biases, while other AI-assisted interventions have also been used to create better interventions by, for example, using predictive and prescriptive analytics to identify biased decision-making or patterns of bias within the workplace[494]. The box below further details how biases are exhibited within general-purpose AI models specifically.

Figure 10. Example: biases in general-purpose AI (GPAI) models

Preliminary studies of the providers of industry-leading GPAI models have identified samples generated from language models such as Open AI's ChatGPT, Google's Gemini and Meta's LLaMA that **contain and reinforce social biases towards**

484 Hanna, M.G., Pantanowitz, L., Jackson, B., Palmer, O., Visweswaran, S., Pantanowitz, J., Deebajah, M., & Rashidi, H.H. (2024). Ethical and Bias Considerations in Artificial Intelligence/Machine Learning. *Modern Pathology*, 38(3), 100686. Advance online publication. Available at: https://doi.org/10.1016/j.modpat.2024.100686

485 Bachelet, M (2019). Human rights in the digital age, United Nations Hum. Rts.Off. High Comm'r (17 October 2019), https://www.ohchr.org/en/speeches/2019/10/human-rights-digital-age

486 Council of Europe (2024). *The metaverse and its impact on human rights, the rule of law, and democracy*. Retrieved from https://rm.coe.int/the-metaverse-and-its-impact-on-human-rights-the-rule-of-law-and-democ/1680b178b0

487 European Commission: Joint Research Centre, Gaudeul, A., Arrigoni, O., Charisi, V., Escobar Planas, M., & Hupont Torres, I. (2025). The Impact of Human-AI Interaction on Discrimination, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2760/0189570, JRC139127

488 Council of Europe (2024). *The metaverse and its impact on human rights, the rule of law, and democracy*. Retrieved from https://rm.coe.int/the-metaverse-and-its-impact-on-human-rights-the-rule-of-law-and-democ/1680b178b0

489 Bolukbasi, T., Chang, K.-W., Zou, J., Saligrama, V., & Kalai, A. (2016). Man is to computer programmer as woman is to homemaker? Debiasing word embeddings. arXiv preprint arXiv:1607.06520. https://doi.org/10.48550/arXiv.1607.06520

490 Wood, D.C. (2021). Facial Recognition, Racial Recognition, and the Clear and Present Issues with AI Bias. *RAIL: The Journal of Robotics, Artificial Intelligence & Law*, 4(3), 219–222.

491 Hao, K. (2021, 23 June). LinkedIn's job-matching AI was biased. The company's solution? More AI. *MIT Technology Review*. https://www.technologyreview.com/2021/06/23/1026825/linkedin-ai-bias-ziprecruiter-monster-artificial-intelligence/

492 Obermeyer, Z, Powers, B, Vogeli, C, & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, 2019 Oct 25;366(6464):447-453. doi: 10.1126/science.aax2342. PMID: 31649194.

493 Liao, W., & Sundar, S.S. (2022). Are we morally obligated to eliminate bias in AI? Algorithmic biases and users' moral concerns. *Philosophy & Technology*, 35(3), 58. https://doi.org/10.1007/s13347-022-00512-8

494 Lin, Y. T., Hung, T.W., & Huang, L. T. L. (2021). Engineering equity: How AI can help reduce the harm of implicit bias. *Philosophy & Technology*, *34*(suppl 1), 65-90.

certain demographics[495]. These biases include gender, racial, ethnic, religious, age-based and socio-economic biases[496,497,498]. For example, the performance of these models might vary when dealing with different demographic groups, leading to discriminatory outcomes such as stereotyping, the inequitable allocation of resources, dehumanisation, or the erasure of certain groups[499].

Biases in GPAI models often stem from human-generated training data. Large quantities of labelled data, predominantly retrieved from the web, may reflect historical and societal inequalities, or can inherit prejudices of prior decision-makers[500]. When GPAI models are then used in various downstream applications, such as language modelling, image captioning and visual recognition models, embedded stereotypes, biases and their associated harms can be further amplified. For instance, in a study on the amplification of gender bias in object classification and visual labelling models, researchers found that cooking was over 33 % more likely to involve women than men in a model's training set, and a trained model further amplified this disparity to 68 %[501].

These systems, while demonstrating remarkable capabilities in specified tasks, can often reinforce stereotypes or create "filter bubbles" that limit exposure to diverse perspectives[502]. **The immersive nature of virtual worlds can intensify these effects, as users engage with information on a deeper emotional level than traditional media allows**. For example, virtual reality simulations that portray emotionally charged or controversial content can manipulate users' emotions to evoke fear, loyalty or anger, thereby shaping their perceptions of real-world events or political issues. This heightened emotional engagement makes users more vulnerable to manipulation, as immersive experiences can elicit strong emotional responses that significantly influence decision-making[503].

In virtual worlds, the adoption of virtual identities also introduces novel forms of bias. Due to the heightened sense of presence and realism in such environments, such experiences of discrimination can be more visceral and psychologically damaging for users[504]. **Web 4.0 users may also face discrimination on the basis of the characteristics of their avatars** (e.g. in terms of race, age or disability), which can amplify psychological harm due to the visceral realism of XR experiences. For example, presenting users with elderly avatars has been shown to motivate support for non-profit organisations serving seniors[505]. However, without careful design choices (e.g. inaccessible VR interfaces), virtual worlds can also risk replicating real-world marginalisation such as profiling, targeting or discrimination based on the appearance or embodiment of their avatars, and on the behavioural and biometric data collected. Recent trends have underlined these challenges, revealing that while users with disabilities may be willing to disclose certain aspects of their disabilities through

495 Sheng, E., Chang, K.-W., Natarajan, P., & Peng, N. (2019). The woman worked as a babysitter: On biases in language generation. Available at: https://arxiv.org/pdf/1909.01326

496 Bolukbasi, T., Chang, K.-W., Zou, J.Y., Saligrama, V., & Kalai, A.T. (2016). Man is to computer programmer as woman is to homemaker? debiasing word embeddings. *Advances in Neural Information Processing Systems*, 29. Available at: https://proceedings.neurips.cc/paper_files/paper/2016/file/a486cd07e4ac3d270571622f4f316ec5-Paper.pdf

497 Dev, S., Sheng, E., Zhao, J., Amstutz, A., Sun, J., Hou, Y., Sanseverino, M. et al. (2021). On measures of biases and harms in NLP. Available at: https://arxiv.org/pdf/2108.03362

498 Zhao, D., Wang, A., & Russakovsky, O. (2021). Understanding and evaluating racial biases in image captioning. In: *Proceedings of the IEEE/CVF International Conference on Computer Vision*, pp. 14830-14840. Available at: https://openaccess.thecvf.com/content/ICCV2021/papers/Zhao_Understanding_and_Evaluating_Racial_Biases_in_Image_Captioning_ICCV_2021_paper.pdf

499 Dev, S., Sheng, E., Zhao, J., Amstutz, A., Sun, J., Hou, Y., Sanseverino, M. et al. (2021). On measures of biases and harms in NLP. Available at: https://arxiv.org/pdf/2108.03362

500 Barocas, S., & Selbst, A.D. (2016). Big data's disparate impact. *Calif. L. Rev.* 104: 671

501 Zhao, J., Wang, T., Yatskar, M., Ordonez, V., & Chang, K.-W. (2017). Men also like shopping: Reducing gender bias amplification using corpus-level constraints. Available at: https://arxiv.org/pdf/1707.09457

502 Rodilosso, E. (2024). Filter Bubbles and the Unfeeling: How AI for Social Media Can Foster Extremism and Polarization. *Philosophy & Technology*, 37(2). https://doi.org/10.1007/s13347-024-00758-4

503 Kourtesis, P. (2024). A Comprehensive Review of Multimodal XR Applications, Risks, and Ethical Challenges in the Metaverse. *Interact*, 2024, 8, 98. https://doi.org/10.3390/mti8110098

504 More information is available in the Background document accompanying this paper.

505 Yoo, S.-C., Peña, J.F., & Drumwright, M.E. (2015). Virtual shopping and unconscious persuasion: The priming effects of avatar age and consumers' age discrimination on purchasing and prosocial behaviors. *Computers in Human Behavior*, 48, 62–71. https://doi.org/10.1016/j.chb.2015.01.042

their avatars, these disclosures are often selective, reflecting ongoing concern about bias and exclusion in virtual worlds[506].

Exclusionary design is another critical issue. Thus, encouraging the design and production of affordable and accessible ICT equipment and services is also a key focus of WSIS Action Line 2 on promoting inclusive information and communication infrastructure[507]. XR technologies are especially susceptible to being exclusionary by design for people with disabilities, due to the immersive nature of the technologies deployed[508]. Exclusion and a lack of consideration for certain groups such as people with functional limitations during the design stages of virtual worlds can lead to the creation of spaces that introduce or perpetuate biases and discrimination[509]. While more specialised Web 4.0 technologies such as neurotechnologies are currently limited to healthcare applications, they also involve invasive implants for medical treatment and have therefore been scrutinised from an accessibility standpoint. While technologies hold promise for conditions such as rheumatoid arthritis or severe paralysis, their invasiveness raises ethical questions with regard to broader adoption and discriminatory design[510]. However, with a growing range of technological options available, from fully external to partially invasive devices, solutions can also be tailored to meet user needs and comfort levels. Importantly, as commercial applications grow, it is essential to ensure that these technologies do not exacerbate existing inequalities or create new forms of exclusion.

In Web 4.0, the adoption of AI and other advanced technologies further enables threats to information access, freedom of speech and thought, as well as rising levels of online misinformation. Issues including the profiling of users, or limiting access to certain discourses or information as a result of biased algorithmic recommendation systems, often serve as the basis for misinformation. Coupled with the exploitation of cognitive biases in immersive environments, such as the use of emotionally appealing or repetitive content, or subtle alterations of user beliefs and perceptions, can lead to the spread of wider disinformation campaigns[511].

3.5. Sustainability, resource efficiency and the ethical production of technology

Evolution towards Web 4.0 presents **significant sustainability challenges**, including rising energy consumption, competition for critical resources, and the environmental impacts associated with digital infrastructure and technologies. The growing demand for digital services exacerbates pressures on electricity grids, raw material supplies and waste management systems. At the same time, **AI and digital twins offer solutions for energy efficiency**. These include enhanced governance over energy consumption, material use and waste management. Through advanced modelling and optimisation, these technologies can contribute to more sustainable economies.

The upcoming subsections cover two key areas of challenge with respect to sustainability, resource efficiency and the ethical production of technology. Subsection 3.5.1 discusses energy efficiency in light of the advancement of Web 4.0. The challenges associated with resource extraction, the use of materials and e-waste are elaborated in subsection 3.5.2.

---

506 Zhang, K., Deldari, E., Lu, Z., Yao, Y., & Zhao, Y. (2022). "It's just part of me:" understanding avatar diversity and self-presentation of people with disabilities in social virtual reality. In: *The 24th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '22)*, p. 1. Association for Computing Machinery (ACM). https://doi.org/10.1145/3517428.3544829

507 WSIS (2003). Declaration of Principles. Building the Information Society: a global challenge in the new Millennium. Available at: https://www.itu.int/net/wsis/docs/geneva/official/dop.html

508 Fox, D., Thornton, I.G. (2022). White Paper - The IEEE Global Initiative on Ethics of Extended Reality (XR) Report - -Extended Reality (XR) Ethics and Diversity, Inclusion, and Accessibility, *IEEE*. Available at: https://ieeexplore.ieee.org/document/9727122

509 Council of Europe (2024). *The metaverse and its impact* on human rights, the rule of law, and democracy. Retrieved from https://rm.coe.int/the-metaverse-and-its-impact-on-human-rights-the-rule-of-law-and-democ/1680b178b0

510 Accenture (2024). *Tech Vision 2024*. Retrieved from https://www.accenture.com/content/dam/accenture/final/accenture-com/document-2/Accenture-Tech-Vision-2024.pdf.

511 Council of Europe (2024). *The metaverse and its impact on human rights, the rule of law, and democracy*. Retrieved from https://rm.coe.int/the-metaverse-and-its-impact-on-human-rights-the-rule-of-law-and-democ/1680b178b0

3.5.1. Energy efficiency

The exponential growth in ICT infrastructure driven by hyperscale data centres, cloud computing and use of AI accounts for a significant and growing share of energy demand. Electricity consumption by data centres (excluding cryptocurrencies) accounted for between 1 % and 1.3 % of global electricity demand in 2022. This could rise to between 1.5 % and 3 % by 2026 and more[512]. To put this into perspective, primary aluminium production consumes around 4 % of the world's electricity. Electric vehicles are likely to account for between 1.5 % and 2 % of electricity consumption by 2026. In some regions, energy consumption by data centres already accounts for a significantly larger share of total electricity usage (e.g. 18 % in Ireland and 10 % in Denmark in 2022)[513]. In the online consultation carried out during the preparation of this paper, a majority of respondents – 36 out of 66 (54 %) – fully agreed that environmental sustainability should be a core consideration in the development of Web 4.0 infrastructure, while 9 respondents (14 %) partially agreed with this statement (see Annex 2)[514].

The **development and use of AI has significant implications** for future energy consumption. Training generative AI is energy intensive and consumes significantly more electricity than traditional data-centre activities. For instance, training GPT-3 is estimated to have consumed about 1,300 megawatt hours (MWh), while the training of the more advanced GPT-4 is estimated to have used 50 times more electricity. Meanwhile the example of DeepSeek shows that LLMs can be trained using more limited resources – although these energy savings may be offset by the energy consumption of a given model in generating answers, as well as the length of the responses produced[515].

Conversely, AI is also emerging as a **key enabler of energy efficiency**. It is driving innovations that support the transition towards cleaner energy systems. Some use cases include forecasting energy supply and demand, energy grid management, predictive maintenance and energy efficiency in buildings[516,517,518]. In addition to these improvements in efficiency, AI also accelerates the discovery of materials (e.g. identifying improved battery chemistries) and process optimisation in energy-intensive industries such as steel manufacturing[519].

Beyond AI, other Web 4.0 related technologies will have significant impacts on energy consumption – for example, digital trust technologies. Quantum technologies are also energy intensive[520], although they may also suggest solutions for optimising energy use[521].

Ensuring a **reliable and sustainable energy supply** Is central to the development of Web 4.0 and virtual worlds. ICT facilities, especially data centres and AI computing clusters, compete with other electrified sectors (e.g. electric vehicles, residential heating) for limited power resources. This places stress on power grids, potentially leading to regional instability. The risk of energy shortages varies by country,

---

512 International Energy Agency (IEA) (2024, July). Electricity market mid-year update 2024. IEA. Available at: https://iea.blob.core.windows.net/assets/234d0d22-6f5b-4dc4-9f08-2485f0c5ec24/ElectricityMid-YearUpdate_July2024.pdf

513 World Economic Forum (2024, July). AI and energy: Will AI help reduce emissions or increase demand? Here's what to know. World Economic Forum. Available at: https://www.weforum.org/stories/2024/07/generative-ai-energy-emissions/

514 The rest of the responses were broken down as follows: a total of 7 of respondents (11 %) fully disagreed with the statement, while 4 (6 %) disagreed to some extent. A total of 5 of respondents (8 %) did not express a strong preference with regard to this statement (responding "neither agree nor disagree"), while the same number of respondents offered no opinion on the topic at all.

515 MIT Technology Review (2025 Januari 31). DeepSeek might not be such good news for energy after all. Available at: https://www.technologyreview.com/2025/01/31/1110776/deepseek-might-not-be-such-good-news-for-energy-after-all/

516 International Energy Agency (2023). Why AI and energy are the new power couple – Analysis. Available at: https://www.iea.org/commentaries/why-ai-and-energy-are-the-new-power-couple

517 International Energy Agency (2024). What the data centre and AI boom could mean for the energy sector – Analysis. Available at: https://www.iea.org/commentaries/what-the-data-centre-and-ai-boom-could-mean-for-the-energy-sector

518 European Commission (2020). White Paper on Artificial Intelligence: European approach to artificial intelligence. Available at: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

519 International Energy Agency (IEA) (2024). How will artificial intelligence transform energy innovation? Available at: https://www.iea.org/commentaries/how-will-artificial-intelligence-transform-energy-innovation

520 Martin, M., Hughes, C., Moreno, G., Jones, E., Sickinger, D., Narumanchi, S., & Grout, R. (2021). Designing energy-efficient quantum computers through prediction and reduction of cooling requirements for cryogenic electronics. National Renewable Energy Laboratory (NREL). Available at: https://www.nrel.gov/docs/fy21osti/77200.pdf

521 Reymond, G.O. (2025, 8 January). How quantum computing can revolutionize energy forecasting and optimization. World Economic Forum. Available at: https://www.weforum.org/stories/2025/01/quantum-computing-energy-forecasting/

with some regions facing a higher likelihood of constraints due to existing grid vulnerabilities and energy transition challenges[522].

Grid vulnerability analyses indicate that nearly 65 % of public internet infrastructure components are clustered within fewer than 10 power grid failure zones[523]. Furthermore, when considering dependencies on the grids that supply data centres, the effective number of isolated availability zones for cloud services (e.g. AWS) can drop from 87 to 19, illustrating the high concentration of risk to energy networks posed by digital infrastructure. These dependencies underline the need to integrate renewable energy sources, develop microgrids and develop energy storage solutions[524].

To address grid vulnerabilities and alleviate pressure on individual power grids, companies are considering the wider geographical distribution of their data centre locations, thereby ensuring more balanced energy demand across regions[525]. **Edge computing solutions** present another useful approach, as these distribute processing power and reduce reliance on large, centralised data centres[526].

AI-powered energy management systems leverage machine learning and predictive analytics to enhance the resilience of data centres. Meanwhile, digital twins enable the real-time monitoring and optimisation of energy distribution and consumption, improving resource (re-)allocation. In addition, digital technologies can facilitate the creation of virtual power plants, which aggregate distributed energy resources and better manage the dynamics of supply and demand.

Lastly, implementing advanced grid management systems allows utilities to more effectively handle the fluctuating energy loads associated with data centres[526]. These solutions will be critical to balancing the growing energy demands of digital infrastructure while ensuring a sustainable and resilient energy future.

3.5.2. Resource extraction, use of materials and e-waste

The **semiconductor industry** is the backbone of modern digital systems, yet its production is highly resource-intensive, requiring significant amounts of rare earth elements, cobalt, copper, lithium, selenium and nickel. Manufacturing a two-kilogram computer requires up to 800 kilograms of raw materials, while a single smartphone requires approximately 70 kilograms from production to disposal[527]. Beyond semiconductors, the broader digital hardware industry is equally material-intensive, relying on critical raw materials to sustain the integration of digital technologies across all sectors.

Development **towards the future internet and Web 4.0** will require an increasing amount of critical materials. This contributes to ecological disruption and increases carbon emissions due to extraction and processing. In addition, data centres also place significant pressure on **water resources**. The cooling systems in data centres rely on clean water to prevent corrosion, which leads to competition with local communities for potable water[528]. In the United States, 20 % of direct water consumption by data centre servers originates from watersheds that experience moderate to high water stress[527]. Despite these challenges, data centre operators are often drawn to such locations, due to the availability of energy sources such as solar and wind power.

522 World Economic Forum (2025). Global risks report 2025. Available at: https://www.weforum.org/publications/global-risks-report-2025/
523 Jyothi, S. (2023). Characterizing the role of power grids in internet resilience. Available at: https://arxiv.org/abs/2306.02502
524 World Economic Forum (2024). Energy transition: Getting grids ready for an electrified future. Available at: https://www.weforum.org/stories/2023/08/energy-transition-electricity-grids-digital-net-zero/
525 Mytton, D., Ashtine, D., Wheeler, S., & Wallom, D. (2023). Stretched grid? Managing data center energy demand and grid capacity, *Oxford Open Energy*, Volume 2, 2023, oiad014, Available at: https://doi.org/10.1093/ooenergy/oiad014
526 International Energy Agency (2024). What the data centre and AI boom could mean for the energy sector. Available at: https://www.iea.org/commentaries/what-the-data-centre-and-ai-boom-could-mean-for-the-energy-sector
527 United Nations Conference on Trade and Development (UNCTAD) (2024). Digital Economy Report 2024: Shaping an environmentally sustainable and inclusive digital future. Available at: https://unctad.org/publication/digital-economy-report-2024
528 Li, P., Yang, J., Islam, M.A., & Ren, S. (2025). Making AI less "thirsty": Uncovering and addressing the secret water footprint of AI models. arXiv preprint arXiv:2304.03271. Available at: https://doi.org/10.48550/arXiv.2304.03271

Digitalisation has led to an **e-waste crisis**, due to rising device consumption, limited repairability and short product lifecycles. E-waste is the fastest growing category of waste[529]. Between 2010 and 2022, waste from screens and small IT equipment rose by 30 %, reaching 10.5 million tons. Rising demand for high-performance computing, immersive extended reality (XR) devices and decentralised digital infrastructures could lead to ever-larger amounts of e-waste. Because only a small share of it is currently collected and recycled, e-waste leads to pollution and environmental hazards, especially in developing countries. Historically, a significant share of e-waste has been exported to developing countries – in many cases, by exploiting loopholes in legislation[530].

Many modern devices are **intentionally designed to be difficult to repair**, featuring glued components, non-replaceable batteries and proprietary restrictions that limit independent repair options. This design approach forces consumers to replace rather than repair, contributing to the premature disposal of devices. Sometimes, manufacturers intentionally limit product lifespan through hardware restrictions or discontinued software support. This pushes consumers towards upgrading devices frequently. Non-standardised accessories such as chargers and cables further drive unnecessary waste by limiting interoperability between brands[531].

The **short lifespan of digital products** remains a significant issue. Laptops typically last up to four or five years, while smartphones are often replaced within three years. Other Web 4.0-related infrastructure, including the hardware for cloud and edge computing, XR devices and AI-powered systems will contribute significantly to electronic waste. Such hardware requires regular replacement, as it operates 24/7 and is subject to high performance demands, leading to the large-scale disposal of servers and networking equipment. The increasing integration of electronics into short-lived consumer products, including gadgets and toys, further accelerates the accumulation of digital waste[532]. Thus, without systemic change in the way digital products are designed, used and disposed of, the **environmental footprint** of digitalisation is likely to continue to grow as technologies evolve towards Web 4.0.

Lastly, the **extraction of raw materials** has been linked to human rights violations[533]. Given that this is the beginning of the supply chain, it affects many digital technologies and products. For instance, a significant share of cobalt and copper, used in smartphones, tablets, laptops and electric vehicles, is supplied by the Democratic Republic of Congo, where forced evictions and child labour have been documented[534]. The growing amount of the digital equipment involved in the evolution towards Web 4.0 will significantly increase demand such raw materials. Companies producing digital technologies must not ignore evidence of human rights violations in the supply chain. At the same time, Web 4.0 innovations also offer powerful tools to mitigate their adverse impacts. For example, IoT and AI can enhance resource efficiency, while smart contracts and digital product passports create transparent,

529 IEEE Standards Association (2022). Extended Reality (XR) and Metaverse Governance: A framework for responsible development and implementation. IEEE. Available at: https://standards.ieee.org/wp-content/uploads/2022/06/XR_Metaverse_Governance.pdf

530 UNITAR Global e-Waste Monitor 2024: Electronic Waste Rising Five Times Faster than Documented E-waste Recycling. Available at: https://unitar.org/about/news-stories/press/global-e-waste-monitor-2024-electronic-waste-rising-five-times-faster-documented-e-waste-recycling

531 United Nations Environment Programme (UNEP) (2021). *Global e-waste monitor 2020*. Available at: https://globalewaste.org/

532 Organisation for Economic Co-operation and Development (OECD) (2020). Improving resource efficiency and the circularity of economies for a greener world. Available at: https://www.oecd.org/en/publications/improving-resource-efficiency-and-the-circularity-of-economies-for-a-greener-world_1b38a38f-en.html

533 Kara, S. (2023). *Cobalt red: How the blood of the Congo powers our lives*. St. Martin's Press.

534 Amnesty International (2023). *DRC: Powering Change or Business as Usual?* (Document No. AFR 62/7009/2023). Available at: https://www.amnesty.org/en/documents/AFR62/7009/2023/en/

immutable records of each product's lifecycle, from extraction and production to use and disposal, thereby enhancing accountability throughout the supply chain[535,536,537].

3.6. Economic challenges and business opportunities

As acknowledged in the Global Digital Compact, advancing meaningful inclusion requires groundwork to be laid for a predictable and transparent environment which, among other things, promotes fair competition and digital entrepreneurship, and tackles existing concentrations of technological capacity and market power[538]. Similarly, the WSIS states that "policies that create a favourable climate for stability, predictability and fair competition at all levels should be developed and implemented in a manner that not only attracts more private investment for ICT infrastructure development but also enables universal service obligations to be met in areas where traditional market conditions fail to work"[539].

In recent years, investment in research and development (R&D) on the metaverse has grown, reaching levels comparable to early investments in AI[540]. When it comes to providing Web 4.0 technologies, new business models for virtual worlds and development platforms, as well as software and hardware (e.g. headsets, haptic devices) are set to become increasingly important. According to some estimates, the industrial metaverse is set to be even bigger than the consumer metaverse[541]. The global metaverse market, which combines virtual reality, AI and blockchain to create interactive digital ecosystems, is expected to reach **2,633 million users by 2030**[542].

In the present paper, we identify several distinct challenges and opportunities that are relevant to the advancement of Web 4.0 and virtual worlds. These include gaps in investment and capacity, as well as competition and power concentration, global trade and data ownership, and business adoption. These are described in more detail in the subsections below.

3.6.1. Investment

The development of Web 4.0 and virtual world technologies requires **sustained interest and investment** in innovation and digital infrastructure. Multiple players are acting as first movers in this field, investing millions in Web 4.0 and virtual worlds. These players include existing Big Tech companies, as well as gaming companies and venture capital. Overall, forecasts show that the global market for virtual worlds could reach more than USD 800 billion by 2030[543]. At the same time, significant gaps in investment exist that could affect the realisation of the full potential of virtual worlds and Web 4.0.

---

535 McKinsey Global Institute (2021). The Internet of Things: Catching up to an accelerating opportunity. Available at: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/iot%20value%20set%20to%20accelerate%20through%202030%20where%20and%20how%20to%20capture%20it/the-internet-of-things-catching-up-to-an-accelerating-opportunity-final.pdf

536 Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, 57(7), 2117-2135. https://doi.org/10.1080/00207543.2018.1533261

537 European Parliament and Council. (2023, 12 July). Regulation (EU) 2023/1542 concerning batteries and waste batteries, amending Directive 2008/98/EC and Regulation (EU) 2019/1020 and repealing Directive 2006/66/EC. Official Journal of the European Union, L 191/1. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1542

538 UN (2024). Global Digital Compact. Available at: https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf

539 WSIS (2003). Declaration of Principles. Building the Information Society: a global challenge in the new Millennium. Available at: https://www.itu.int/net/wsis/docs/geneva/official/dop.html

540 McKinsey & Company (2022). Value creation in the metaverse. Available at: https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/value-creation-in-the-metaverse

541 Collin, J.,Pellikka, J., &Penttinen, J.T.J. (2024). Next Steps Toward the Industrial Metaverse and 6G. 5G Innovations for Industry Transformation: Data-driven Use Cases , IEEE, pp.235-253, doi: 10.1002/9781394181513.ch15

542 Taken from: https://www.statista.com/outlook/amo/metaverse/worldwide

543 Verified Market Research (2022) Metaverse Market size worth $824.53 Billion, Globally, by 2030 at 39.1%. https://www.prnewswire.com/news-releases/metaverse-market-size-worth--824-53-billion-globally-by-2030-at-39-1-cagr-verified-market-research-301585725.html

Big Tech companies including Meta, Microsoft, Google and Apple are investing heavily in metaverse infrastructure, hardware (VR/AR headsets), software platforms and content creation tools[544]. The focus of these investments ranges from building immersive social platforms (Meta's Horizon Worlds) to enterprise collaboration tools (Microsoft Mesh), cloud computing infrastructure for metaverse applications, and proprietary hardware ecosystems. Meta, for example, has unveiled a USD 100 billion investment plan for its XR portfolio[545]. Similarly, Google has invested USD 39.5 million in a private equity fund for virtual world-related technologies. Gaming companies such as Fortnite and Roblox are also at the forefront of investments in virtual worlds.

Looking at hardware specifically, current investment trends show that several large companies are driving investments in this area. This runs the risk of power being concentrated in the hands of a few players, thereby raising barriers to access for other companies looking to develop applications for virtual worlds[546]. Other large companies besides Meta are investing in hardware such as headsets. Sony Corporation is investing in the PSV2R2 headset; similarly, Lenovo has invested in its Mirage series of VR headsets, including the Lenovo Mirage Solo and Lenovo Explorer mixed-reality headsets[547]. The barriers to entry for smaller companies in the field are compounded by the fact that VC funds do not tend to trust VR/AR companies enough to provide them with finance, as they still perceive VR/AR technologies as a high-risk investment[548]. Subsection 3.6.2 further explores the risks of power concentration in virtual worlds and Web 4.0 environments.

Despite large investments in virtual worlds and Web 4.0-related technologies, gaps remain. First, significant investments are still **needed in the next-generation networks and computing power** needed to realise virtual worlds. As described in Section 2.3, the full realisation of virtual worlds and Web 4.0 requires low-latency and high-throughput network connections. Mass adoption of virtual worlds would lead to surges in demand for bandwidth, potentially leading to network congestion. Similarly, edge computing, which brings data processing closer to the user, requires large capital investments in distributed data centres and content delivery networks.

To address some of the above gaps, investments in next-generation networks are already on the rise. For example, investment priorities in the telecommunication sector are shifting to higher-speed access infrastructure such as fibre optic cable to the premises, next-generation mobile network connectivity and wireless technologies[549]. Similarly, companies are investing in data infrastructure. Nevertheless, a gap exists, with low- and middle-income countries struggling to attract private investments in data centres[550]. According to an analysis by the World Bank, a combination of factors including the cost and reliability of energy supply, digital infrastructure and regulatory environment tend to concentrate private sector investments in cloud infrastructure in the Global North[551]. Globally, 80 % of investments in the Web 4.0-related technologies of AI and blockchain are concentrated in China and the US[552].

Second, the development of high-quality 3D environments and interactive assets requires dedicated engines and 3D modelling tools. Similarly, 3D immersive environments must be able to scale and accommodate a growing number of participants in real time. An ICT skills gap exists in the

544 Smethurst, R., Barbereau, T., & Nilsson, J. (2023). The Metaverse's Thirtieth Anniversary: From a Science-Fictional Concept to the "Connect Wallet" Prompt. *Philosophy & Technology*, 36(3). https://doi.org/10.1007/s13347-023-00612-z

545 *Financial Times* (2025). Meta's investment in VR and smart glasses on track to top USD 100bn. https://www.ft.com/content/c513949e-3fc1-43a2-9358-363dff823bc1

546 Snijders, D., Horsman, S., Kool, L., & van Est, R. (2020). Responsible VR. Protect consumers in virtual reality. The Hague: Rathenau Instituut

547 https://www.emergenresearch.com/blog/top-10-companies-in-virtual-reality-headset-market

548 https://www.oficinamediaespana.eu/images/media_europa/StrategicpaperVRARCoalition.pdf

549 ITU (2025). Digital Infrastructure Investment Initiative Closing the digital infrastructure investment gap by 2030. Available at: https://www.itu.int/hub/publication/s-dii-diii-whitepaper-2025/

550 World Bank (2024) Digital Progress and Trends report 2023. Available at: https://openknowledge.worldbank.org/entities/publication/7617f89d-2276-413d-b0a7-e31e7527d6af

551 Ibid.

552 European Investment Bank (EIB) (2021). New EIB report: EUR 10 billion investment gap in artificial intelligence and blockchain technologies is holding back the European Union. Available at: https://www.eib.org/en/press/all/2021-181-new-eib-report-eur10-billion-investment-gap-in-artificial-intelligence-and-blockchain-technologies-is-holding-back-the-european-union

development of virtual environments[553]. Section 3.7 further elaborates on skills gaps in relation to virtual worlds and Web 4.0.

Furthermore, ensuring access to virtual worlds will require the connectivity gap to be bridged. Upgrading connectivity infrastructure alone will require significant investment[554,555,556,557]. The latest estimates point to a shortfall in investments globally of at least USD 1.6 trillion, primarily in developing regions[558]. Similarly, in a future in which XR hardware is developed within proprietary ecosystems, their high cost could exclude large segments of the population, leading to a widening connectivity gap.

The key factors determining adequate investment include public-private collaboration, market conditions that foster competition, and societal attitudes that maintain consumer and business demand for these technologies[559]. Insufficient or poorly distributed funding could lead to a stagnation in innovation, a loss of interest from the public and private sectors, and a concentration of market power, limiting opportunities for broader economic and social benefits[560].

Looking ahead, a gap exists in the "hype" surrounding virtual worlds and related technologies and their current capabilities[561]. Investments in virtual worlds and Web 4.0 technologies will be key to developing seamless and well-integrated virtual world experiences, as well as in overcoming existing technological barriers to virtual worlds, including sensors, reducing latency and improving the user-friendliness of hardware.

3.6.2. Competition and the concentration of power

The concentration of market power is common in digital markets, driven by factors such as network effects, economies of scale, switching costs, vertical integration and the benefits of early market entry[562,563]. As a result, digital markets are prone to strong advantages for incumbents, which make it harder for new entrants to challenge the existing dominant market players. For example, the concentration of power has, in the past, been observed in the markets for search engines, social media, e-commerce marketplaces and mobile operating systems[564].

The emerging segment of Web 4.0 and virtual worlds technologies is currently characterised by a variety of players from Big Tech to hardware providers and gaming companies. As noted above, some prominent players in the virtual worlds space include Meta, Microsoft, Nvidia, Epic Games, Roblox, Apple, Alphabet, Unity Technologies, Niantic, Tencent and others. Despite the lack of a single dominant

553 National Centre for Immersive Storytelling (2020). *Skills For Immersive Experience Creation*. Available at: https://www.storyfutures.com/uploads/images/SFICC-Report-2019-20.2.20.pdf
554 European Commission (2023). Results of the exploratory consultation on the future of the electronic communications sector and its infrastructure. Available at: https://digital-strategy.ec.europa.eu/en/library/results-exploratory-consultation-future-electronic-communications-sector-and-its-infrastructure
555 UN (2022). Achieving universal and meaningful digital connectivity. Setting a baseline and targets for 2030. Available at: https://www.itu.int/itu-d/meetings/statistics/wp-content/uploads/sites/8/2022/04/UniversalMeaningfulDigitalConnectivityTargets2030_BackgroundPaper.pdf
556 *The Guardian* (2019). Universal internet access unlikely until at least 2050, experts say. Available at: https://www.theguardian.com/technology/2019/jan/10/universal-internet-access-unlikely-until-2050-experts-say-lack-skills-investment-slow-growth
557 European Parliament: Directorate-General for External Policies of the Union, Directorate-General for Parliamentary Research Services, Directorate-General for the Presidency, Anghel, S., Antunes, L. et al. (2023). Future shocks 2023 – Anticipating and weathering the next storms, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2861/88235
558 UN Agency for Digital Technologies (2025). Digital infrastructure investment: USD 1.6 trillion to close the gap. Available at: https://www.itu.int/hub/2025/01/digital-infrastructure-investment-usd-1-6-trillion-to-close-the-gap/
559 PPMI & TNO (2025, forthcoming). Future of virtual worlds. Project 'Participatory Foresight for Next Generation Online Platforms'.
560 PPMI & TNO (2025, forthcoming). Future of the internet. Project 'Participatory Foresight for Next Generation Online Platforms'.
561 Rathenau Instituut (2023). Immersive technologies. Available at: https://www.rathenau.nl/en/digitalisation/immersive-technologies
562 Brühl, V. (2023). Big Tech, the platform economy and the European digital markets. *Intereconomics*, 58(5), 274–282. Available at: https://www.intereconomics.eu/contents/year/2023/number/5/article/big-tech-the-platform-economy-and-the-european-digital-markets.html
563 Hupont Torres, I. et al. (2023). Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU, Publications Office of the European Union, Luxembourg, doi:10.2760/51579, JRC133757.
564 Ibid.

player, the virtual worlds market is characterised by **few large and medium-sized players** located in a relatively small number of countries, predominantly in the Global North[565,566,567].

However, while the Web 4.0 and virtual worlds segment is still new, interview respondents expressed concerns about the possible dominance of a few platform and service providers that could limit access to the market for smaller players in the future. This is because the same structural characteristics that contribute to **power concentration** in today's digital markets could become even more pronounced with the advancement of virtual worlds and Web 4.0[568,569]. For example, the increased amount and types of data that could be collected in virtual worlds may not only amplify network effects, but also raise questions about user privacy and data security, as well as possible manipulation and exploitation. The emergence of a plethora of new services could enable novel ways of bundling services and increasing switching costs[570]. Some interviewees suggested that dominant players in the market could shape Web 4.0 technology landscapes to benefit their own interests, making it harder for new entrants and decentralised initiatives to compete. Moreover, the concentration of power in this technological evolution could place significant control over access and users' data, as well as influence over its governance, in the hands of a few large companies[571]. The complexity of Web 4.0 and virtual worlds also presents challenges in terms of assessing market dominance and ensuring fair competition[572].

These concerns are further substantiated by the growing number of **mergers and acquisitions** in the sector, as businesses seek to gain competitive advantage by acquiring new talent and technologies and expanding their market presence[573]. For example, Microsoft acquired gaming company Activision Blizzard in 2022 for USD 70 billion USD, in order to strengthen its virtual world capabilities[574]. Players in the Web 4.0 and virtual worlds space are frequently acquired by bigger companies, while new businesses can struggle to access funding and scale their businesses[575,576].

A related phenomenon is the **expansion of technology companies into other parts of the supply chain or into adjacent markets**. In recent years, for example, Big Tech firms have made significant investments in internet infrastructure (e.g. undersea cables, data centres, satellite communications, content delivery networks), and in semiconductors and AI, as well as virtual world

565 Grand View Research (2024). Metaverse market size, share & trends analysis report by product (software, services), by platform (desktop, mobile), by technology (VR & AR, mixed reality), by application (gaming, online shopping), by end-user, and segment forecasts, 2024-2030 (Report ID: GVR-4-68039-915-5). Available at: https://www.grandviewresearch.com/industry-analysis/metaverse-market-report

566 Emergen Research (2023, May). Metaverse market by component (hardware, software, services), by application (social events & trade shows, health surgery), by platform (desktop, mobile), by offering, by technology, by end-use, and by region forecast to 2032 (Report ID: ER_00840). Available at: https://www.emergenresearch.com/industry-report/metaverse-market

567 Council of Europe (2024). The metaverse and its impact on human rights, the rule of law, and democracy. Retrieved from https://rm.coe.int/the-metaverse-impact-on-and-its-impact-on-human-rights-the-rule-of-law/1680ae6bce

568 Vigkos, A., Bevacqua, D., Turturro, L., & Kuehl, S. (2022). The Virtual and Augmented Reality Industrial Coalition: Strategic paper.

569 PPMI & TNO (2025, forthcoming). Future of virtual worlds. Project 'Participatory Foresight for Next Generation Online Platforms'.

570 Online consultation (see Annex 2).

571 Council of Europe. (2024). The metaverse and its impact on human rights, the rule of law, and democracy. Retrieved from https://rm.coe.int/the-metaverse-impact-on-and-its-impact-on-human-rights-the-rule-of-law/1680ae6bce

572 Council of Europe (2024). The metaverse and its impact on human rights, the rule of law, and democracy. Retrieved from: https://rm.coe.int/the-metaverse-impact-on-and-its-impact-on-human-rights-the-rule-of-law/1680ae6bce

573 Grand View Research (2024). Metaverse market size, share & trends analysis report by product (software, services), by platform (desktop, mobile), by technology (VR & AR, mixed reality), by application (gaming, online shopping), by end-user, and segment forecasts, 2024-2030 (Report ID: GVR-4-68039-915-5). Available at: https://www.grandviewresearch.com/industry-analysis/metaverse-market-report

574 Microsoft (no date). Microsoft to acquire Activision Blizzard to bring the joy and community of gaming to everyone, across every device. Available at: https://news.microsoft.com/features/microsoft-to-acquire-activision-blizzard-to-bring-the-joy-and-community-of-gaming-to-everyone-across-every-device/

575 European Commission (2023). Staff Working Document: information, insights and market trends on web 4.0 and virtual worlds. Available at: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-information-insights-and-market-trends-web-40-and-virtual-worlds

576 Online consultation, see Annex 2.

technologies[577,578,579,580,581]. Google, Amazon and Microsoft control over two-thirds of the global cloud market, giving them unique access to computing capabilities and storage capacity[582,583]. These same companies are also making significant investments in the development of foundational AI models, such as Microsoft's investment in OpenAI[584]. US and Chinese Big Tech companies are well positioned to come out on top in the AI race[585]. Meanwhile, Meta, Apple, Sony and Microsoft have all invested in virtual reality hardware (e.g. headsets)[586,587]. As a result of their size, such businesses can build large ecosystems that span several markets and layers of the internet ecosystem.

Another consideration in the evolution of Web 4.0 and virtual worlds is the potential **creation of "walled gardens"** (see also Section 3.1). Most current virtual worlds operate in isolation, with limited interoperability[588,589]. Despite growing interest in XR interoperability and various ongoing initiatives, commonly recognised interoperability standards for the virtual world technology stack remain far from being achieved. The standardisation ecosystem for virtual worlds is highly fragmented and contains a number of competing open and proprietary initiatives[590,591]. Moreover, corporate actors have so far played a leading role in the development of standards for virtual worlds[592,593,594]. This issue extends beyond mere technical interoperability. Even when technical interoperability is ensured, providers may have strong incentives to pursue walled gardens in spite of the interests and needs of users[595]. Just because two entities speak the same protocol and can talk to each other, this doesn't mean that they *will*. Ensuring that they do so depends on economic incentives or otherwise – or, if the incentives turn out not to be aligned with user needs, regulation.

577 Baroudy, K., Dexeus, C., & Travasoni, A. (2023, 23 February). Delayering: An organizational overhaul for growing Europe's telcos. McKinsey & Company. Available at: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/delayering-an-organizational-overhaul-for-growing-europes-telcos
578 Abecassis, D. et al (2022). Economic impact of Google's submarine cable network in Latin America and the Caribbean. Analysys Mason. Available at: https://www.analysysmason.com/contentassets/45baaaa7225849e090c1d6853ee96d94/analysys-mason_economic-impact-of-google-submarine-cable-in-lac_english.pdf
579 BEREC (2023). The future of the electronic communications sector and its infrastructure. Available at: https://www.berec.europa.eu/system/files/2023-05/BoR%20%2823%29%20131c%20Annex%20to%20Section%201.pdf
580 Metz, C. (2021, 30 December). Everybody into the metaverse! Virtual reality beckons Big Tech. *New York Times*. Available at: https://www.nytimes.com/2021/12/30/technology/metaverse-virtual-reality-big-tech.html
581 Radu, R., & De Gregorio, G. (2023). The new era of internet governance: technical fragmentation and digital sovereignty entanglements.
582 Kowalski, K., Volpin, C., & Zombori, Z. (2024, September). Competition in generative AI and virtual worlds. Competition Policy Brief, Issue 3. European Commission. ISBN: 978-92-68-16497-6.
583 Synergy Research Group, European Cloud Provider Share of Local Market. Available at: https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-marketshare
584 Iyer, P. (2023). The AI supply chain: An emerging oligopoly? Tech Policy Press. Available at: https://www.techpolicy.press/the-ai-supply-chain-an-emerging-oligopoly/
585 World Bank (2024). Digital Progress and Trends Report 2023. World Bank. https://doi.org/10.1596/978-1-4648-2049-6.
586 Ladikas, M., Madeira, O., Hahn, J., Correa Pérez, M., Caplice, G., & Gerasymenko, A. (2024). D3.1: State-of-art in XR policy debates. In: M. Ladikas & M. Correa Pérez (Eds.), *The Equitable, Inclusive, and Human-Centered XR Project (XR4Human)* (Deliverable No. 3.1). Karlsruhe Institute of Technology (KIT). Grant Agreement No. 101070155.
587 Kowalski, K., Volpin, C., & Zombori, Z. (2024). Competition in Generative AI and Virtual Worlds. Competition Policy Brief, (3). European Commission. ISBN 978-92-68-16497-6, ISSN 2315-3113.
588 Yang, L., Ni, S.T., Wang, Y., Yu, A., Lee, J.A., & Hui, P. (2024). Interoperability of the Metaverse: A Digital Ecosystem Perspective Review. arXiv preprint arXiv:2403.05205.
589 Stephens, M. (2022). Metaverse and its governance: The IEEE global initiative on ethics of extended reality (XR) report. IEEE Standards Association.
590 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., & Vespe, M. (2023). Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU, Publications Office of the European Union, Luxembourg, doi:10.2760/51579, JRC133757.
591 Kowalski, K., Volpin, C., & Zombori, Z. (2024). Competition in Generative AI and Virtual Worlds. Competition Policy Brief, (3). European Commission. ISBN 978-92-68-16497-6, ISSN 2315-3113.
592 Yang, L. (2023). Recommendations for metaverse governance based on technical standards. *Humanities and Social Sciences Communications*, 10(1), 1-10.
593 McStay, A. (2023). The Metaverse: Surveillant Physics, Virtual Realist Governance, and the Missing Commons. *Philos. Technol.*, 36, 13 (2023). https://doi.org/10.1007/s13347-023-00613-y
594 McCarthy, K. (2022). Revitalising Global Internet Governance. Tony Blair Institute for Global Change. Available at: https://institute.global/insights/tech-and-digitalisation/revitalising-global-internet-governance
595 McStay, A. (2023). The Metaverse: Surveillant Physics, Virtual Realist Governance, and the Missing Commons. *Philos. Technol.*, 36, 13 (2023). https://doi.org/10.1007/s13347-023-00613-y

3.6.3. Global trade and data ownership

Virtual worlds and immersive technologies offer vast potential to contribute to global trade and unlock new economic opportunities. Virtual environments enable the creation of new revenue streams through the sale of digital assets and virtual goods. The applications of this technology can already be seen, with luxury brands such as Gucci and Ralph Lauren being present on platforms such as Roblox[596]. Similarly, companies can set up virtual storefronts and attend virtual exhibitions to showcase their products globally without any physical presence[597].

In parallel, immersive experiences offer unique ways to engage consumers. For example, one large British department store erected a "sensory reality pod" in the middle of its store to offer its customers the opportunity to escape and relax from real-life shopping using VR, while playing relaxing music and dispersing fragrances inside the pod. As commercial use cases for virtual worlds and XR technologies grow, the emergence of entirely new business models is expected. Some examples include virtual real estate, as well as commercial spaces on platforms such as Decentraland[598] and The Sandbox[599]. Similarly, digital identity and avatar-based services could create new markets for virtual and real-life goods and services.

Data is the main driver for economic opportunities to be unleashed by virtual world technologies. In the EU alone, it is estimated that data transfers will be worth at least EUR 3 trillion by 2030[600]. The trade in virtual products, experiences and artefacts relies on the seamless exchange of information across borders[601]. This necessitates a rethinking of traditional concepts of territoriality, especially when goods and services are traded across diverse legal jurisdictions[602].

Specific attention is needed for the trade of personally created assets. For example, the previously mentioned platform Roblox features a vast amount of user generated content. This content is owned by the user, but the platform has a large part of control over it. Clear and balanced agreements between users and platforms about the ownership, usage rights and trade of user generated content is needed.

With the economic and strategic value of digital markets on the rise, governments are paying closer attention to potential power imbalances in these emerging sectors. The intersection of data as an input for technological advances, together with an increasing focus on sovereignty, has become a critical factor in harnessing the economic benefits of virtual worlds, AI and related technologies. Regulatory measures such as data localisation laws, antitrust measures and intellectual property protections are often framed as safeguards for national security, information sovereignty and equitable access to emerging technologies[603],[604]. Yet these same policies can undermine the global and decentralised nature of the internet, reducing opportunities for cross-border innovation, limiting market dynamism, and increasing the burdens of compliance for smaller players[605]. For instance, data localisation mandates may require that data concerning a nation's citizens be stored and processed within its borders. Historically, these requirements were driven by concerns over data privacy and access rights,

596 Decentraland (no date). Marketplace Volume. Available at: https://decentraland.org/marketplace
597 Swarovski Virtual Shopping experience, https://www.swarovski.com/en_GB-AU/s-go-instore/New-Virtual-Shopping-Experience-/
598 Decentraland (no date). Decentraland. Available at: https://decentraland.org/
599 The Sandbox (no date). The Sandbox. Available at: https://www.sandbox.game/en/
600 Digital Europe (2021). Data flows and the Digital Decade. Available at: https://www.digitaleurope.org/resources/data-flows-and-the-digital-decade/
601 Stephens, M., Mathana, Morrow, M.J., McBride, K., Mangina, E. et al. (2024). The Emerging 'Metaverse' and Its Implications for International Business. *AIB Insights*, 24(2). https://doi.org/10.46697/001c.118572
602 Stephens, M., Mathana, Morrow, M.J., McBride, K., Mangina, E., et al. (2024). The Emerging 'Metaverse' and Its Implications for International Business. *AIB Insights*, 24(2). https://doi.org/10.46697/001c.118572
603 Daniel F Spulber. (2023). Antitrust and Innovation Competition, *Journal of Antitrust Enforcement*, Volume 11, Issue 1, March 2023, pp. 5–50, https://doi.org/10.1093/jaenfo/jnac013
604 Jones, E. (2023). Digital disruption: artificial intelligence and international trade policy, *Oxford Review of Economic Policy*, Volume 39, Issue 1, Spring 2023, pp. 70-84, https://doi.org/10.1093/oxrep/grac049
605 Brevini, B., Fubara-Manuel, I., Le Ludec, C., Jensen, J.L., Jimenez, A., & Bates, J. (2024). Critiques of data colonialism. In: J. Jarke & J. Bates (Eds.), *Dialogues in data power: Shifting response-abilities in a datafied world*. Bristol University Press. https://www.jstor.org/stable/jj.15617032.11

as well as concerns over the use of data use by the data brokerage industry, which generates billions in revenue from profiling, recommendations and advertising[606]. Yet, in today's technological race to develop AI systems, data localisation requirements are increasingly driven by sovereignty concerns. For instance, the recent introduction of the Chinese DeepSeek model triggered bans among several government agencies worldwide, citing concerns over national security[607].

Geopolitical competition further inhibits the potential for harnessing global economic opportunities, as tensions between major economies drive divergent approaches to data governance, threatening the seamless exchange of information and global trade[608]. According to some estimates, the number of data localisation measures in force around the world has more than doubled between 2017 and 2021, with 144 such measures enacted and dozens more under consideration[609].

Excessive data localisation restrictions can create barriers for international businesses, leading to increased operational costs and hindering access to innovative technologies[610]. These regulations impact various sectors, including telecommunications, healthcare and cloud computing, where data localisation can disrupt market efficiencies and hinder innovation[611]. The OECD points out that data localisation mandates can impede the adoption of advanced digital technologies and diminish overall competitiveness in global markets[612].

In this context, global multistakeholder cooperation is important to ensure data flows and unlock the benefits of new technologies. International instruments such as the United Nations Convention against Cybercrime[613] and the OECD Privacy guidelines[614] are examples of efforts to coordinate regulatory approaches globally. Meanwhile, concepts such as "data equity" highlight the human dimension of data-driven systems, which is an increasingly pressing concern as digital technologies deepen their influence on every aspect of society[615]. Multistakeholder forums such as the IGF have devoted significant attention to data localisation and the critical role of secure data exchange, reflecting a growing awareness that effective governance must strike a balance between sovereignty, innovation and equitable access to the economic benefits of emerging technologies.[616,617].

3.6.4. Business adoption

The most common areas in which businesses are currently adopting XR technologies are production (e.g. assistant assembly and maintenance, training, manufacturing), R&D, and marketing and

606 IEEE (2024). The metaverse and its impact on human rights, the rule of law and democracy. Available at: https://rm.coe.int/the-metaverse-and-its-impact-on-human-rights-the-rule-of-law-and-democ/1680b178b0

607 Euronews (2025). DeepSeek: Which countries have restricted the Chinese AI company or are questioning it? Available at: https://www.euronews.com/next/2025/02/03/deepseek-which-countries-have-restricted-the-chinese-ai-company-or-are-questioning-it

608 White & Case (2024). The Rise of Artificial Intelligence, Big Data, and the Next Generation of International Rules Governing Cross-Border Data Flows and Digital Trade. Available at: https://www.whitecase.com/insight-our-thinking/rise-artificial-intelligence-big-data-next-generation-international-rules

609 White & Case (2024). *The Rise of Artificial Intelligence, Big Data, and the Next Generation of International Rules Governing Cross-Border Data Flows and Digital Trade.* Available at: https://www.whitecase.com/insight-our-thinking/rise-artificial-intelligence-big-data-next-generation-international-rules

610 ICLG (2024). Data Protection Laws and Regulations USA 2024-2025. Available at: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

611 Frontier Economics (2022) The extent and impact of data localisation. Available at: https://assets.publishing.service.gov.uk/media/63a1a2e88fa8f539198d9bb5/Frontier_Economics_-_data_localisation_report_-_June_2022.pdf

612 Organisation for Economic Co-operation and Development (OECD) (2020). *Data in the Digital Age: Cross-Border Data Flows, Digital Transformation and Innovation*.OECD Publishing, Paris.

613 UN General Assembly (2024). Countering the use of information and communications technologies for criminal purposes. Report of the Third Committee. Available at: https://docs.un.org/en/A/79/460

614 OECD legal instruments (2013). Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

615 WEF (2024). Advancing Data Equity: An Action-Oriented Framework. White Paper. Available at: https://www3.weforum.org/docs/WEF_Advancing_Data_Equity_2024.pdf

616 IGF (2024). IGF 2024 WS #180: Protecting Internet data flows in trade policy initiatives. Available at: https://review.intgovforum.org/en/content/igf-2024-ws-180-protecting-internet-data-flows-in-trade-policy-initiatives

617 IGF (2024). IGF 2024 WS #102: Harmonising approaches for data free flow with trust. Available at: https://whm.intgovforum.org/en/content/igf-2024-ws-102-harmonising-approaches-for-data-free-flow-with-trust

design[618,619]. However, in the long term, Web 4.0 technologies and virtual worlds have the potential to transform processes, business models and whole sectors of the economy. Experts predict that future applications will have significant impacts on sectors such as financial services, manufacturing, agriculture, health care and others (see figure below) through technologies such as digital twins, spatial computing, AI and blockchain. Some of the key benefits businesses cite for the adoption of Web 4.0 and virtual world technologies include higher efficiency and process optimisation, cost reduction, better consumer engagement, and improved employee performance and brand awareness[620,621].

Figure 11. Examples of Web 4.0 opportunities across sectors

Education, media and cultural experiences

- Immersive learning environments Virtual classrooms and skill development simulations
- Social virtual worlds, interactive cultural events

Production processes

- Collaborative product design, prototyping in virtual environments
- Real-time monitoring of manufacturing processes, supply chains, and logistics
- Integrated IoT, AI, and blockchain solutions for quality assurance and efficiency

Commerce, retail and financial services

- Virtual marketplaces and personalized shopping experiences
- Secure and transparent financial transactions
- Innovative marketing, product presentations, and targeted campaigns

Health and care services

- Immersive and virtual treatment, diagnostics, rehabilitation etc.
- Health care professional training and simulations (e.g. in surgery)
- Personalised health care

Infrastructure, smart cities, environmental management

- Digital twins for urban planning, traffic management, and energy optimisation
- Environmental monitoring and sustainable resource usage
- Smart grids, renewable energy integration

Public services, safety and governance

- Simulations for crisis management, disaster preparedness, and emergency response
- Predictive policing, secure public infrastructure
- Data-driven policymaking

618 European Commission (2023). Staff Working Document: information, insights and market trends on web 4.0 and virtual worlds. Available at: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-information-insights-and-market-trends-web-40-and-virtual-worlds

619 Vigkos, A., Bevacqua, D., Turturro, L., & Kuehl, S. (2022). The Virtual and Augmented Reality Industrial Coalition: Strategic paper.

620 European Commission (2023). Staff Working Document: information, insights and market trends on web 4.0 and virtual worlds. Available at: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-information-insights-and-market-trends-web-40-and-virtual-worlds

621 Vigkos, A., Bevacqua, D., Turturro, L., & Kuehl, S. (2022). The Virtual and Augmented Reality Industrial Coalition: Strategic paper.

Source: authors' own elaboration, based on Kind et al. (2019)[622]; Hupont Torres et al. (2023)[623]; Briggs et al. (2021) [624]; He (2019)[625]; WEF (2023)[626]; Deloitte (2020)[627]; European Commission (2023)[628]; and the results of the stakeholder consultation (See Annex 2, 3).

Platform, service and hardware providers, as well as early adopters in industries such as the media and entertainment, retail and finance are likely to benefit significantly from Web 4.0 and virtual worlds[629,630,631]. In a survey conducted by Accenture[632], 92 % of executives planned to leverage spatial computing to achieve a competitive advantage for their organisation. Another Accenture survey from 2023 showed that immersive technologies are already inspiring the long-term strategies and visions of companies in various sectors, including automotive, manufacturing, health care, energy and public service[633]. Moreover, according to McKinsey, 95 % of executives stated that they "expect virtual worlds to have a positive impact on their industry within five to ten years" [634].

The integration between physical and digital world facilitated by Web 4.0 is likely to result in fundamental shifts in product experiences and business operations[635]. For instance, in a stakeholder survey conducted for the Virtual and Augmented Reality Industrial Coalition Strategic paper, the majority of respondents stated that innovation in XR has the potential to disrupt the existing market, or will create gradual and continuous improvements in products and services[636].

As such, Web 4.0 and virtual worlds could disrupt **existing business models** in various sectors, especially in traditional industries. Insufficient access to virtual worlds and Web 4.0 skills and digital infrastructures could disadvantage SMEs, businesses operating in areas with connectivity barriers and companies in the least digitalised industries[637]. Uneven adoption due to geographical location, business size or sector could deepen existing the digital divides that affect regional competitiveness and development (see subsection 3.7.3).

Several factors affect the ability of businesses, especially SMEs, to adopt Web 4.0 and virtual worlds technologies (see figure below). Many of these are not necessarily unique to Web 4.0 and virtual worlds, and overlap with the challenges or opportunities businesses face with respect to the adoption of any emerging technology. Nonetheless, Web 4.0 and virtual worlds present some unique

[622] Kind, S., Ferdinand, J.P., Jetzke, T., Richter, S., & Weide, S. (2019). Virtual und Augmented Reality: Status quo, Herausforderungen und zukünftige Entwicklungen. TA-Vorstudie.

[623] Hupont Torres, I., Charisi, V., De Prato, G., Pogorzelska, K., Schade, S., Kotsev, A. … & Vespe, M. (2023). Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/51579

[624] Briggs, R., Mariani, J., Dul, J., Kishnani, P. K. (2021). Exploring the Industrial Metaverse. Deloitte. https://www2.deloitte.com/us/en/insights/industry/public-sector/augmented-virtual-reality-government-services.html

[625] He, J. (2019). Application of virtual reality technology in industrial design. Journal of Physics: Conference Series. https://www.researchgate.net/publication/337596262_Application_of_virtual_reality_technology_in_industrial_design/citation/download

[626] WEF (2023). Exploring the industrial metaverse: A roadmap to the future. Briefing Paper. World Economic Forum, https://www3.weforum.org/docs/WEF_Exploring_the_Industrial_Metaverse_2023.pdf

[627] Deloitte Insights (2020). A brave new world with virtual worlds. https://www2.deloitte.com/us/en/insights/topics/emerging-technologies/virtual-world-for-business.html

[628] European Commission (2023). Staff Working Document: information, insights and market trends on web 4.0 and virtual worlds. Available at: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-information-insights-and-market-trends-web-40-and-virtual-worlds

[629] McKinsey & Company (2020). What is the metaverse? Available at: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-the-metaverse

[630] Ladikas, M., Madeira, O., Hahn, J., Correa Pérez, M., Caplice, G., & Gerasymenko, A. (2024). D3.1: State-of-art in XR policy debates. In: M. Ladikas & M. Correa Pérez (Eds.), *The Equitable, Inclusive, and Human-Centered XR Project (XR4Human)* (Deliverable No. 3.1). Karlsruhe Institute of Technology (KIT). Grant Agreement No. 101070155.

[631] PPMI & TNO (2025, forthcoming). Future of virtual worlds. Project 'Participatory Foresight for Next Generation Online Platforms'.

[632] Accenture (2024). Technology Vision 2024, Accenture, 9 January 2024. Available at: https://www.accenture.com/us-en/insights/technology/technology-trends-2024

[633] Accenture (2023). Technology Vision 2023 When Atoms Meet Bits, Accenture, 29 March 2023. Available at: https://www.accenture.com/us-en/insights/technology/technology-trends-2023

[634] McKinsey & Company (2022). Value creation in the Metaverse: The real business of the virtual world; the respondents were executives from 448 companies representing Europe, Asia and the United States.

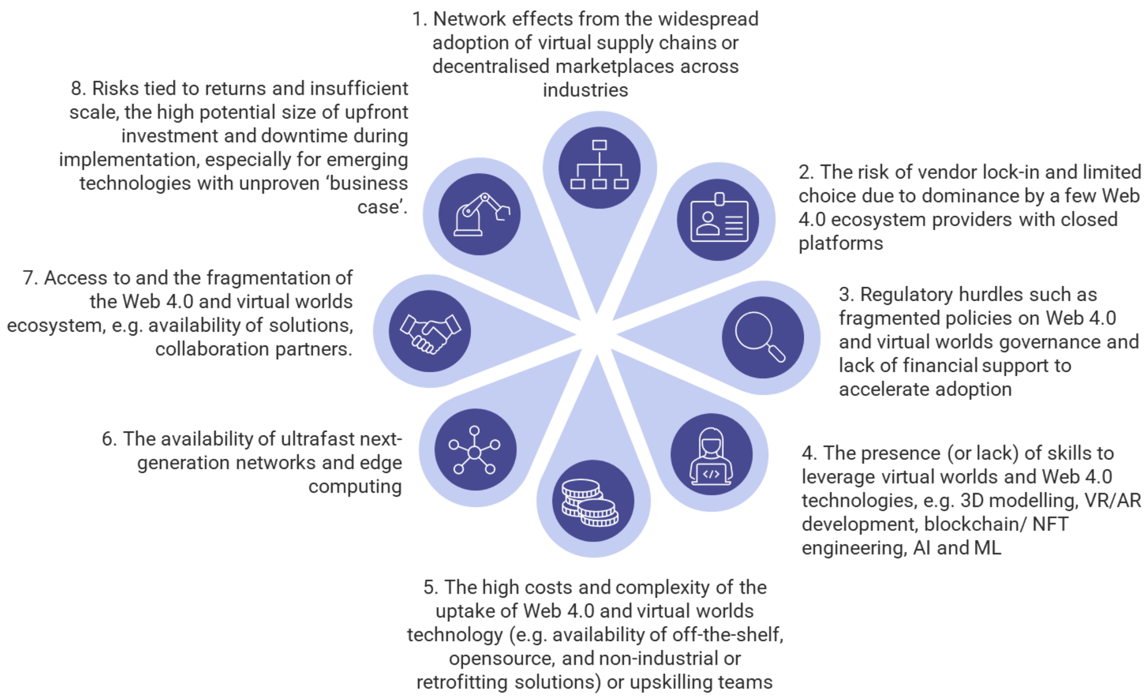
[635] European Commission (2023). Staff Working Document: information, insights and market trends on web 4.0 and virtual worlds. Available at: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-information-insights-and-market-trends-web-40-and-virtual-worlds

[636] Vigkos, A., Bevacqua, D., Turturro, L., & Kuehl, S. (2022). The Virtual and Augmented Reality Industrial Coalition: Strategic paper.

[637] PPMI & TNO (2025, forthcoming). Future of virtual worlds. Project 'Participatory Foresight for Next Generation Online Platforms'.

considerations – for example, in terms of the skills and expertise needed, the importance of network effects in supply chains, and access to next-generation digital infrastructure.

Figure 12. Factors affecting the adoption of Web 4.0 and virtual worlds by businesses



Source: European Commission (2023)[638]; PPMI & TNO (2025, forthcoming)[639]; Barcevičius et al. (2022)[640]; McFarlan et al. (2022)[641]; McFarlan et al. (2019)[642]; European Commission (2023)[643]; VR/AR Industrial Coalition (2022)[644]; Elhusseiny & Crispim (2022)[645].

Virtual and immersive environments, as well as the technologies that enable them, raise questions regarding new modes of work. For example, in the future, virtual reality experiences are likely to adopt subscription-based models, whereby users pay for ongoing access while also providing extensive personal data. Such models enable companies to refine and personalise experiences, driving continuous engagement and revenue. Consequently, ownership of this user-generated data and the resulting "value imbalance" – in which consumers repeatedly pay and share information, yet have limited control over this information – represents a growing ethical and regulatory concern[646].

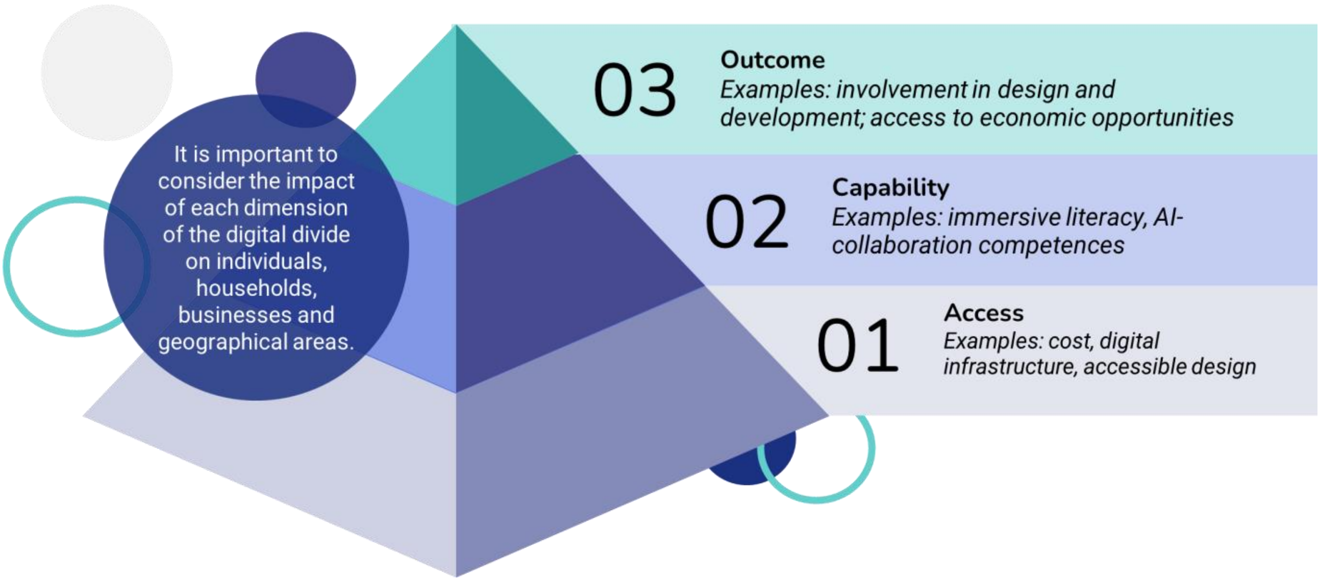
638 European Commission (2023). Staff Working Document: information, insights and market trends on web 4.0 and virtual worlds. Available at: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-information-insights-and-market-trends-web-40-and-virtual-worlds
639 PPMI & TNO (2025, forthcoming). Future of virtual worlds. Project 'Participatory Foresight for Next Generation Online Platforms'.
640 Barcevičius, E., Gabaliņa, R., Kudzmanaitė, B., & Yevdokymova, O. (2022). Smart industrial remoting: Remote working in non-digitalised industries (Best Practice Collection report D.6). European Commission, Directorate-General for Communications Networks, Content and Technology.
641 McFarlane, D., Ratchev, S., de Silva, L., Hawkridge, G., Schönfuβ, B., & Angulo, G. T. (2022). Digitalisation for SME Manufacturers: A Framework and a Low-Cost Approach. *IFAC-PapersOnLine*, 55(2), 414-419. Available at: https://doi.org/10.1016/j.ifacol.2022.04.229
642 McFarlane, D., Ratchev, S., Thorne, A., Parlikad, A.K., Silva, L. D., Schönfuß, B., ... & Tlegenov, Y. (2019). Digital manufacturing on a shoestring: Low cost digital solutions for SMEs. In: *International Workshop on Service Orientation in Holonic and Multi-Agent Manufacturing*. Springer, Cham, pp. 40-51.
643 European Commission: Directorate-General for Communications Networks, Content and Technology (2023), Zero-distance XR applications and services – Final report, Publications Office of the European Union, 2024, https://data.europa.eu/doi/10.2759/0405)
644 Vigkos, A., Bevacqua, D., Turturro, L., & Kuehl, S. (2022). The Virtual and Augmented Reality Industrial Coalition: Strategic paper.
645 Elhusseiny, H.M., & Crispim, J. (2022). SMEs, Barriers and Opportunities on adopting Industry 4.0: A Review. Procedia Computer Science, 196, 864-871.
646 IEEE (2022) The IEEE Global Initiative on Ethics of Extended Reality (XR) report – Business, finance and economics. Available at: https://standards.ieee.org/wp-content/uploads/2022/04/XR_Business_Finance_Economics.pdf

3.7. Accessibility and digital divides

The **digital divide** refers to the gap between those individuals, communities or regions that have access to and are able to effectively use digital technologies, and those that do not. WSIS Action Line 2 recognises the importance of information and communication infrastructure as an essential foundation for the information society[647]. The digital divide is typically conceptualised as manifesting itself in three dimensions: the access divide, the capability divide, and the outcome divide[648]. The access divide describes differences in access to digital devices, connectivity and other technological infrastructure, often influenced by factors such as geography, socio-economic status or gender. The capability divide describes differences in digital skills, technological literacy and the ability to use digital tools effectively. The outcome divide usually refers to differences in the benefits derived from digital technologies, such as economic opportunities, educational progress and access to information, which can lead to unequal societal or personal development. When assessing these divides, it is important to consider their effects not just on individuals, but also on households, businesses and geographic areas. The sections that follow describe each of these areas in further detail.

Such divides are relevant to the environment of Web 4.0 and virtual worlds, but they manifest themselves differently. For example, where traditional digital divides would typically point to a lack of basic connectivity, Web 4.0 requires not only access to the internet but specifically access to high upload speeds and low-latency connectivity. By 2035, we can expect most of the world population to have access to internet-connected devices[649]. However, Web 4.0 and virtual worlds will also require access to specialised hardware and software, such as head-mounted displays and haptic devices.

Figure 13. Dimensions of the digital divide



Source: dimensions - Wei et al. (2011)[650]; examples – authors' own elaboration.

[647] ITU (2003). WSIS Plan of Action. Available at: https://www.itu.int/net/wsis/docs/geneva/official/poa.html

[648] Wei, K.K., Teo, H.-H., Chan, H.C., & Tan, B.C.Y. (2011). Conceptualizing and testing a social cognitive model of the digital divide. *Information Systems Research*, 22(1) March, 170–187.

[649] Statista (no date). Smartphones – statistics & facts. Available at: https://www.statista.com/topics/840/smartphones/

[650] Wei, K.K., Teo, H.-H., Chan, H.C., & Tan, B.C.Y. (2011). Conceptualizing and testing a social cognitive model of the digital divide. *Information Systems Research*, 22(1) March, 170-187.

3.7.1. Access divide

In terms of the **access divide**, several elements are important to consider. These include access to digital infrastructure; the affordability of hardware, software and connectivity; and accessible design. The WSIS states that *"the ability for all to access and contribute information, ideas and knowledge is essential in an inclusive Information Society"*[651]. Furthermore, the Global Digital Compact[652] contains a commitment to connect all persons to the internet.

In terms of **digital infrastructure**, 2.6 million people in the world currently still do not have access to the internet[653]. In fact, in recent years, internet speed and data gaps have grown between high-income and low- and medium-income countries[654]. Emerging virtual world and Web 4.0 technologies will need high upload speeds and ultra-low latency, thus requiring the widespread deployment of 5G/6G networks[655]. For example, Telefonica estimates that virtual worlds could require significantly more processing capacity, and could generate up to 20 more traffic than current technologies[656] (although some estimates suggest that avatar traffic would not create an increase relative to video traffic[657]).

Two of the issues most frequently mentioned by interviewees as being critical to enabling immersive experiences were bandwidth and latency. Most stakeholders highlighted how significant the issue of ensuring connectivity was to the widespread adoption of Web 4.0 technologies, especially from a global perspective. Existing mobile infrastructure is insufficient to meet the advanced needs of Web 4.0 and virtual worlds, and thus significant further investment will be needed to support their uptake. According to the ITU, closing the connectivity gap will cost an estimated USD 1.6 trillion[658]. While the proportion of mobile connections using 5G is forecasted to grow from 18 % in 2023 to 56 % in 2030, significant disparities between global regions are likely to remain[659].

651 WSIS (2003). Declaration of Principles. Building the Information Society: a global challenge in the new Millennium. Available at: https://www.itu.int/net/wsis/docs/geneva/official/dop.html

652 UN (2024). Global Digital Compact. Available at: https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf

653 ITU (2023). Global offline population steadily declines to 2.6 billion people in 2023. Available at: https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use/

654 World Bank (2024). Digital progress and trends report 2023. Washington, DC: World Bank. https://doi.org/10.1596/978-1-4648-2049-6

655 Arkenberg, C., & Arbanas, J. (2023). What does it take to run a metaverse? Deloitte Insights. Available at: https://www2.deloitte.com/us/en/insights/industry/technology/metaverse-infrastructure.html

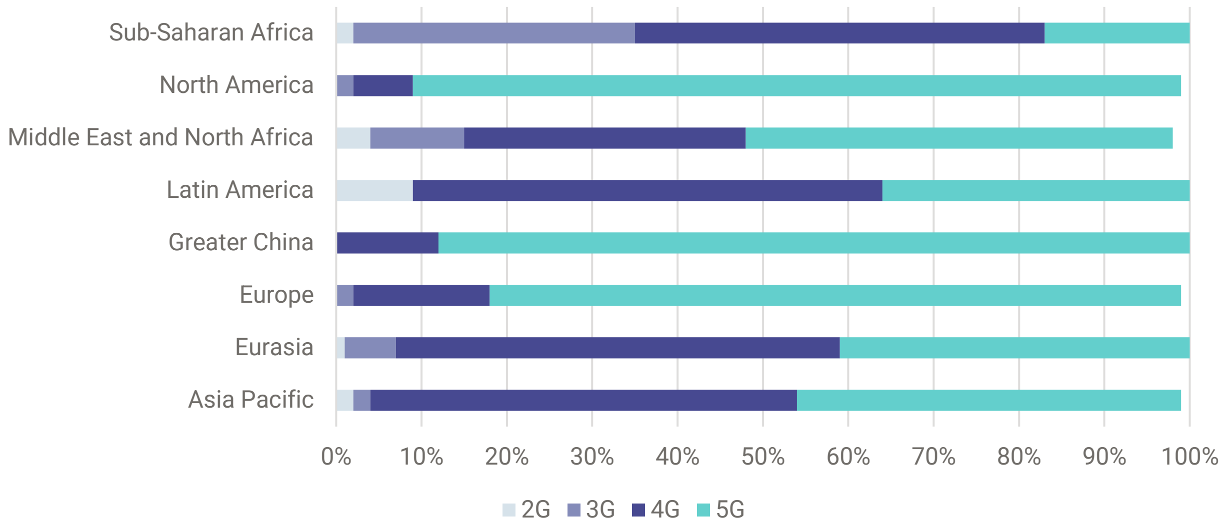
656 Telefonica (no date). Metaverse Ready Networks. Available at: https://www.telefonica.com/en/about-us/public-policy-and-regulation/public-positioning/metaverse-ready-networks/

657 Kolkman, O., Robachevsky, A., Gahnberg, C., & Badran, H. (2022, August). Evolution of the edge, what about the internet?. In: *Proceedings of the ACM SIGCOMM Workshop on Future of Internet Routing & Addressing*, pp. 1-5.

658 ITU (2025). Digital Infrastructure Investment Initiative Closing the digital infrastructure investment gap by 2030. Available at: https://www.itu.int/hub/publication/s-dii-diii-whitepaper-2025/

659 GMSA (2024). The Mobile Economy 2024. Available at: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/02/260224-The-Mobile-Economy-2024.pdf

Figure 14. Forecasted technology mix in 2030 – 2G, 3G, 4G and 5G, by region



Source: GSMA (2024)[660]; note: due to rounding errors, figures for some individual regions may not add up to 100 %.

Virtual worlds and Web 4.0 will also require specialised devices and software, as well as high upload speeds and low-latency connectivity. While the currently **high cost** of immersive hardware is likely to decrease over time, the cost of access is likely to remain a barrier[661,662]. In addition, the rapid evolution of these technologies may require the frequent updating and replacement of devices and software to enable engagement with virtual worlds, further increasing the associated costs.

For comparison, today's mobile phone penetration can only be considered universal (i.e. >95 %) in high-income countries, while in low-income economies, only 56 % of people over the age of 10 years own mobile phones[663]. In South Asia and sub-Saharan Africa, the cost of a smartphone exceeds 40 % of the average monthly income. In Africa, the cost of mobile data is more than three times the global average[664]. Thus, Web 4.0 and virtual worlds – which typically involve real-time interactions and require high bandwidth and specialised devices – present particular challenges in terms of accessibility. Maintaining the opportunity to access relevant platforms and services using low bandwidth, 2D and low-cost devices and with some offline functionality could become highly relevant considerations in ensuring accessibility in a Web 4.0 environment.

Another area that is important to consider in terms of access is **accessible and inclusive design**. Currently available XR technologies are comfortable to wear only for around half of the population [665]. For example, many current VR and AR devices are not designed for use by children or older adults, and

660 GMSA (2024). The Mobile Economy 2024. Available at: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/02/260224-The-Mobile-Economy-2024.pdf

661 Jensen, M.B. (2022). The accessibility and affordability of the metaverse in education right now. Forbes. Available at: https://www.forbes.com/councils/forbestechcouncil/2022/08/24/the-accessibility-and-affordability-of-the-metaverse-in-education-right-now/

662 Internet Society (2022). Paths to our Digital Future – Area of Impact: Digital Divides. Available at: https://www.internetsociety.org/wp-content/uploads/2022/12/Paths-to-our-Digital-Future-Area-of-Impact-Digital-Divides.pdf

663 ITU (2023). Worldwide, four out of five people own a mobile phone. Available at: https://www.itu.int/itu-d/reports/statistics/2024/11/10/ff24-mobile-phone-ownership/

664 ITU (2022). Measuring digital development: Facts and Figures 2022. ITU, Geneva.

665 Pladere, T., Svarverud, E., Krumina, G., Gilson, S.J., & Baraas, R.C. (2022). Inclusivity in stereoscopic XR: Human vision first. *Frontiers in Virtual Reality*, 3. https://www.frontiersin.org/articles/10.3389/frvir.2022.1006021

are not suitable for users with vision, vestibular or cognitive impairments [666,667,668]. Women are also much more likely to experience cybersickness compared with men. In addition, the sensory overload associated with immersive environments can be particularly overwhelming for individuals with autism spectrum disorders or sensory processing sensitivities[669]. There is also a need to consider the compatibility of new devices with assistive tools and technologies, we well as their suitability for persons with disabilities who do not use any assistive technologies[670]. Existing accessibility formats will also require rethinking in light of the adoption of Web 4.0 technologies, to make them accessible to diverse users. Examples include the inclusion of captions or subtitles to account for visual or hearing impairments[671]. Language exclusion should also be addressed, such as with the use of real-time AI-powered translation technologies[672].

3.7.2. Capability divide

The capability divide describes differences in digital skills, technological literacy and the ability to use digital tools effectively. WSIS Action Line 4 stresses that "everyone should have the necessary skills to benefit fully from the Information Society"[673]. With the evolution towards Web 4.0 and virtual worlds, these gaps could widen, as more immersive and intuitive technologies demand new forms of expertise. Although these developments present new opportunities, they can also exacerbate exclusion for those who are already behind in terms of basic digital skills.

Virtual worlds may still present **significant challenges** for individuals or communities who have historically been digitally excluded, even if the required infrastructure and policies are in place[674]. The digital skills gap remains far from being bridged, with populations in the Global South and low-income countries disproportionately lacking basic digital skills. For example, in Chad and the Central African Republic, only 1.6 % and 2.4 % of adults, respectively, have copied or moved a folder. In many other countries across Africa, Central America and Asia, this percentage does not exceed 40 %[675].

As technology evolves towards more intuitive, immersive formats, many existing digital competencies in relation to 2D devices risk becoming **outdated**. To take full advantage of emerging environments, users will need to handle devices that enable **immersive experiences** (such as headsets or haptic gloves) and become adept at working alongside AI, while also sharpening their ability to detect sophisticated misinformation (see subsection 3.4.13.4.1)[676]. This indicates the potential for an ever-widening gap in relation to Web 4.0, which would require new and advanced digital skills.

With the development of Web 4.0, a widening digital skills gap could have **significant consequences for employment, privacy and security**. First, the skills needed to use virtual worlds-related technologies

---

666 Zallio, M., & Clarkson, P.J. (2022). Designing the metaverse: A study on inclusion, diversity, equity, accessibility and safety for digital immersive environments. *Telematics and Informatics*, *75*, 101909.
667 World Economic Forum (2023). *Social implications of the metaverse*. In collaboration with Accenture. Available at: https://www3.weforum.org/docs/WEF_Social_Implications_of_the_Metaverse%20_2023.pdf
668 Lukava, T., Morgado Ramirez, D.Z., & Barbareschi, G. (2022). Two sides of the same coin: accessibility practices and neurodivergent users' experience of extended reality. *Journal of Enabling Technologies*, 16(2), 75-90.
669 World Economic Forum (2023). *Social implications of the metaverse*. In collaboration with Accenture. Available at: https://www3.weforum.org/docs/WEF_Social_Implications_of_the_Metaverse%20_2023.pdf
670 Othman, A., Chemnad, K., Hassanien, A.E., Tlili, A., Zhang, C.Y., Al-Thani, D., & Altınay, Z. (2024). Accessible Metaverse: A Theoretical Framework for Accessibility and Inclusion in the Metaverse. *Multimodal Technologies and Interaction*, 8(3), 21.
671 Fox, D., Thornton, I.G. (2022). The IEEE Global Initiative on Ethics of Extended Reality (XR) Report -- Extended Reality (XR) Ethics and Diversity, Inclusion, and Accessibility. The IEEE Global Initiative on Ethics of Extended Reality (XR) Report--Extended Reality (XR) Ethics and Diversity, Inclusion, and Accessibility.
672 Council of Europe (2024). *The metaverse and its impact* on human rights, the rule of law, and democracy. Retrieved from: https://rm.coe.int/the-metaverse-and-its-impact-on-human-rights-the-rule-of-law-and-democ/1680b178b0
673 ITU (2003). WSIS Plan of Action. Available at: https://www.itu.int/net/wsis/docs/geneva/official/poa.html
674 World Economic Forum (2023). *Social implications of the metaverse*. https://www3.weforum.org/docs/WEF_Social_Implications_of_the_Metaverse%20_2023.pdf
675 United Nations Industrial Development Organization (2023). Digital skills in the Global South: Gaps, needs and progress. Inclusive and Sustainable Industrial Development (IAP).Digital skills in the Global South: Gaps, needs, and progress. https://iap.unido.org/articles/digital-skills-global-south-gaps-needs-and-progress
676 World Economic Forum (2023). *Social implications of the metaverse*. https://www3.weforum.org/docs/WEF_Social_Implications_of_the_Metaverse%20_2023.pdf

may become standard requirements for many **jobs**, thus leaving candidates without such competencies at a disadvantage[677]. Second, individuals and populations with limited **cybersecurity** skills face a disproportionately high risk from cyberthreats, including data breaches and online scams[678]. Furthermore, **privacy** concerns are also magnified in immersive environments. Many people fail to recognise that even subtle physical responses, such as involuntary body movements, can reveal sensitive private information, including emotional and health-related data[679]. In addition, while technologies such as AI and generative AI, as well as quantum computing, drive progress in knowledge-based societies, they also introduce significant risks that are amplified by a lack of adequate digital skills. These advances increase the likelihood of **misinformation**, propaganda and advanced cyber attacks, creating serious security vulnerabilities[680].

Beyond basic usage skills, there is a rising need for more **advanced skills**[681] such as 3D modelling and design, VR/AR development, programming, proficiency with low-code or no-code world-building solutions, blockchain and NFT engineering, data analytics, UI/UX design and cybersecurity. However, the technology sector already faces widespread shortages in skilled labour[682]. If these gaps remain unaddressed, they may not only hamper the development of Web 4.0 and virtual worlds, but could also hinder economic growth and regional competitiveness.

Despite these challenges, immersive technologies could **boost digital inclusion** by offering more engaging and effective learning environments. Virtual training tools allow learners to practise practical tasks before moving on to real-life scenarios[683]. For example, surgeons can train using virtual reality before performing operations on real patients, while pilots, military personnel, and other professionals in high-risk environments can train for critical scenarios without being exposed to actual risk[684]. These same platforms can also be adapted to develop soft skills, expanding their relevance beyond purely technical roles[685]. By placing learners in rich, interactive settings, immersive education can fuel motivation and curiosity, especially in **low-income or remote areas** where formal training options may be limited.[686] Over time, these methods could help to narrow the digital skills gap by providing broader access to high-quality, practical learning experiences that resonate with diverse populations.

A entirely virtual environment could present distinctive educational opportunities through immersive learning. Yet, without the widespread provision of suitable hardware and specialised software, the existing educational divide could unintentionally grow. This risk is especially pronounced for low-

[677] Egliston, B., & Carter, M. (2024). 'The metaverse and how we'll build it': The political economy of Meta's Reality Labs. *New Media & Society*, *26*(8), 4336-4360.

[678] Internet Society (2022). Paths to our Digital Future – Area of Impact: Digital Divides. Available at: https://www.internetsociety.org/wp-content/uploads/2022/12/Paths-to-our-Digital-Future-Area-of-Impact-Digital-Divides.pdf

[679] Heller, B. (2021). Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law, *23 Vanderbilt Journal of Entertainment and Technology Law*, 1 (2021). Available at: https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss1/1

[680] IGF 2024 DC-PAL & DC-Digital Inclusion Transformative digital inclusion: Building a gender-responsive and inclusive framework for the underserved.

[681] The skills required to design, develop and innovate using these technologies.

[682] European Commission (2023). Staff Working Document: information, insights and market trends on web 4.0 and virtual worlds. Available at: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-information-insights-and-market-trends-web-40-and-virtual-worlds ; VR/AR Industrial Coalition – Strategic paper, Publications Office of the European Union, 2022.

[683] 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., & Vespe, M. (2023). Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU, Publications Office of the European Union, Luxembourg, doi:10.2760/51579, JRC133757; PwC. (2020). PwC's study into the effectiveness of VR for soft skills training. PwC. Available at: https://www.pwc.co.uk/issues/emerging-technologies/metaverse-technologies/study-into-vrtraining-effectiveness.html

[684] PwC (2020). Total recall: How virtual reality is transforming training. https://www.pwc.co.uk/issues/technology/immersive-technologies/total-recall-how-virtual-reality-is-transforming-training.html; Forbes (2020). Training For Dangerous Jobs With Virtual Reality. https://www.forbes.com/councils/theyec/2020/07/28/training-for-dangerous-jobs-with-virtual-reality/

[685] PwC (2020). PwC's study into the effectiveness of VR for soft skills training. Available at: https://www.pwc.com/us/en/services/consulting/technology/emerging-technology/assets/pwc-understanding-the-effectiveness-of-soft-skills-training-in-the-enterprise-a-study.pdf

[686] World Economic Forum (2023). Social implications of the metaverse. Available at: https://www3.weforum.org/docs/WEF_Social_Implications_of_the_Metaverse%20_2023.pdf

income groups and people with specific needs, who might lack access to assistive technology or accessibility solutions[687].

In conclusion, the potential of immersive digital experiences highlights existing disparities in the skills needed to participate in virtual worlds. While new technologies can enrich learning, boost economic prospects and improve engagement, they can also deepen inequalities where infrastructure, expertise or supportive tools are lacking. Gaps in digital proficiency, shortages of talent, sophisticated cyber threats and concerns about privacy can create an environment in which some individuals, businesses and regions stand to benefit considerably, while others risk being left behind.

3.7.3. Outcome divide

The outcome divide refers to disparities in the benefits that individuals, businesses and regions gain from Web 4.0 and virtual worlds. Even where infrastructure and skills are in place, not everyone may be able to translate these opportunities into tangible advantages.

For individuals, the evolution towards Web 4.0 has the potential to exacerbate the existing **gender gap**. Currently, women account for only 29 % of the IT services workforce[688]. Initial research in relation to Web 4.0 indicates that while women are increasingly active in virtual worlds as both consumers and leaders, they tend to receive less financial backing for virtual worlds-related projects and are disproportionately underrepresented in leadership positions[689]. The lack of gender equality in development of virtual realities may have negative implications for gender equality in the future internet.

There is also a risk of widening gaps in **access to employment**. Recent findings show that for clerical functions (e.g. typists, data entry), over 50 % of tasks are subject to automation, while roles in agriculture, crafts, or other basic occupations show a susceptibility of automation less than 10 %. Conversely, professional service positions that require complex thinking tend to offer have high possibilities for augmentation. On a broader scale, high-income nations have the largest shares of jobs vulnerable to automation, although low- and middle-income nations also exhibit a similarly large share of jobs that could be enhanced by technology[690]. The rising influence of AI in virtual worlds could diminish the perceived value of certain skill sets, leaving many workers vulnerable[691].

For **businesses**, smaller players may face significant hurdles in the evolving Web 4.0 landscape. While a number of innovative SMEs and start-ups are contributing to developments in this domain, a large share of progress remains concentrated among a few dominant technology companies (see subsection 3.6.23.6.2)[692]. Smaller businesses often become targets for acquisition by bigger firms, curtailing their ability to obtain investment and limiting their scope for scaling up[693].

When it comes to **the geographical divide, a** shortage of talent in XR and related technologies could hold back the development and **uptake of virtual worlds in certain regions**, weakening their

---

687 Council of Europe (2024). *The metaverse and its impact* on human rights, the rule of law, and democracy. https://rm.coe.int/the-metaverse-and-its-impact-on-human-rights-the-rule-of-law-and-democ/1680b178b0

688 World Bank (2024). Digital progress and trends report 2023. Washington, DC: World Bank. https://doi.org/10.1596/978-1-4648-2049-6

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

690 World Bank (2024). Digital progress and trends report 2023. https://openknowledge.worldbank.org/server/api/core/bitstreams/95fe55e9-f110-4ba8-933f-e65572e05395/content

691 Council of Europe (2024). *The metaverse and its impact* on human rights, the rule of law, and democracy. Retrieved from: https://rm.coe.int/the-metaverse-and-its-impact-on-human-rights-the-rule-of-law-and-democ/1680b178b0

692 European Commission (2023). Staff Working Document: information, insights and market trends on web 4.0 and virtual worlds. Available at: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-information-insights-and-market-trends-web-40-and-virtual-worlds

693 European Commission (2023). Staff Working Document: information, insights and market trends on web 4.0 and virtual worlds. Available at: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-information-insights-and-market-trends-web-40-and-virtual-worlds

competitiveness and worsening existing divides[694]. Forecasts by the European Parliamentary Research Service suggest that those nations leading in AI and XR could evolve into ecosystems dominated by a few major players, mirroring the power wielded by today's largest technology firms, favouring wealthier and more technologically advanced societies[695]. Currently, most technological wealth is already concentrated in the hands of a limited number of nations, such as the United States and China.[696,697] The evolution towards Web 4.0 and virtual worlds risks repeating this pattern, and in the absence of targeted measures, job opportunities in developing countries may be reduced – particularly if resource extraction and manufacturing processes become increasingly automated[698].

At the same time, research points to potentially significant **economic benefits from expanding digital access**, particularly in lower-income regions. For instance, a 10 % jump in mobile broadband adoption could reportedly boost GDP by up to 0.8 %, with marked gains in less developed economies[699].

Overall, the outcome divide under Web 4.0 highlights uneven gains arising from access, skills and opportunities in virtual worlds. Differences in gender representation, the potential for automation and regional competitiveness show how certain groups or locations may face barriers, even where basic infrastructure is in place. At the same time, examples of immersive training, potential growth in GDP and the development of new technologies illustrate the scope for both positive and disruptive effects. As evolution towards Web 4.0 unfolds, these factors could shape emerging disparities in digital environments and across broader economic and social landscapes.

694 Marr, B. (2022). *The most in-demand metaverse skills every company will be looking for*. *Forbes*. Available at: https://www.forbes.com/sites/bernardmarr/2022/06/24/the-most-in-demand-metaverse-skills-every-company-will-be-looking-for/?sh=4b776db07ccd

695 Szczepański, M. (2019). Economic impacts of artificial intelligence (AI). EPRS: European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/637967/EPRS_BRI(2019)637967_EN.pdf ; Middleton, M. (2022). Business, finance, and economics: The IEEE global initiative on ethics of extended reality (XR) report. IEEE Standards Association.

696 United Nations (2023). Global digital compact policy brief: A global digital compact – An open, free and secure digital future for all. Available at: https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/Global_Digital_Compact_Policy_Brief_Infographics_2.pdf

697 United Nations Conference on Trade and Development, Digital Economy Report 2021 (UNCTAD/DER/2021).

698 Middleton, M. (2022). Business, finance, and economics: The IEEE global initiative on ethics of extended reality (XR) report. IEEE Standards Association.

699 Ericsson (no date). Bridging the digital divide with human brilliance. https://www.ericsson.com/en/about-us/new-world-of-possibilities/imagine-possible-perspectives/bridging-the-digital-divide

4. How might Web 4.0 challenges affect internet governance?

Global internet governance[700] is a fairly stable yet evolving environment, with established global institutions and a strong anchor in a multistakeholder approach. In this chapter of the present paper, we look specifically at the challenges and needs for **internet governance** in light of advances towards Web 4.0 and virtual worlds. It is important to note, however, that this chapter does not assess the governance of other technologies that are relevant for Web 4.0 and virtual worlds, such as AI or quantum, beyond their relevance to internet governance.

The term "**multistakeholder governance"** was defined in NETmundial+10 as follows: "internet governance should be built on democratic, multistakeholder processes, ensuring the meaningful and accountable participation of all stakeholders, including governments, the private sector, civil society, the technical community, the academic community and users"[701].

Global multistakeholder collaboration is essential to maintaining the interoperability of the internet, the establishment of consistent rules, the protection of digital rights, as well as addressing the social, economic and environmental impacts of technology. In this chapter, we describe some of the challenges identified with respect to internet governance institutions and their mandates, the importance of multistakeholder involvement, and the observed risks of the fragmentation of governance and policy and regulatory coordination across regions.

This discussion is of particular relevance, given the upcoming review of the WSIS (WSIS +20). The WSIS+20 review in 2025, facilitated by the UN General Assembly, will assess progress and the challenges encountered since the inception of the WSIS. The review will take stock of the implementation of the WSIS Action Lines, review the mandate of the IGF, and ensure its alignment with the Sustainable Development Goals[702]. In particular, the review provides an opportunity to reaffirm commitment towards a multistakeholder approach to internet governance that upholds an open, global and interoperable internet. It also provides an opportunity to consider how internet governance could consider emerging technologies including Web 4.0 and virtual worlds.

In light of the upcoming WSIS+20 review, there is scope to strengthen the role of internet governance institutions in serving as a central space for processes aimed at anticipating and addressing the impacts on the internet of virtual worlds and Web 4.0.

4.1. Internet governance institutions and mandates

The decentralised internet governance model has been integral to the success of internet governance over the past several decades. In this multistakeholder approach, a multitude of actors including governments, the technical community, civil society, the private sector and experts. play a role in shaping decision-making on a global scale. The table below provides an overview of some of the main bodies currently involved in internet governance and standardisation, together with their respective

[700] Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet (Tunis Agenda for the Information Society).

[701] NETmundial+10. (2024). Joint statement on the NETmundial+10. Available at: https://netmundial.br/statement/joint-statement-of-the-netmundial10

[702] WSISI (no date). What is the World Summit on the Information Society (WSIS)? Available at: https://www.itu.int/net4/wsis/forum/2025/Home/About

roles, based on desk research. Extensive cooperation between the various actors underpins the internet's development as a largely open and interoperable environment[703].

Table 2. List of key organisations and mandates, and examples of work related to Web 4.0

MANDATE	ORGANISATION	Example work in relation to Web 4.0
	ICANN	

A non-profit organisation responsible for coordinating the global Domain Name System (DNS), IP address allocation, root server management and other Internet protocol management tasks.	ICANN operates through a multistakeholder approach, and includes:
	• **Board** of Directors, composed of 21 members, including those from various supporting organisations and the community at large
	• **Supporting organisations (SOs),** including the:
	  ◦ Generic Names Supporting Organisation (GNSO), which focuses on the development of policy related to generic top-level domains
	  ◦ Country-code Names Supporting Organisation (ccNSO), which focuses on country-code top-level domains
	  ◦ Address Supporting Organisation (ASO), which manages the distribution and allocation of IP addresses.
	• **Advisory committees (ACs),** which provide advice on specific issues**, including the:**
	  ◦ At-Large Advisory Committee (ALAC), which represents individual internet users.
	  ◦ Governmental Advisory Committee (GAC), which advises on government-related concerns.
	  ◦ Security and Stability Advisory Committee (SSAC), which focuses on security issues within the DNS.
	  ◦ Root Server System Advisory Committee (RSSAC), which advises on the root server system's operations
	• **Special Interest Forums on Technology (SIFT)**, a discussion platform for knowledge sharing and discussions on evolving identifier technologies.
		ICANN actively monitors and assesses emerging technologies to understand their potential impacts on internet governance and the DNS. This includes assessing how advances in areas such as AI, IoT and 5G networks may affect its operations and the broader internet ecosystem[704]. ICANN also assesses challenges to DNS from emerging technologies such as blockchain[705], and has recently accredited two companies specialising in blockchain technologies[706].
		
		ICANN has established forums to provide fact-based presentations on newly emerging topics relevant to its mission. One example of these is the ATU Task Group on Emerging Technologies, which is a collaborative effort between ICANN and the African Telecommunications Union (ATU), focusing on addressing emerging technology issues in Africa[707].

	IGF	
A multistakeholder forum that "informs and inspires" those with policymaking power in both the public and private sectors.	The IGF is composed of several work streams, including the: • **Leadership Panel:** which consists of experts from diverse stakeholder groups and regions. Its purpose is to strengthen the IGF's impact by providing strategic advice. The panel has its dedicated Chair and Vice Chair.	The IGF provides a platform for multistakeholder dialogue on the governance of emerging internet technologies. Several discussions have been held at the IGF, including on the protection of democratic values[708] and children in the

[703] Ringhof, J. (2015). Multilateral internet: Unplugged and somewhat slightly dazed. ECFR. Available at: https://ecfr.eu/article/multilateral-internet-unplugged-and-somewhat-slightly-dazed/
[704] https://www.icann.org/en/system/files/files/draft-pti-fy26-30-strategic-plan-2024-en.pdf
[705] ICANN (2022). Challenges with alternative name systems. Available at: https://www.icann.org/en/system/files/files/octo-034-27apr22-en.pdf
[706] More information is available at: https://www.dreyfus.fr/en/2024/11/25/icanns-accreditation-of-blockchain-specialized-companies-a-new-chapter-for-domain-names/
[707] More information is available at: https://www.icann.org/es/engagement-calendar/details/the-8th-meeting-of-the-atu-task-group-on-emerging-technologies-2025-02-17
[708] IGF (2023). IGF 2023 Day 0 Event #207 Pursuing a metaverse based on democratic values. Available at: https://www.intgovforum.org/en/content/igf-2023-day-0-event-207-pursuing-a-metaverse-based-on-democratic-values

MANDATE	ORGANISATION	Example work in relation to Web 4.0

The mandate of the IGF was laid out in paragraphs 72-78 of the Tunis Agenda, endorsed at the World Summit on the Information Society (WSIS) in 2005.
 	
The forum serves as a space for:
• facilitating dialogue on the main issues affecting the internet;
• identifying emerging issues related to internet governance;
• capacity building; and
• the exchange of best practices.
	• **Multistakeholder Advisory Group (MAG),** which serves as the primary advisory body to the UN Secretary-General. It consists of 40 representatives, and is responsible for planning and designing the annual IGF meeting. Members are selected through a nomination process.
	• **Secretariat,** which facilitates and coordinates the activities of IGF and is responsible for long-term planning.
	• **Intersessional work,** which takes place between annual IGF meetings, and includes:
	  ◦ **dynamic coalitions**: ongoing collaborative groups focusing on specific internet governance topics;
	  ◦ **best practice forums**: platforms for sharing and developing best practices in various internet-related areas;
	  ◦ **policy networks**: multistakeholder expert groups, established in 2020, to conduct research and develop recommendations between annual meetings; and
	  ◦ **regional and national** IGF Initiatives, e.g. EuroDIG.
		metaverse[709], as well as on the governance of Web 4.0 and virtual worlds[710]. The 2023 edition of EuroDIG also included a focus on virtual worlds and associated risks[711].
		
		The IGF uses its policy networks to discuss emerging internet governance issues. Pertinent policy networks include the Policy Network on Artificial Intelligence[712] and the Policy Network on Internet Fragmentation[713].

	ITU	

The ITU is a United Nations specialised agency. It is a multilateral organisation that develops standards for telecommunication networks and services.	The ITU is a multilateral organisation made up of 194 member states, which meets every four years in a plenipotentiary conference. Its organisational structure includes:
	• The **Council**, which acts on behalf of the plenipotentiary conference and meets annually. The Council oversees the administration and management of the ITU.
	• The **General Secretariat**, which manages the overall administration of the ITU.
	• The ITU operates through three main sectors:
	  ◦ **Radiocommunication sector** (ITU-R)
	  ◦ **Telecommunication Standardisation sector** (ITU-T)
	  ◦ **Telecommunication Development sector** (ITU-D)
	• **Administrative** regions and regional offices – the ITU is divided into five administrative regions.
		The telecommunication Standardisation Sector (ITU-T) has initiated specific metaverse activities within Study Groups SG16, SG17 and SG20, such as the October 2022 workshop on the metaverse and multimedia.
		
		In December 2022, the **ITU-T Telecommunication Standardisation Advisory Group (TSAG)** established a new Focus Group on Metaverse (FG-MV). This group recently concluded its analysis of the technical requirements of the metaverse[714].

	IETF	
A global community of network designers, operators, vendors and researchers responsible for developing and	The IEFT consists of: • The **Internet Architecture Board**, a committee responsible for architectural oversight of IETF activities and oversight of standardisation	Members of the IETF have initiated some work in relation to virtual worlds and Web 4.0. More specifically, topics related to virtual worlds have been explored through

[709] IGF (2024). IGF 2024 WS #14 Children in the Metaverse. Available at: https://intgovforum.org/en/content/igf-2024-ws-14-children-in-the-metaverse

[710] In the context of the Global Multistakeholder High Level Conference on Governance for Web 4.0 and virtual worlds, hosted by the European Commission and the Polish Presidency of the Council on 31 March–1 April 2025, IGF (2024) session 'Governing the Future Internet The 2025 Web 4 0 Conference'

[711] More information is available at: https://comment.eurodig.org/eurodig-2023-messages/main-topic-3-digital-platforms/subtopic-1-virtual-worlds-but-real-risks-navigating-metaverses-as-a-next-generation-of-digital-platform

[712] More information is available at: https://www.intgovforum.org/en/pnai

[713] https://www.intgovforum.org/en/content/policy-network-on-internet-fragmentation

[714] Taken from: https://standict.eu/success-stories/accessibility-metaverse-itu-t-focus-group-metaverse-fg-mv

MANDATE	ORGANISATION	Example work in relation to Web 4.0
promoting internet standards, including TC/IP, HTTP and others.	processes. The IAB also plays an advisory role to ISOC. • The **Internet Engineering Steering Group (IESG**), which is composed of area directors (ADs) and is responsible for the standards process. The ADs oversee working groups and guide their progress toward producing requests for comments (RFCs) • Working groups organised by technical domains. The process of standards development is consensus-driven, developing standards through the "request for comment" process.	recent internet drafts, such as those exploring information-centric networking (ICN), focusing on enhancing interoperability between different metaverse platforms[715,716,717].
	Internet Society	
The Internet Society (ISOC) is a non-profit organisation that aims to ensure the open development, evolution and use of the internet for the benefit of all people.	The governance structure of ISOC includes the: • **Board of Trustees**, composed of members elected from various stakeholder groups, including ISOC chapters, ISOC organisation members, and the IETF. The Board is responsible for strategic direction and the oversight of ISOC's activities. • **President and CEO,** who oversees day-to-day operations and implements ISOC's strategic direction. • **Organisation members' Advisory Council**, which represents the interests of organisation members, including businesses, NGOs, governments and educational institutions. The Advisory Council provides advice and prioritises issues of concern to ISOC members. • **Chapters** – ISOC has numerous local chapters around the world. • **Membership** – including individual and organisational members. Decisions are taken following an extensive consultation process, and are consensus driven.	The Internet Society's internet impact assessment is a useful tool for assessing the impacts of emerging technologies on the internet.
	Internet Research Task Force (IRTF)	
The IRTF is an organisation that promotes research on issues such as internet protocols, architecture and applications.	The IRTF is composed of the: • **Chair**, appointed by the Internet Architecture Board and responsible for ensuring that research groups produce coherent and timely outputs. • **Internet Research Steering Group** – assists the chair in managing the research groups. • **Research Groups** – focused, long-term research groups that work on various topics related to internet protocols, applications, architecture and technology. Examples include the Applied Networking Research Group and the Crypto Forum Research Group. The IRTF operates with a focus on collaboration and inclusivity, encouraging participation from a diverse	The IRTF's current research groups cover some pertinent issues through groups such as the Crypto Forum Research Group and Human Rights Protocol Considerations Research Group[718].

[715] Taken from: https://datatracker.ietf.org/doc/draft-hong-icn-metaverse-interoperability/
[716] Taken from: https://datatracker.ietf.org/doc/html/draft-fmbk-icnrg-metaverse-01#section-7
[717] Taken from: https://datatracker.ietf.org/doc/draft-hong-icn-metaverse-interoperability/
[718] Taken from: https://www.irtf.org/

MANDATE	ORGANISATION	Example work in relation to Web 4.0
	range of contributors in the internet research community. The organisation is overseen by the Internet Architecture Board, which maintains an architectural overview and provides guidance on its activities.	
	World Wide Web Consortium (W3C)	
W3C is an international community that develops open standards to ensure the long-term growth and interoperability of the World Wide Web. W3C's work includes HTML, CSS, and web accessibility standards.	• The **Board of Directors** has ultimate authority over the Consortium's strategic direction and fiduciary responsibilities. • The **President** leads the organisation and is responsible for the day-to-day implementation of the Board's strategic directives. • The **Advisory Committee** consists of one representative from each W3C member organisation. It reviews W3C processes and elects members of the Advisory Board and Technical Architecture Group (TAG). • The **Advisory Board** provides guidance on technical and strategic issues. • The **Technical Architecture Board** documents principles of web architecture, and addresses issues related to the overall design of the web. • **Chartered groups** focus on specific areas of web standards development. These groups produce most of the W3C's standards, guidelines and supporting materials. • **Committees and task forces** assist the Board in areas such as finance, governance and personnel management. • **Community groups** are informal forums for discussing ideas relevant to specific interests within the web community.	In April 2021, W3C established the Metaverse Interoperability Community Group (MICG) to bridge virtual worlds by designing and promoting protocols for identity, social graphs, inventory and more[719]. At the time of reporting, this group does not appear to be active.
	Regional internet registries (RIRs)	
Regional internet registries (RIRs) are structured to manage the allocation and registration of internet number resources within specific geographical regions.	There are five main RIRs, each serving a distinct region: • **AFRINIC** serves Africa (founded in 2005) • **APNIC** serves the Asia-Pacific region (founded in 1993) • **ARIN** serves North America (founded in 1997) • **LACNIC** serves Latin America and the Caribbean (founded in 2001) • **RIPE NCC** serves Europe, Central Asia and the Middle East (founded in 1992) Each RIR operates as a not-for-profit, membership-based organisation.	No direct work to date in relation to virtual worlds or Web 4.0

The strengths of the multistakeholder approach to internet governance is its horizontal nature and its ability to address a diverse range of issues from the perspectives of diverse stakeholder groups globally. Nevertheless, given the challenges to internet governance arising from the Web 4.0-related developments presented in Chapter 3 of this paper, it is important to consider how existing multistakeholder organisations' mandates can be adapted.

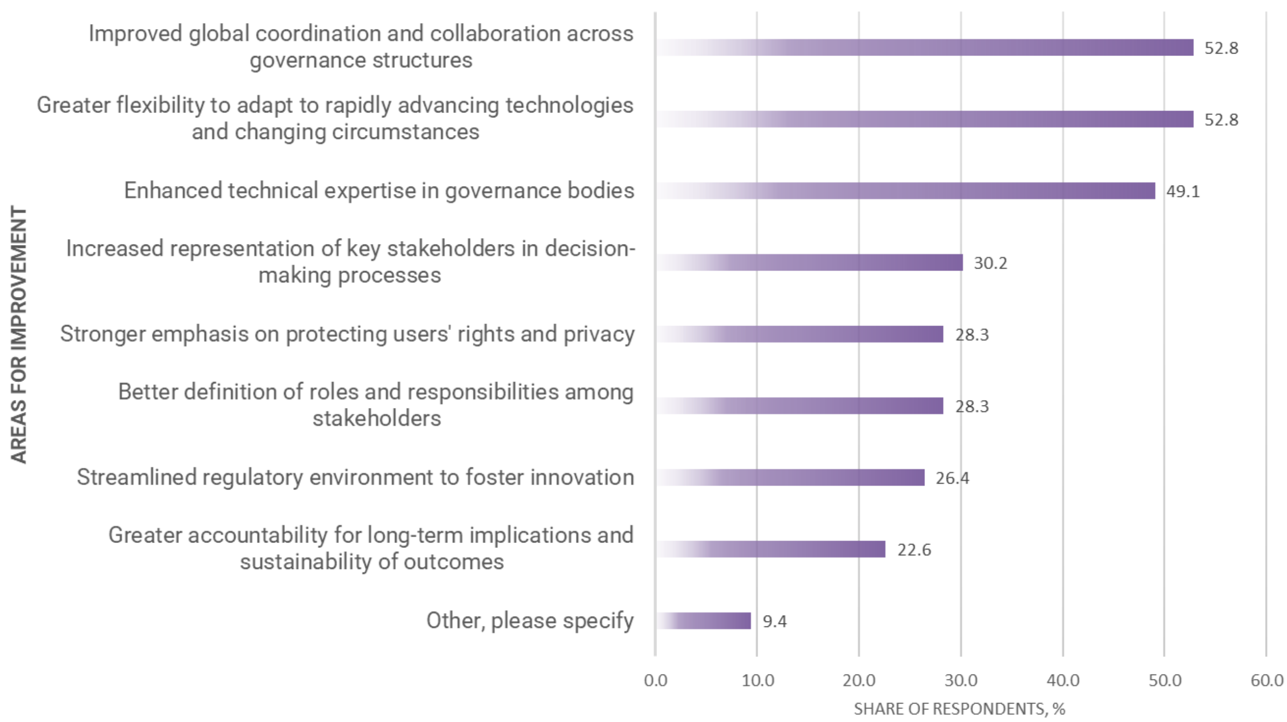
When asked how adequate current internet governance mechanisms are in tackling Web 4.0-related developments, a total 52.4 % of respondents to the online consultation stated that internet governance

[719] Taken from: https://www.w3.org/community/metaverse-interop/

mechanisms are **generally adequate, but require adjustments** to address the challenges of virtual worlds and Web 4.0. Meanwhile, 38.1 % advocated for entirely new mechanisms, and only 9.5 % considered the current frameworks fully sufficient.

While the mandates of multistakeholder internet governance organisations focus on making the internet "work better"[720], and ensuring it remains open, global, secure and trustworthy[721], the distributed nature of these organisations results in work that focuses on "neutrally facilitating the interoperability, resilience, and growth of the internet"[722]. According to some stakeholders, the challenges and impacts on the internet that are anticipated to arise from developments in Web 4.0 and virtual worlds call for a **future-focused and anticipatory approach to governance**. In the online consultation conducted as part of this project, "Greater flexibility to adapt to rapidly advancing technologies and changing circumstances" was seen as being among the most necessary adjustments to current internet governance mechanisms (see figure below). Similarly, the outcomes of NETmundial 10+ highlighted the importance of increased agility and adaptability to changing circumstances, as well as proactive engagement with emerging technologies[723]. To ensure the flexibility and speed needed to respond to urgent emerging issues[724,725], it is important that internet governance processes are open It is also necessary that support is available for the participation and capacity building of stakeholders who can bring issues related to Web 4.0 to the discussion, while following a consensus driven, bottom-up and distributed approach.

Figure 15. Online consultation: necessary adjustments to internet governance mechanisms



[720] Taken from: https://www.ietf.org/about/introduction/
[721] Taken from; https://www.internetsociety.org/mission/
[722] Ringhof, J. (2015). Multilateral internet: Unplugged and somewhat slightly dazed. ECFR. Available at: https://ecfr.eu/article/multilateral-internet-unplugged-and-somewhat-slightly-dazed/
[723] NETmundial (2024). NETmundial+10 Multistakeholder Statement. Available at: https://netmundial.br/pdf/NETmundial10-MultistakeholderStatement-2024.pdf
[724] Ringhof, J. (2015). Multilateral internet: Unplugged and somewhat slightly dazed. ECFR. Available at: https://ecfr.eu/article/multilateral-internet-unplugged-and-somewhat-slightly-dazed/
[725] McCarthy, K. (2022). Revitalising Global Internet Governance. Tony Blair Institute for Global Change. Available at: https://institute.global/insights/tech-and-digitalisation/revitalising-global-internet-governance

Source: Online consultation; Q18. "With the above challenges in mind, what adjustments are needed to the current internet governance mechanisms for a successful transition to virtual worlds and Web 4.0? Please select the top 3 areas where improvements are necessary"; N=53.

In addition, while the argument that **improved coordination** is needed between internet governance institutions is not new, it is particularly important in relation to Web 4.0 and virtual worlds. The NETmundial+10 process highlights fragmentation and duplication as key challenges to address in order to strengthen the effectiveness of internet governance and digital policy processes[726]. Moreover, stakeholders consulted for this project ranked "Improved global coordination and collaboration across governance structures" among the most necessary adjustments to internet governance approaches (see figure above). Furthermore, the IGF PNIF 2023 report stressed the importance of institutionalised coordination mechanisms aimed at clarifying mandates and eliminating duplication rather than relying on informal networks[727]. The **emergence of various governance initiatives** targeting different issues in relation to Web 4.0 and virtual worlds technologies could lead to a siloed approach (see also Section 4.3)[728]. Isolated initiatives, including those that focus on standardisation, run the risk of failing to consider the impacts on the internet of virtual worlds and related technologies. For example, civil society groups have voiced concerns about the efforts of the ITU to promote national visions for a more centrally controlled digital technology landscape[729]. If not addressed, such isolated approaches to virtual worlds and Web 4.0 governance could lead to internet fragmentation.

Web 4.0 and virtual worlds developments present both opportunities and challenges across the entire internet stack. Historically, internet governance bodies have primarily focused on the network layer of the internet, with governments and private companies primarily driving the content and applications layers. While the architecture of the internet can enable and influence how the internet is used, on its own it cannot address abuse, misinformation, inequality or many other issues that are also pertinent to Web 4.0 and virtual worlds[730]. With regard to technology developments in the application layer, the current standards-setting process for the internet is increasingly becoming a space for geopolitical contestation in which governments and Big Tech players take a large role (see Section 4.2). While both of these groups of stakeholders are very important, it is also crucial that discussions include other stakeholders such as smaller companies, technical community and civil society[731]. To this end it is important to **consider the geopolitical and human rights implications of the internet's evolution**, alongside its technical development. In relation to this, civil society organisations are calling for lower barriers to entry to standardisation processes, to ensure that the human rights implications of new standards are considered[732]. Furthermore, as elaborated in Section 4.2 below, representatives of civil society face numerous other barriers to participation in internet governance discussions.

It is therefore important to reflect on the **modalities of collaboration** between stakeholders within internet governance organisations. Currently, internet governance organisations operate using a "layered" or "building block governance approach"[733]. This approach has been instrumental to the

[726] NETmundial+10. (2024). Joint statement on the NETmundial+10. Available at: https://netmundial.br/statement/joint-statement-of-the-netmundial10

[727] IGF PNIF (2023). IGF 2023 Policy Network on Internet Fragmentation Output report, November 2023. Available at: https://www.intgovforum.org/en/filedepot_download/256/26667

[728] Kleinwächter, W. (2025). IGF 2024 in Riyadh: AI, WSIS+20 and the Global South. Available at: https://circleid.com/posts/igf-2024-in-riyadh-ai-wsis20-and-the-global-south

[729] Barber, I., Bopanna, A., Canales, M.P., McDonald, E., & Payne, R. (2025). 2025: a stress test for the multistakeholder model? Global Partners Digital. Available at: https://www.gp-digital.org/2025-a-stress-test-for-the-multistakeholder-model/

[730] Barber, I., Bopanna, A., Canales, M.P., McDonald, E., & Payne, R. (2025). 2025: a stress test for the multistakeholder model? Global Partners Digital. Available at: https://www.gp-digital.org/2025-a-stress-test-for-the-multistakeholder-model/

[731] Bennett, A., Garson, M., Boakye, B., Beverton-Palmer, M., & Erzse, A. (2021). The Open Internet on the Brink: A Model to Save Its Future. Tony Blair Institute for Global Change. Available at: https://institute.global/insights/tech-and-digitalisation/open-internet-brink-model-save-its-future

[732] Barber, I., Bopanna, A., Canales, M.P., McDonald, E., & Payne, R. (2025). 2025: a stress test for the multistakeholder model? Global Partners Digital. Available at: https://www.gp-digital.org/2025-a-stress-test-for-the-multistakeholder-model/

[733] This approach conceptualises the internet ecosystem as a series of distinct but interconnected layers, each requiring specific governance mechanisms and frameworks. These layers are typically defined as the infrastructure layer (cables, routers, servers, protocols such as the TCP/IP that enable communication – governance institutions include ICAAN and regional internet registries); the logical layer (data transmission and processing over the internet, including DNS management and technical standards – governance institutions include the IETF and W3C); the content layer (information and applications); and the social and economic layer.

success of internet governance, allowing for flexibility[734]. While this approach is integral to standardisation process, when addressing the cross-cutting impacts of emerging technologies, it is important to first hold broader discussions. These should bring together diverse stakeholders, including representatives of different internet governance institutions, before standardisation efforts begin. While ICANN handles DNS, the ITU handles telecommunication standards, W3C works on web standards, etc. It is important to recognise that the challenges of Web 4.0 do not map always neatly on to these categories, and broader discussions on the cross-cutting risks and opportunities of emerging technologies would be useful. For example, ensuring interoperability is not just a problem of technical standards, because it could require policy agreements (which could involve the IGF or governments) and business cooperation (which might involve consortia such as the Metaverse Standards Forum). Without efficient communication and collaboration between stakeholders, there is a risk of either duplication or gaps. For example, in the future, coordination between the IETF and W3C might become more frequent, as standards for application-level protocols intersect with developments in the transport layer.

Furthermore, emerging issues, by the nature of being new, **often do not have a clear place** within the existing internet governance ecosystem[735]. This is not necessarily a criticism of existing internet governance institutions or processes, but rather a feature of some of these issues being novel or only recently becoming relevant to certain institutions. For instance, some experts interviewed as part of this project noted that issues such as blockchain and machine learning are not clearly reflected in existing mandates, and require collaboration across internet governance institutions. ICANN's mandate does not currently extend to alternative naming or identity solutions. Furthermore, as mentioned above, the IETF focuses on creating consensus-based technical standards. Nevertheless, issues of identity, data governance and content moderation are becoming increasingly transversal. The ITU, as part of its focus on expanding digital connectivity and promoting sustainable digital transformation, set up a Focus Group on the Metaverse (FG-MV) in 2023[736] – although some in the multistakeholder community have raised concerns non-state actors might be excluded from such a multilateral approach[737]. Lastly, while the IGF serves as a bottom-up forum on internet governance issues and aims to focus on emerging issues associated with Web 4.0 technologies, it can inform policy discussions – but does not make any binding decisions.

While there is general consensus that multistakeholder internet governance institutions have a wealth of expertise to address governance questions in relation to the impacts on the internet of virtual worlds and Web 4.0 technologies, it is key for them to ensure future-focused and cross-cutting working approaches.

4.2. Strengthening multistakeholder involvement

Web 4.0 and virtual worlds technologies pose novel challenges and opportunities for stakeholder involvement in internet governance discussions. As virtual worlds and immersive technologies become more prevalent, the stakeholder ecosystem will expand to include new groups. This evolution also amplifies some of the longstanding concerns about stakeholder representation in internet governance processes. Our research shows that these shifting dynamics associated with the evolution towards Web 4.0 necessitate renewed efforts to ensure inclusivity, transparency and meaningful engagement.

[734] McCarthy, K. (2022). Revitalising Global Internet Governance. Tony Blair Institute for Global Change. Available at: https://institute.global/insights/tech-and-digitalisation/revitalising-global-internet-governance

[735] McCarthy, K. (2022). Revitalising Global Internet Governance. Tony Blair Institute for Global Change. Available at: https://institute.global/insights/tech-and-digitalisation/revitalising-global-internet-governance

[736] ITU (no date). Explore the Impact of FG-MV. Available at: https://www.itu.int/metaverse/fg-mv-outcomes/

[737] DigWatch (no date). China's push for metaverse regulation raises concerns over privacy and freedom. Available at: https://dig.watch/updates/chinas-push-for-metaverse-regulation-raises-concerns-over-privacy-and-freedom

The evolution to Web 4.0 introduces new stakeholder groups into discussions of governance. First among these are **virtual world developers, creators, and immersive technology companies and start-ups,** who shape entire digital ecosystems that aim to blur the divide between physical and virtual environments. In this sense, these actors are both technology infrastructure providers and environment architects, who make significant decisions about avatar systems and environmental rendering, as well as biometric data collection and use, and various social aspects of immersive experiences[738]. These stakeholders bring diverse perspectives and unique expertise and experiences that can inform and enrich governance discussions.

Second, beyond commercial developers, **open-source projects and communities** represent another significant group of stakeholders, having played a considerable role in the development of various Web 4.0 technologies – in particular, in establishing standards and tools for immersive experiences[739]. Projects such as Open Source Virtual Reality (OSVR) and A-Frame have been instrumental in democratising VR development[740], while initiatives such as the Open Metaverse Interoperability Group[741] work to create open protocols for virtual world interconnectivity. Interviews conducted for this study also highlighted the importance of diverse **creative communities** in building and maintaining virtual worlds. These communities, which include digital artists, 3D modellers, game designers and independent developers, are increasingly important in the evolution towards Web 4.0. Unlike corporate actors, many open-source initiatives operate on volunteer-based, distributed models that do not easily integrate into traditional internet governance frameworks. Moreover, the financial and time constraints faced by such stakeholders limit their ability to engage in governance processes at the same level as well-resourced actors from the private sector.

Third, the technological foundations of Web 4.0 encompass various emerging technologies. The **companies developing advanced technologies** such as quantum computing, brain–computer interfaces and next-generation networking systems bring specialised expertise and unique perspectives. For instance, **quantum computing** companies are developing solutions that could fundamentally alter internet infrastructure, particularly in areas such as cryptography and secure communications. Their participation in governance discussions is crucial as Web 4.0 evolves, given the potential impact that quantum computing will have on privacy, security and the underlying architecture of virtual worlds[742].

The focus on decentralisation associated with Web 4.0 could also introduce some novel considerations into traditional multistakeholder internet governance processes. Traditional standards bodies such as the IETF and W3C operate through consensus-based processes with identified participants[743]. Conversely, decentralised communities often make decisions through anonymous or pseudonymous participation in open-source projects[744]. This could create parallel standards development processes that might not align effectively. For example, blockchain-based standards for the interoperability of virtual assets (e.g. NFTs, digital currencies, tokenised virtual real estate, virtual goods sold in online marketplaces, reward tokens) might develop separately from traditional standards processes. Moreover, open-source protocols for virtual worlds might conflict with proprietary platforms' business models, while the emphasis of creative communities on user-generated content

738 McKinsey & Company (2022). Value creation in the metaverse. Available at: https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/value-creation-in-the-metaverse

739 Kocher, L. (2023, 26 January). The importance of open source in the metaverse. Open Source For You. https://www.opensourceforu.com/2023/01/the-importance-of-open-source-in-the-metaverse/

740 Erickson, L. (2022, 14 June). The open source metaverse: The future of digital worlds? OpenSource.com. Available at: https://opensource.com/article/22/6/open-source-metaverse

741 More information available at: https://omigroup.org/

742 Ghosh, A., Hassija, V., Chamola, V., & El Saddik, A. (2024). A Survey on Decentralized Metaverse using Blockchain and Web 3.0 technologies, Applications, and more. *IEEE Access*.

743 Internet Society. (2015, 30 October). Policy Brief: Internet Governance. Available at: https://www.internetsociety.org/policybriefs/internetgovernance/

744 Ghosh, A., Hassija, V., Chamola, V., & El Saddik, A. (2024). A Survey on Decentralized Metaverse using Blockchain and Web 3.0 technologies, Applications, and more. *IEEE Access*.

and participatory design could challenge conventional approaches to content moderation and digital rights management.

Furthermore, stakeholders involved in the consultation conducted for this project highlighted concerns about the **influence of corporate actors** on developments in Web 4.0. Some stakeholders highlighted that a few corporate actors – usually large tech companies from the Global North – could wield an increasingly disproportionate influence over internet governance conversations[745]. Similarly, research suggests that current XR governance conversations are greatly influenced by industry actors[746]. This is relevant to both multilateral forums, in which corporate actors may enjoy better access to national bodies, compared with civil society actors, as well as the technical discussions, where technical experts may be associated with specific corporate actors[747,748]. On a similar note, the stakeholders consulted also raised concerns about **power imbalances** between large technology firms and small developers. Major technology companies can dedicate substantial resources to participating in governance discussions and standards development. Smaller independent developers and studios, meanwhile, often lack the capacity to engage meaningfully in these processes, despite potentially offering more diverse and innovative approaches to the design of virtual worlds. The results of the online consultation highlight this concern, with stakeholders identifying transparent mechanisms for incorporating input, as well as fair and equitable discussions that address the distinct needs of all stakeholders, as being among the most important elements for stakeholder involvement in internet governance (see Annexes 1). This concentration of power, knowledge and financial resources has given a small number of corporations considerable leverage in determining the standards and protocols that will define the internet of the future[749]. This runs the risk of creating an ecosystem in which power is concentrated, and in which major players are the primary drivers of standards and practices – potentially leading to siloed developments and limited interoperability.

This disparity in participation also has direct implications for smaller economic actors, particularly **SMEs**. Their participation in governance discussions is crucial to developing frameworks that support innovation while ensuring interoperability and fair competition for Web 4.0 and virtual worlds. As described in Chapter 3, Web 4.0 is expected to bring significant changes to business models, especially as SMEs increasingly engage with virtual worlds and immersive digital marketplaces. Despite their importance, SMEs often lack the resources to engage in multistakeholder processes, leaving governance decisions to be shaped primarily by larger corporations.

As highlighted by some stakeholders involved in the consultation, one of the major obstacles to meaningful stakeholder engagement, particularly for civil society, is the **technical knowledge gap**, which often prevents non-technical organisations from effectively engaging in governance discussions that are dominated by industry and government actors. The complexity of emerging Web 4.0 technologies such as decentralised virtual worlds and AI-driven ecosystems, further exacerbates this challenge. Responses to the online consultation indicate that many civil society organisations lack the resources and technical expertise to keep pace with rapidly evolving governance issues. Similarly, respondents to the online consultation indicated that the most important elements for ensuring stakeholder representation in internet governance were capacity-building initiatives and open, inclusive consultation processes – each of which was selected by a majority of respondents (see Annex 1).

745 Moore, M., & Tambini, D. (Eds.). (2018). *Digital dominance: the power of Google, Amazon, Facebook, and Apple*. Oxford University Press.

746 Egliston, B., Carter, M., & Clark, K.E. (2024). Who will govern the metaverse? Examining governance initiatives for extended reality (XR) technologies. *New Media & Society*, 0(0). https://doi.org/10.1177/14614448231226172

747 Cath, C. (2021). The technology we choose to create: Human rights advocacy in the Internet Engineering Task Force. *Telecommunications Policy*, 45(6), 102144.

748 De Gregorio, G., & Radu, R. (2022). Digital constitutionalism in the new era of Internet governance. *International Journal of Law and Information Technology*, 30(1), 68-87.

749 European Parliament, Directorate-General for Parliamentary Research Services, Perarnaud, C., Rossi, J., Musiani, F. et al. (2022) 'Splinternets' – Addressing the renewed debate on internet fragmentation, European Parliament. Available at: https://data.europa.eu/doi/10.2861/183513

Last, there is a need to **reflect and protect diverse cultural, social and indigenous values** in the design and use of digital technologies – particularly as Web 4.0 technologies begin to shape more immersive and identity-driven experiences. As outlined in WSIS Action Line 8, Cultural and Linguistic Diversity and Local Content Promotion, there is a challenge in balancing the innovative potential of emerging technologies such as AI with the need to protect cultural heritage, creativity and ethical considerations in the cultural sector[750]. This concern is especially acute, given the persistent **underrepresentation of civil society and geographic imbalances** in internet governance processes. In 2022, civil society groups occupied only 12 % of leadership roles within the ICANN community, while 63 % of those seated in leadership roles represented North America and Europe[751]. Similarly, at 2024 IGF in Riyadh, civil society representation remained disproportionately low at 12 %, compared with 45 % for governments and 25 % for the private sector. The Global South faces particular challenges to participation in internet governance discussions, with key meetings and events predominantly taking place in the Global North. This disparity is evident in the geographical distribution of CSO representatives at IGF during the period 2009-2019, with just six countries accounting for around 39 % (1,113 out of 2,830) of total CSO representation. Meanwhile, 27 countries have only ever been represented by a single CSO[752]. These disparities not only limit the diversity of perspectives in governance discussions; they also hinder the development of inclusive policies that reflect the interests of all virtual worlds and Web 4.0 users. In conclusion, strengthening the multistakeholder governance model for Web 4.0 requires not only addressing the barriers outlined above but also ensuring that emerging stakeholder groups, such as virtual world developers, decentralised communities and quantum computing firms, are meaningfully integrated into governance discussions.

4.3. Fragmentation of internet governance and the need for coordination

The multistakeholder approach has been central to internet governance. It emphasises inclusive, democratic collaboration by governments, private sector actors, civil society and users to maintain interoperability, safeguard rights and address technological impacts. This section examines the risk of internet governance becoming fragmented, and the need for coordination in light of advances in Web 4.0 and virtual worlds. It is important to note that while fragmentation in governance is closely interrelated with other forms of fragmentation, it differs from the fragmentation of the internet's technical layer or user experience[753]. According to the PNIF framework, the fragmentation of internet governance refers to a lack of coordination between and inclusion in internet governance and standards bodies[754].

750 International Telecommunication Union (ITU) (2003). Plan of Action. Available at: https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!PDF-E.pdf

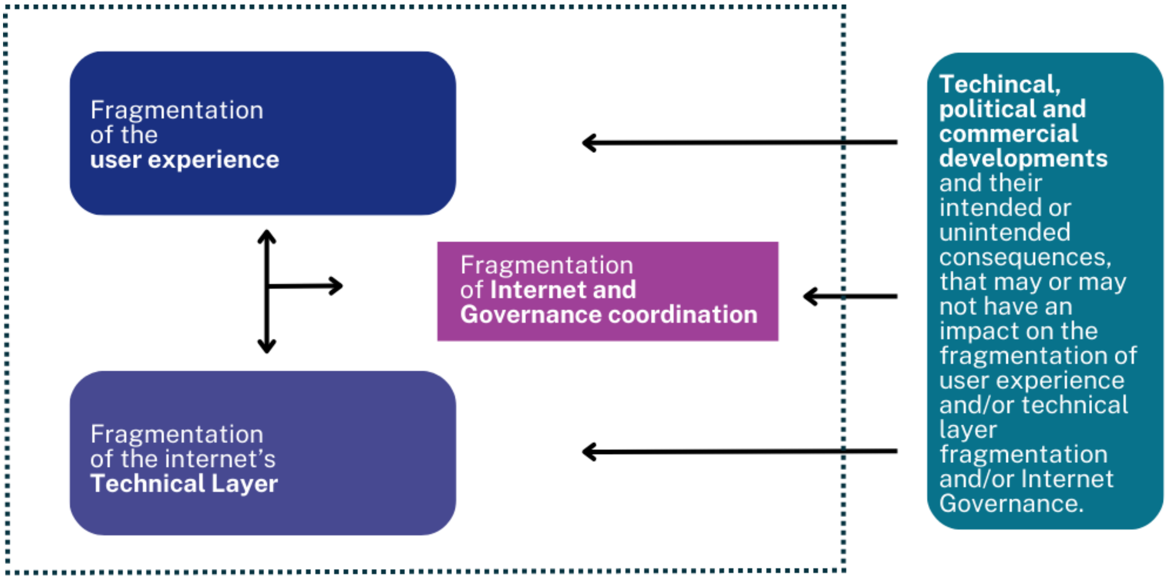
751 National Democratic Institute (2022). Influencing the Internet: Democratising the Politics that Shape Internet Governance. Available at: https://www.ndi.org/sites/default/files/NDI%20Norms%20White%20Paper%20May%202022_1.pdf

752 Tjahja, N., Meyer, T., & Shahin, J. (2021). What is civil society and who represents civil society at the IGF? An analysis of civil society typologies in internet governance. *Telecommunications Policy*, *45*(6), 102141.

753 IGF PNIF (2023). IGF 2023. IGF 2023 Policy Network on Internet Fragmentation Output report. November 2023. Available at: https://www.intgovforum.org/en/filedepot_download/256/26667

754 IGF PNIF (2023). IGF Policy Network on Internet Fragmentation. Available at: https://intgovforum.org/en/filedepot_download/256/28194

Figure 16. PNIF framework for discussing internet fragmentation



Source: IGF PNIF[755]

Fragmentation of internet governance can manifest in various ways, including **siloed or duplicated discussions, the exclusion of specific groups, governance conflicts** between multistakeholder internet governance and standards bodies, and with national policies[756]. The fragmentation of internet governance and coordination can be caused by various issues, including but not limited to: (1) a lack of coordination or cooperation; (2) one body taking up issues that are already part of another institution's mandate; (3) creating a new body whose mandate overlaps with that of another body; (4) not allowing the full participation of the multistakeholder community[757].

Efforts to manage the risk of fragmentation of the internet and its governance are reflected in **global declarations and commitments**. The Global Digital Compact emphasises the need for international cooperation among stakeholders to address the risks of internet fragmentation. Moreover, the IGF statement on preventing fragmentation[758] has not changed significantly throughout different iterations of the Global Digital Compact text, suggesting a consensus around this challenge[759]. This commitment builds on earlier declarations, such as those by the G77, ITU and the Declaration for the Future of the Internet, which have recognised the importance of preventing internet fragmentation. When it comes to governance, NETmundial+10 reaffirmed the importance of avoiding the duplication and fragmentation of governance spaces, emphasising better coordination between processes.

Respondents to the **stakeholder consultation** called for improved cooperation and cohesion, while avoiding duplication and siloed initiatives. For example, they highlighted the need to promote greater cooperation between stakeholders in internet governance institutions in order to avoid duplication and ensure a more coherent approach to governance. Respondents also warned of the risks of fragmented or competing initiatives, and stressed the importance of discussing the internet governance issues arising from Web 4.0 and the development of virtual worlds in a multistakeholder context.

755 Available at: https://intgovforum.org/en/filedepot_download/256/28194
756 IGF PNIF (2023). IGF Policy Network on Internet Fragmentation. Available at: https://intgovforum.org/en/filedepot_download/256/28194
757 IGF PNIF (2023). IGF 2023 Policy Network on Internet Fragmentation Output report. November 2023. Available at: https://www.intgovforum.org/en/filedepot_download/256/26667
758 "Promote international cooperation among all stakeholders to prevent, identify and address risks of fragmentation of the Internet in a timely manner".
759 IGF (2025). Policy Network on Internet Fragmentation: Output report. January 2025. Available at: https://intgovforum.org/en/filedepot_download/256/28579

It should be noted that the emergence of Web 4.0 and virtual worlds is not inherently likely to lead to the fragmentation of internet governance and coordination. A key theme that emerged from the interview programme was that the current internet architecture and its multistakeholder governance could be adapted to the development of Web 4.0 and virtual worlds without the need to create any additional organisational forums.

However, there is a risk that stakeholders might attempt to address Web 4.0 and virtual world-related governance questions in a siloed, duplicative or inconsistent manner. Some specific mechanisms for how this could take place are elaborated below.

- **Mechanism 1: Mismatch between policy and regulatory measures and decisions made by internet governance bodies**

As with today's digital landscape, full policy and regulatory alignment between countries is neither expected nor feasible. Instead, stakeholders within global governance bodies discuss and collaborate on issues that require international agreement, such as internet standards, protocols and human rights.

Therefore, the discussion of this mechanism specifically talks about inconsistencies between the discussions and agreements that take place in global internet governance institutions on the one hand, and government policies and regulatory measures on the other. More specifically, as the IGF PNIF 2024 report states, "national governments can also contribute to fragmentation by introducing governance that conflicts with processes and policies agreed through multistakeholder internet governance and standard bodies"[760].

Various authors and stakeholders have highlighted some incentives that could lead to such fragmentation. For instance, the Digital Policy Hub suggests that concerns about public safety, cybersecurity and the impact of AI on intellectual property could be used as a pretext for some governments to push for stricter internet regulations, potentially expanding their influence in comparison to the present[761]. While not an issue in itself, this could drive more state-centric decision-making, potentially sidelining other stakeholders such as private companies, civil society and technical experts, or coming into conflict with global internet governance agreements[762,763]. Moreover, as described in Section 3.43.4, it is possible that some governments might misuse the capabilities of Web 4.0 and virtual worlds in ways that conflict with global human rights principles or which compromise the open and global nature of the internet – for example, under the pretext of security, sovereignty or increased control over citizens.

- **Mechanism 2: Commercial interests that contradict incentives towards openness and inclusiveness**

The private sector plays a strong role in internet governance, including the shaping of future standards and protocols[764]. So far, large technology companies have generally supported the global and open architecture of the internet[765]. According to the IGF PNIF 2024 report, "commercial

[760] IGF (2025). Policy Network on Internet Fragmentation: Output report. January 2025. Available at: https://intgovforum.org/en/filedepot_download/256/28579
[761] Digital Policy Hub (2024). Assessing the Near Future of Multistakeholder Internet Governance. Available at: https://www.cigionline.org/static/documents/DPH-paper-Cramer.pdf
[762] Digital Policy Hub (2024). Assessing the Near Future of Multistakeholder Internet Governance. Available at: https://www.cigionline.org/static/documents/DPH-paper-Cramer.pdf
[763] McCarthy, K. (2022). Revitalising Global Internet Governance. Tony Blair Institute for Global Change. Available at: https://institute.global/insights/tech-and-digitalisation/revitalising-global-internet-governance
[764] European Parliament, Directorate-General for Parliamentary Research Services, Perarnaud, C., Rossi, J., Musiani, F. et al. (2022) 'Splinternets' – Addressing the renewed debate on internet fragmentation, European Parliament. Available at: https://data.europa.eu/doi/10.2861/183513
[765] Ringhof, J. (2023). Multilateral internet: Unplugged and somewhat slightly dazed. European Council on Foreign Affairs. Available at: https://ecfr.eu/article/multilateral-internet-unplugged-and-somewhat-slightly-dazed/

decisions by large platforms and providers also raise concerns, as they may risk further fragmenting the Internet, potentially undermining its openness and interoperability"[766].

When it comes to metaverse-specific standards, international cooperation in developing standards is only in its early stages[767], during which corporate actors have taken a leading role[768,769,770]. Some respondents warned that the lack of a single interoperability framework or widely agreed standards for virtual worlds and Web 4.0 technologies raises concerns about fragmentation between different virtual world platforms.

Several stakeholders who took part in the consultation pointed out that the development of standards in a flexible manner by the private sector, without requiring consensus and standards in the early stages, is important for innovation. In the past, major technology standardisation battles eventually led to industry convergence around a single standard. Therefore, Web 4.0 could follow a similar trajectory, with industry-driven standardisation emerging over time.

Companies working on the development of virtual worlds and other Web 4.0-related technologies may be incentivised to pursue walled gardens, for instance to gain from the limited transfer of user data between platforms or a lack of integration of identities between systems that use behavioural data[771]. Therefore, some stakeholders believe that action should be taken to establish open and transparent standards to ensure interoperability.

- **Mechanism 3: Lack of coordination between internet governance bodies**

As discussed in Section 4.1, it is crucial to coordinate governance initiatives connected with the rapidly evolving technologies related to Web 4.0 and virtual worlds. Respondents of the online consultation identified "improved global coordination and collaboration across governance structures" as one of the most essential adjustments needed for internet governance in response to the emergence of Web 4.0 and virtual worlds, as shown in Figure 15. According to the IGF PNIF 2024 report, "when these [global internet governance] bodies do not coordinate or are not inclusive, it can and does result in fragmentation" and recommends *to* "improve coordination between existing internet governance bodies"[772]. Moreover, as already highlighted above, NETmundial +10 also states that "it is important to avoid fragmentation and duplication of fora, to make sure that Internet governance and digital policy processes can be effective. Instead, better coordination between processes dealing with overlapping issues is strongly needed".

- **Mechanism 4: Diverging priorities of governments**

In global internet governance, multilateral processes involve decision-making by governments and international organisations, whereas multistakeholder processes include a broader range of participants, such as private companies, civil society and technical experts. These approaches coexist and complement each other. As a general principle, even where global coordination is multilateral in nature, governments should still engage with the broader multistakeholder communities within their jurisdictions.

Some stakeholders interviewed during the preparation of this paper, as well as various authors, have pointed to a growing interest of national governments in influencing internet governance

---

766 IGF (2025). Policy Network on Internet Fragmentation: Output report. January 2025. Available at: https://intgovforum.org/en/filedepot_download/256/28579

767 Yang, L. (2023). Recommendations for metaverse governance based on technical standards. *Humanities and Social Sciences Communications*, 10(1), 1-10.

768 Yang, L. (2023). Recommendations for metaverse governance based on technical standards. *Humanities and Social Sciences Communications*, 10(1), 1-10.

769 McStay, A. (2023). The Metaverse: Surveillant Physics, Virtual Realist Governance, and the Missing Commons. *Philos. Technol.*, 36, 13 (2023). https://doi.org/10.1007/s13347-023-00613-y

770 McCarthy, K.(2022). Revitalising Global Internet Governance. Tony Blair Institute for Global Change. Available at: https://institute.global/insights/tech-and-digitalisation/revitalising-global-internet-governance

771 McStay, A. (2023). The Metaverse: Surveillant Physics, Virtual Realist Governance, and the Missing Commons. Philos. Technol. 36, 13(2023). https://doi.org/10.1007/s13347-023-00613-y

772 IGF (2025). Policy Network on Internet Fragmentation: Output report. January 2025. Available at: https://intgovforum.org/en/filedepot_download/256/28579

processes[773,774,775]. While this growing interest is not inherently negative, there are certain ways in which some national governments could increase the risk of governance becoming fragmented.

Risks of fragmentation in governance can emerge if a national government chooses to sideline other stakeholders[776,777,778]. For instance, some authors suggest that fragmentation can occur if a country pushes for technical standards that contradict other agreed-upon principles of internet governance (e.g. openness)[779,780]. Some literature also suggests that certain national governments might use next-generation technologies such as AI, quantum and next-generation devices as an argument for establishing new governance mechanisms and architectural solutions while suggesting that current standards and protocols are insufficient – even if this is not the case[781,782].

A number of authors cite examples in which state actors advocate for the expansion of the mandates of multilateral institutions (to increase the relative power of national governments in internet governance processes), even when multi-stakeholder institutions might be better suited or more appropriate for tackling specific issues[783,784,785]. Furthermore, insufficient collaboration and diverging views in the discussions surrounding internet fragmentation means that addressing these issues can be challenging. For instance, the IGF PNIF 2024 report states: "there remains a notable lack of intergovernmental engagement and focused dialogue on the matter [of fragmentation]. (..) Moreover, the term 'fragmentation' has become politicised, often used by countries to criticize each other's policies, further complicating productive discourse"[786]. The report further highlights that preventing fragmentation requires coordinated action by policymakers to prevent and address such risks.

As Web 4.0 and virtual worlds technologies advance, the fragmentation of internet governance could have several negative impacts. First, the fragmentation of internet governance could have a further **impact in terms of fragmentation at the technical and user experience levels**[787]. In turn, if the internet becomes splintered, this could create significant costs by disrupting global markets, raising barriers to trade, restricting the free flow of ideas, and jeopardising the supply of essential components for

[773] Dutton, W.H. (no date). *Multistakeholder internet governance?* Background paper for *World Development Report: Digital Dividends*. Michigan State University. Retrieved from: https://documents1.worldbank.org/curated/en/806901467994676420/pdf/102960-WP-Box394845B-PUBLIC-WDR16-BP-Multistakeholder-Dutton.pdf

[774] Broeders, D. (2016). *The public core of the internet: An international agenda for internet governance*. Amsterdam University Press.

[775] Voelsen, D. (2019). Cracks in the internet's foundation: the future of the internet's infrastructure and global internet governance. SWP Research Paper. Available at: https://www.ssoar.info/ssoar/bitstream/handle/document/65651/ssoar-2019-voelsen-Cracks_in_the_internets_foundation.pdf?sequence=1&isAllowed=y&lnkname=ssoar-2019-voelsen-Cracks_in_the_internets_foundation.pdf

[776] Digital Policy Hub (2024). Assessing the Near Future of Multi stakeholder Internet Governance. Available at: https://www.cigionline.org/static/documents/DPH-paper-Cramer.pdf

[777] Tony Blair Institute for Global Change (2021). The open internet on the brink: A model to save its future. Available at: https://institute.global/insights/tech-and-digitalisation/open-internet-brink-model-save-its-future

[778] European Parliament (2024). Internet governance: Keeping the internet open, free and unfragmented. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766272/EPRS_BRI(2024)766272_EN.pdf

[779] European Parliament, Directorate-General for Parliamentary Research Services, Perarnaud, C., Rossi, J., Musiani, F. et al. (2022). 'Splinternets' – Addressing the renewed debate on internet fragmentation, European Parliament. Available at: https://data.europa.eu/doi/10.2861/183513

[780] Hoffmann, S., Lazanski, D., & Taylor, E. (2020). Standardising the splinternet: how China's technical standards could fragment the internet, *Journal of Cyber Policy*, 5:2, 2020, 239-264. DOI: 10.1080/23738871.2020.1805482

[781] Radu, R., & De Gregorio, G. (2023). The new era of internet governance: technical fragmentation and digital sovereignty entanglements.

[782] Radu, R. (2021). Steering the governance of artificial intelligence: national strategies in perspective. *Policy and Society*, DOI: 10.1080/14494035.2021.1929728

[783] Digital Policy Hub (2024). Assessing the Near Future of Multi stakeholder Internet Governance. Available at: https://www.cigionline.org/static/documents/DPH-paper-Cramer.pdf

[784] Tony Blair Institute for Global Change (2021). The open internet on the brink: A model to save its future. Available at: https://institute.global/insights/tech-and-digitalisation/open-internet-brink-model-save-its-future

[785] European Parliament (2024). Internet governance: Keeping the internet open, free and unfragmented. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766272/EPRS_BRI(2024)766272_EN.pdf

[786] IGF (2025). Policy Network on Internet Fragmentation: Output report. January 2025. Available at: https://intgovforum.org/en/filedepot_download/256/28579

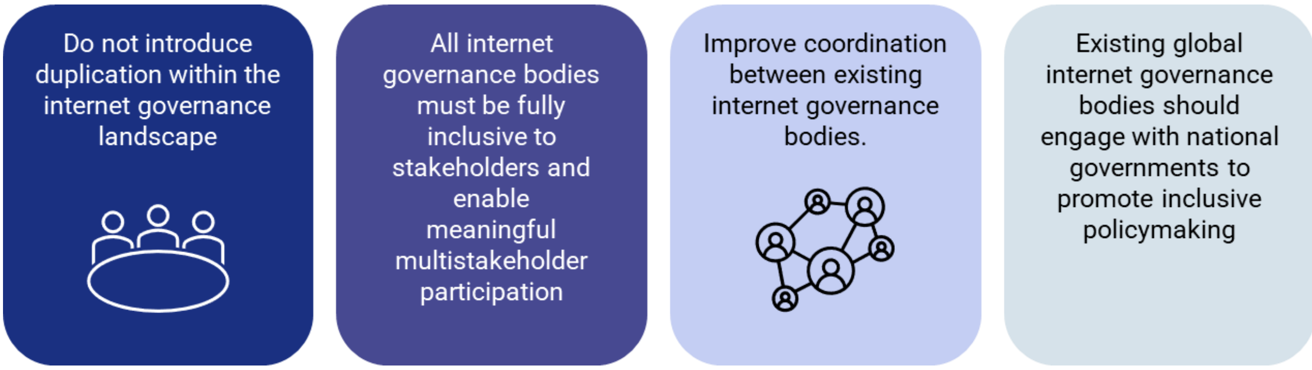
[787] IGFPNIF (2023). IGF Policy Network on Internet Fragmentation. Available at: https://intgovforum.org/en/filedepot_download/256/28194

digital infrastructure[788,789,790,791]. Moreover, if the underlying structure of the internet were to become fragmented, this would be extremely difficult to reverse[792].

Several key SDOs (the IEC, IEEE, ISO/IEC, ITU and W3C) have already initiated pre-standardisation efforts for virtual worlds. In addition, initiatives such as the Metaverse Standards Forum, the Khronos Group and the Open AR Cloud, which exist outside of SDOs, actively contribute to the development and refinement of standards relating to virtual worlds and Web 4.0 within established standards organisations[793].

Currently, the IGF PNIF serves as a platform for multistakeholder discussion on the risks of fragmentation of the internet and its governance[794]. It has outlined four recommendations for addressing the fragmentation of internet governance and coordination, as shown in the figure below. It is also worth noting that the role of IGF PNIF as a potential central platform for identifying risks of fragmentation and avenues to address them was discussed at IGF 2024[795].

Figure 17. IGF PNIF recommendations for addressing the fragmentation of internet governance and coordination



Source: IGF PNIF (2024)[796].

In conclusion, the fragmentation of internet governance risks undermining global standards, excluding stakeholders, and creating irreversible challenges as Web 4.0 and virtual worlds emerge. Preventing these negative impacts requires coordination, multistakeholder collaboration and effective intergovernmental dialogue.

788 European Parliament: Directorate-General for External Policies of the Union, Directorate-General for Parliamentary Research Services, Directorate-General for the Presidency, Anghel, S., Antunes, L. et al. (2023). *Future shocks 2023 – Anticipating and weathering the next storms*, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2861/88235

789 Voelsen, D. (2019). Cracks in the internet's foundation: the future of the internet's infrastructure and global internet governance. SWP Research Paper. Available at: https://www.ssoar.info/ssoar/bitstream/handle/document/65651/ssoar-2019-voelsen-Cracks_in_the_internets_foundation.pdf?sequence=1&isAllowed=y&lnkname=ssoar-2019-voelsen-Cracks_in_the_internets_foundation.pdf

790 Hoffmann, S., Lazanski, D., & Taylor, E. (2020). Standardising the splinternet: how China's technical standards could fragment the internet. *Journal of Cyber Policy*, 5(2), 239-264. https://doi.org/10.1080/23738871.2020.1805482

791 European Parliament (2024). Internet governance: Keeping the internet open, free and unfragmented. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766272/EPRS_BRI(2024)766272_EN.pdf

792 Tony Blair Institute for Global Change (2021). The open internet on the brink: A model to save its future. Available at: https://institute.global/insights/tech-and-digitalisation/open-internet-brink-model-save-its-future

793 European Commission (2023). Commission Staff Working Document accompanying the Communication on an EU initiative on Web 4.0 and virtual worlds: A head start in the next technological transition (SWD(2023) 250 final). Publications Office of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023DC0442

794 IGF (2024). Main Session Policy Network on Internet Fragmentation @IGF2024. Avoiding Internet Fragmentation: Understanding and Contributing to Operationalising the GDC Commitment Policy Network on Internet Fragmentation. Available at: https://www.intgovforum.org/en/content/policy-network-on-internet-fragmentation

795 IGF (2024). Main Session Policy Network on Internet Fragmentation @IGF2024. Avoiding Internet Fragmentation: Understanding and Contributing to Operationalising the GDC Commitment Policy Network on Internet Fragmentation. Available at: https://www.intgovforum.org/en/content/policy-network-on-internet-fragmentation

796 IGF (2025). Policy Network on Internet Fragmentation: Output report. January 2025. Available at: https://intgovforum.org/en/filedepot_download/256/28579

4.4. Policy and regulatory coordination

Web 4.0 technologies present novel challenges that often transcend traditional legal frameworks, particularly as the rapid advancement of digital technology outpaces existing governance systems. The Global Digital Compact acknowledges these challenges, noting how traditional tools such as public policy and legislation are too fragmented and slow to address the diverse impacts of technological innovation. Keeping pace with technological advances and tackling these new regulatory challenges requires unprecedented coordination and cooperation among stakeholders to fully unlock the benefits of the rapid digital transformation and to mitigate potential abuses[797]. WSIS Action Line 11 further highlights the significance of promoting policy coherence, and states that countries can collaboratively develop harmonised policies that create an enabling environment for ICT investment and development[798].

Research identifies several issues on which a commitment to applying and enforcing existing laws to virtual world technologies is needed. Examples include data protection and privacy laws, consumer rights, protection of children, anti-discrimination and accessibility laws[799]. However, as described above, the development by tech companies of virtual environments and augmented reality features and their integration into the companies' platforms gives rise to new issues around data ownership, intellectual property, user privacy, content moderation and interoperability, which also need to be addressed[800,801]. Moreover, respondents to the online consultation ranked legal jurisdiction as one of the most challenging governance and ethical issues involved in managing Web 4.0 and virtual worlds (see Annex 2).

The table below provides a general and non-exhaustive overview of potential legal uncertainties associated with the enhanced use of Web 4.0 technologies and virtual worlds.

Table 3. Potential legal uncertainties in Web 4.0

Category	Description
Enforcement of existing legislation	A lack of clear international legal frameworks for addressing disputes or agreements made in decentralised, borderless virtual environments presents challenges in determining the applicable legal jurisdiction for virtual interactions, conflicts and transactions.
Jurisdiction for virtual crimes	Tied to the cross-border nature of virtual crimes, as well as uncertainties in identity management and international legal cooperation, virtual environments pose challenges in terms of prosecuting virtual crimes across different jurisdictions. Issues may also arise from uncertainties regarding the legal responsibilities of platform operators in cases of virtual harassment, abuse or criminal activities.
Intellectual property	Web 4.0 presents challenges around copyright, trademarks and patents in virtual environments, including the unauthorised use of digital assets. A major concern in enforcing regulations relates to the difficulty of identifying intellectual property rights holders and detecting infringements.

[797] NETmundial. (2023). *Joint statement of the NETmundial+10*. Available at: https://netmundial.br/statement/joint-statement-of-the-netmundial10

[798] International Telecommunication Union (ITU) (2003). Plan of Action. Available at: https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!PDF-E.pdf

[799] Cox, S., Svarverud, E., Adams, J., Kadlubsky, A., Bernabe, R.D.L.C., & Baraas, R.C. (2024). D2.1: Mapping of the ethical issues in XR—Overview of ethical frameworks: A scoping review. In: *The Equitable, Inclusive, and Human-Centered XR Project (XR4Human)* (Deliverable No. 2.1). University of Oslo (UiO). Grant Agreement No. 101070155.

[800] Arbanas, J., Karp, M., McMillan, J., Arkenberg, C., Steinhart, M., & Dhameja, A. (2023). Considerations for regulating the metaverse: New models for content, commerce, and data. Deloitte Insights.

[801] Ladikas, M., Madeira, O., Hahn, J., Correa Pérez, M., Caplice, G., & Gerasymenko, A. (2024). D3.1: State-of-art in XR policy debates. In: M. Ladikas & M. Correa Pérez (Eds.), *The Equitable, Inclusive, and Human-Centered XR Project (XR4Human)* (Deliverable No. 3.1). Karlsruhe Institute of Technology (KIT). Grant Agreement No. 101070155.

Category	Description
Digital assets	The legal framework for virtual property ownership, trading and the transfer of digital assets is largely unclear. Similar uncertainties exist around consumer protection for purchases made in virtual environments, along with the taxation of virtual economic activities, including cryptocurrency and NFT transactions, as well as income earned through virtual work conducted.
Identity management	There are legal ambiguities surrounding legal status of digital avatars, their representation, and potential liability. Potential tensions may arise between the proponents of decentralised approaches and centralised or state-led approaches to identity management. Additional risks include potential fraud, impersonation and complex questions about avatar rights and responsibilities.
Avatar rights	There are uncertainties related to whether and how human rights considerations and existing legal frameworks ought to be applied to online representations of humans, such as avatars and digital twins. While some may argue that existing legislation can largely cover this dimension of virtual worlds, others may find new and tailored regulatory and value frameworks necessary.
Data privacy and protection	Web 4.0 technologies enable unprecedented levels of personal data to be collected through immersive platforms, capturing biometric data, behavioural tracking and detailed user interactions. This raises significant data privacy concerns, including company surveillance, intrusive monitoring, misuse of user data, and potential police surveillance. In addition, the borderless nature of virtual worlds complicates the application and enforcement of data protection laws.
Accessibility	Given the unique characteristics of Web 4.0 technologies, existing digital accessibility regulations may need to be broadened to enhance inclusivity. Moreover, the borderless nature of virtual worlds adds complexity to the consistent enforcement of accessibility standards across jurisdictions.
User health and safety	As the longer-term impacts of Web 4.0 and virtual worlds on health and well-being emerge, uncertainties remain around liability for potential physical and psychological harms to user health and safety caused by experiences in virtual worlds.

Source: Arbanas et al. (2023)[802]; Cox et al. (2024)[803]; Ladikas et al. (2024)[804];Othman et al. (2024)[805]; European Commission (2024)[806]; results of the stakeholder consultation.

Given the multifaceted regulatory challenges posed by virtual worlds and Web 4.0 technologies, the smooth and safe use of virtual worlds demands **global policy coordination** at various levels. At national level, several countries have adopted strategies to address some aspects of virtual worlds:

[802] Arbanas, J., Karp, M., McMillan, J., Arkenberg, C., Steinhart, M., & Dhameja, A. (2023). Considerations for regulating the metaverse: New models for content, commerce, and data. Deloitte Insights.

[803] Cox, S., Svarverud, E., Adams, J., Kadlubsky, A., Bernabe, R.D.L.C., & Baraas, R.C. (2024). D2.1: Mapping of the ethical issues in XR—Overview of ethical frameworks: A scoping review. In: *The Equitable, Inclusive, and Human-Centered XR Project (XR4Human)* (Deliverable No. 2.1). University of Oslo (UiO). Grant Agreement No. 101070155.

[804] Ladikas, M., Madeira, O., Hahn, J., Correa Pérez, M., Caplice, G., & Gerasymenko, A. (2024). D3.1: State-of-art in XR policy debates. In: M. Ladikas & M. Correa Pérez (Eds.), *The Equitable, Inclusive, and Human-Centered XR Project (XR4Human)* (Deliverable No. 3.1). Karlsruhe Institute of Technology (KIT). Grant Agreement No. 101070155.

[805] Othman, A., Chemnad, K., Hassanien, A.E., Tlili, A., Zhang, C.Y., Al-Thani, D., & Altınay, Z. (2024). Accessible Metaverse: A Theoretical Framework for Accessibility and Inclusion in the Metaverse. *Multimodal Technologies and Interaction*, 8(3), 21.

[806] European Commission: Directorate-General for Communications Networks, Content and Technology (2024). Zero-distance XR applications and services – Final report, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2759/0405

- South Korea's metaverse strategy focuses on developing the country's metaverse ecosystem, nurturing local talent and establishing ethical principles for safe virtual environments[807].
- Finland, a first mover in Europe, has collaborated with its domestic ecosystem to create a metaverse strategy that emphasises good governance, predictability and continuity[808].
- Japan's "Principles of the Metaverse" describe the principles and elements for a metaverse that adheres to democratic values and ensures safety and security, self-motivated and autonomous development and trustworthiness[809].
- China has outlined a Three-Year Action Plan (2023-2025) for the innovative development of its metaverse industry[810]. This strategy underlines active participation in international rulemaking for metaverse governance. It also seeks to harmonise international rules with those of China while promoting the internationalisation of Chinese metaverse enterprises.
- At regional level, the EU has adopted a strategy focusing on Web 4.0 and virtual worlds[811]. From a governance perspective, this strategy emphasises the importance of commitment to EU core values and promoting global standards for open and interoperable virtual worlds and Web 4.0. Despite these efforts, the lack of alignment between jurisdictions risks regulatory fragmentation, complicating the establishment of a cohesive and interoperable global metaverse framework.
- Elsewhere, the New South Wales State Government in Australia notes the risk of applying laws too speculatively, suggesting that policymakers and industry should first focus on developing responsible metaverse principles[812].

The private sector has also contributed to shaping discussions on governance. For instance, Meta's XRPRF (Extended Reality Policy Research Forum) seeks to mediate dialogue between industry, civil society and regulators. Meta's stated goal is to ensure that industry standards or regulations take into account the concerns of the civil rights and human rights communities, so that these technologies are built in a way that empowers everyone. Consistent with previous research on tech industry-funded regulation, the XRPRF is closely aligned with Meta's business interests, allowing it to broadly define the scope of governance[813].

In conclusion, effective global policy coordination for Web 4.0 technologies will require collaboration between governments, the private sector, civil society, academia, end users and other key stakeholders. By fostering inclusivity and alignment across jurisdictions, such efforts can support the development of safe, interoperable and innovative virtual worlds.

4.5. Summary of the gaps identified

The evolution towards Web 4.0 and virtual worlds presents both unprecedented opportunities and significant governance challenges. Internet governance institutions are increasingly confronted with complexities that extend well beyond the technical issues they were originally designed to address. As described in Chapter 2, the convergence of advanced AI, billions of interconnected devices, immersive

807 Ministry of Science and ICT (2021). *MSIT unveils strategies to lead the global metaverse market*. Available at: https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=621&searchOpt=ALL&searchTxt=

808 Business Finland (2023). *Metaverse Initiative by the Finnish Ecosystem*. Available at: https://www.digitalfinland.org/

809 Ministry of Internal Affairs and Communications of Japan (2023). Principles of the Metaverse. Available at: https://www.soumu.go.jp/main_content/000975017.pdf

810 Government of China (2023). *China's metaverse strategy*. Available at: https://www.gov.cn/zhengce/zhengceku/202309/content_6903023.htm. Translation available at: https://www.vdc-fellbach.de/en/knowledge-database/national-metaverse-strategies-worldwide/china-metaverse-strategy/

811 European Commission (2023). Towards the next technological transition: Commission presents EU strategy to lead on Web 4.0 and virtual worlds. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3718

812 Digital NSW (no date). Recommendations for developing governance. NSW Government. Available at: https://www.digital.nsw.gov.au/policy/metaverse-and-nsw-government/recommendations-for-developing-governance

813 Egliston, B., Carter, M., & Clark, K.E. (2024). Who will govern the metaverse? Examining governance initiatives for extended reality (XR) technologies. *New Media & Society*, 14614448231226172.

extended reality and breakthroughs in quantum computing is creating a very complex landscape. There is a need for a proactive, coordinated and inclusive approach to ensure that these emerging technologies are developed and deployed in a manner that upholds human rights and preserves the open, global and interoperable internet. To this end, several governance gaps can be identified.

- **The need for a future-oriented approach**: to fully harness the potential of Web 4.0 and virtual worlds technologies, a future-focused approach is needed. Advanced technologies are developing at an unprecedented pace and it is important to anticipate potential challenges, as well as the needs for coordination and the risks they may entail.
- **The need for stronger coordination among stakeholders within internet governance institutions**. Today's convergence of technologies is resulting in issues that span multiple layers, from underlying network protocols to application-level interactions. The emergence of various initiatives that target different aspects of Web 4.0 and virtual worlds further creates a risk of fragmentation. Divergent initiatives on Web 4.0 and virtual worlds could undermine the open, global and interoperable nature of the internet.
- **The need for stronger and more diverse multistakeholder participation**: while the multistakeholder approach is central to internet governance, it faces challenges in ensuring meaningful participation from diverse groups of stakeholders. Virtual worlds and Web 4.0 technologies will affect everyone. The involvement of diverse voices in governance processes is therefore especially pertinent, as Web 4.0 and virtual worlds could exacerbate some existing biases and harms. Furthermore, a range of stakeholders, including immersive technology developers, designers, start-ups and venture capital funds are involved in the development of virtual worlds and Web 4.0, and their perspectives are important to consider in governance discussions.
- **Gaps in technical knowledge**: the complexity of emerging Web 4.0 technologies can give rise to gaps in technical knowledge, which could prevent non-technical organisations from engaging effectively in governance discussions. This lack of expertise hinders civil society's ability to keep pace with rapidly evolving governance issues.
- **The need for policy coordination:** given the potential of virtual worlds and Web 4.0 to create highly immersive, real time and personalised environments, legal uncertainty exists around current legal concepts such as jurisdiction, data ownership, intellectual property and user safety.

Annexes

4.6. Annex 1: Methodology and stakeholder consultation approach

This background paper was developed using a combination of desk research and a stakeholder consultation that involved expert interviews, workshops and an online consultation. Altogether the project has received around 288 contributions from stakeholders[814]. The sections below elaborate our approach to conducting the online consultation, interviews, workshops, and our use of generative AI in preparing this document.

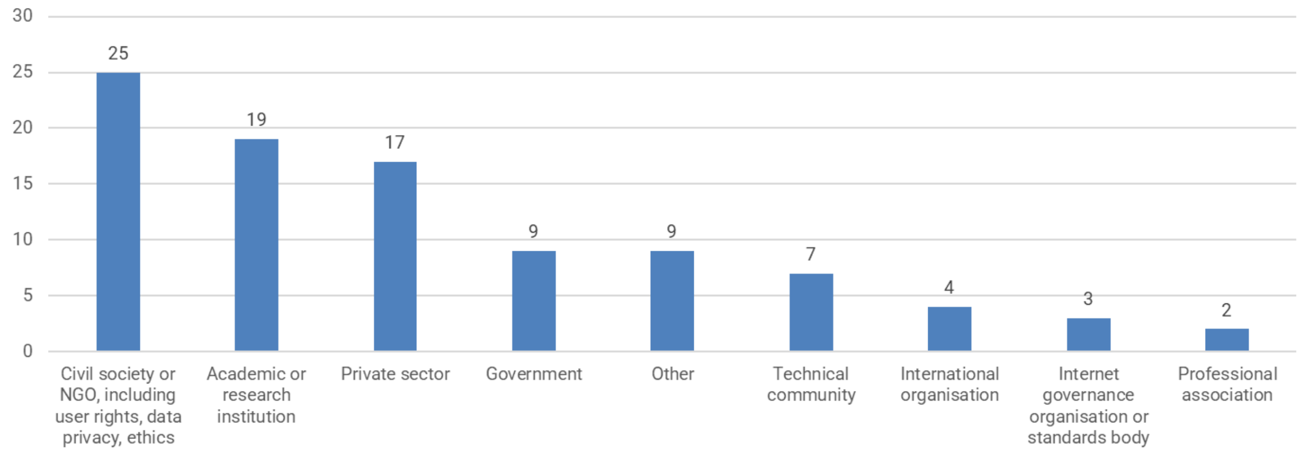
4.6.1. Online consultation

The online consultation was carried out in the form of a survey. The survey form was divided into three sections: the concept of Web 4.0; technical aspects of the evolution towards Web 4.0; and governance principles for Web 4.0 and virtual worlds. None of the questions in the online form were mandatory. Participants chose to answer those questions that were most relevant to them and which fit their expertise.

The online consultation was launched on 20 September 2024. By 20 December 2024, **95 responses had been received, of which 32 were partial and 63 were complete**. The online consultation was open to all stakeholders, and was disseminated widely via an e-mail campaign, social media, the project's website, and presentations at various events and meetings.

The figures below present a breakdown of survey respondents by stakeholder type and country.

Figure 18. Survey respondents by stakeholder type

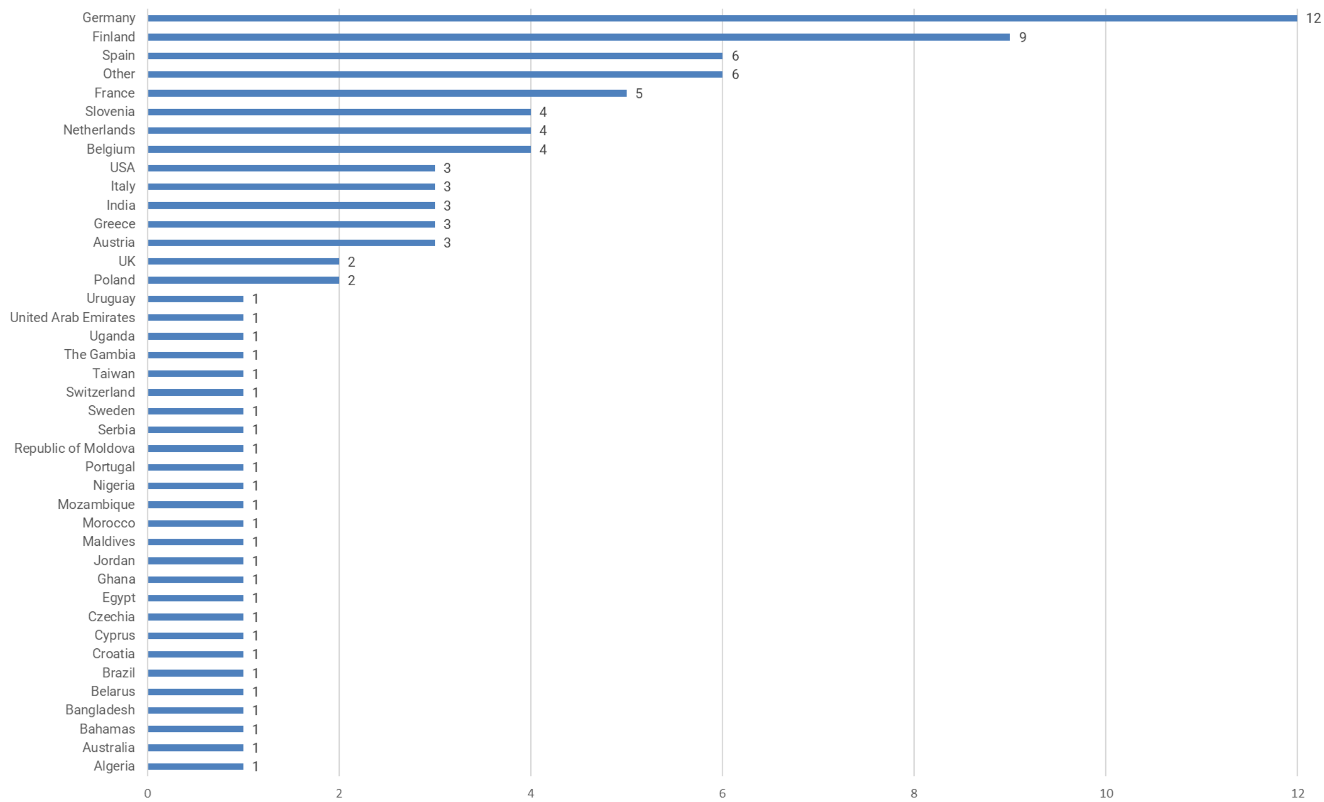


As shown in the figure above, civil society organisations and NGOs represent the largest group, with 25 respondents. Academic or research institutions follow with 19, while the private sector accounts for 17. Government representatives account for nine respondents, while seven respondents came from the technical community. International organisations and internet governance organisations or standards bodies were represented by seven respondents, while two respondents came from professional associations.

[814] In some cases, stakeholders participated with more than one contribution.

In terms of geographical representation, the largest numbers of contributions came from respondents from Germany, Finland, France and Spain. The figure below provides a detailed overview.

Figure 19. Survey respondents by country



4.6.2. Interview programme

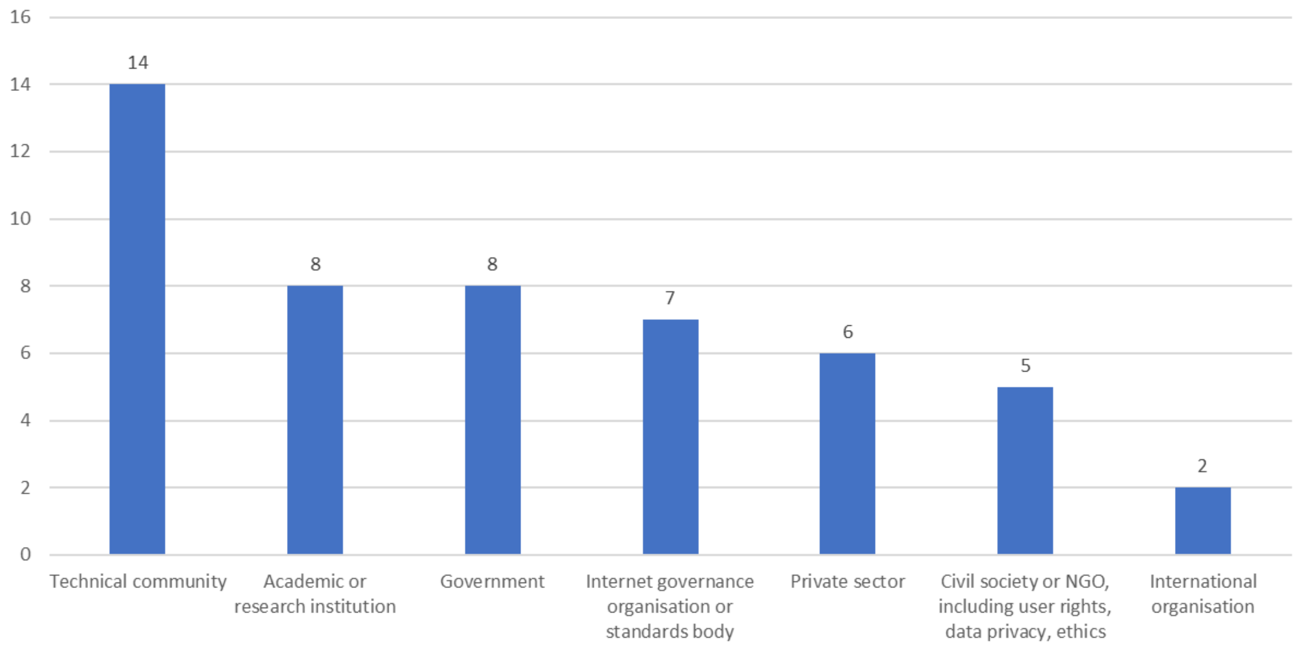
Between 9 October 2024 and 13 January 2025, the study team conducted interviews with stakeholders to gather qualitative insights. These interviews were conducted using a semi-structured format, and were divided into two types: policy-focused and technical. A total of 50 interviews were completed, a breakdown of which is shown in the table below. All interviews were conducted under Chatham House Rules.

Table 4. Interview programme overview

Category	***Number***
Interview invitations sent	98
Interviews conducted	50
Of which, technical	21
Of which, policy	29

The stakeholder group that provided the largest number of interviewees (14) was the technical community, while academic/research institutions and government categories each contributed eight participants. Experts from internet governance organisations or standards bodies participated in seven interviews, while the private sector accounted for six interviewees.

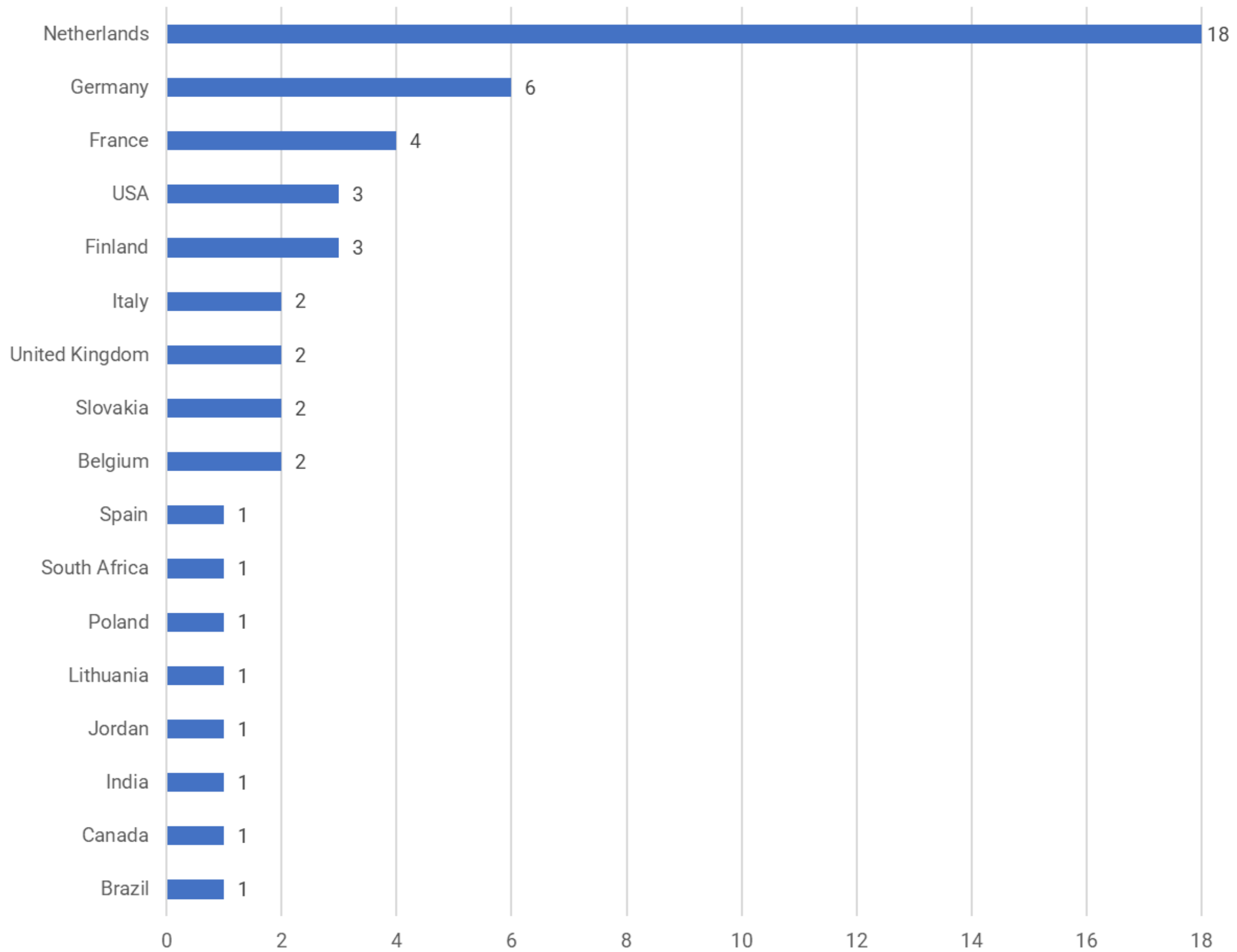
Figure 20. Interview breakdown by stakeholder type[815]



The figure below shows the distribution of interview participants by country. Interviewees came from Spain, South Africa, Poland, Lithuania, Jordan, Italy, India, Canada, Brazil, the United Kingdom, Slovakia, Belgium, the USA, Finland, France, Germany and the Netherlands. Interviewees were affiliated with various organisations, including ICANN, IETF, W3C, EuroDIG, Telefonica, Business Finland and Ofcom.

[815] Please note that there may be some overlap due to interviewees having affiliations with multiple organisations.

Figure 21. Interview breakdown by country



4.6.3. Workshops

To date, the study team has organised three online workshops, bringing together stakeholders from more than 20 countries to shape principles for the governance of Web 4.0 and virtual worlds (see table below).

Table 5. Workshops organised

Date	***Name***	***Number of participants***
22 October 2024	Workshop: Governance of Virtual Worlds and Web 4.0	58
24 October 2024	Workshop: Technology Challenges and Solutions for Web 4.0 and Virtual Worlds	41
26 November 2024	Workshop: Toward virtual world and Web 4.0 governance – action-oriented workshop	44

The outputs of these workshop have also been published on the study's web page[816] and in three separate workshop posts[817].

4.6.4. Use of generative AI

The preparation of this report was partially supported by genAI. This was used for tasks such as generating ideas and rewriting text, as well as streamlining and structuring specific sections. All contributions generated by genAI have been thoroughly reviewed, edited and integrated by the authors, in combination with their own research and insights. The authors take full responsibility for the final content and conclusions presented in this report.

4.7. Annex 2: Results of the online consultation

The online consultation was conducted between 20 September 2024 and 20 December 2024. In total, **95 responses were received, of which 32 were partial and 63 were complete**. The survey form was divided into three sections: the concept of Web 4.0; technical aspects of the transition to Web 4.0; and governance principles for Web 4.0 and virtual worlds. The sections that follow present an overview of the results of the online consultation.

Unless explicitly stated otherwise, the views expressed in the survey responses reflect the personal perspectives of individual stakeholders and should not be interpreted as representing the official positions of their respective organisations.

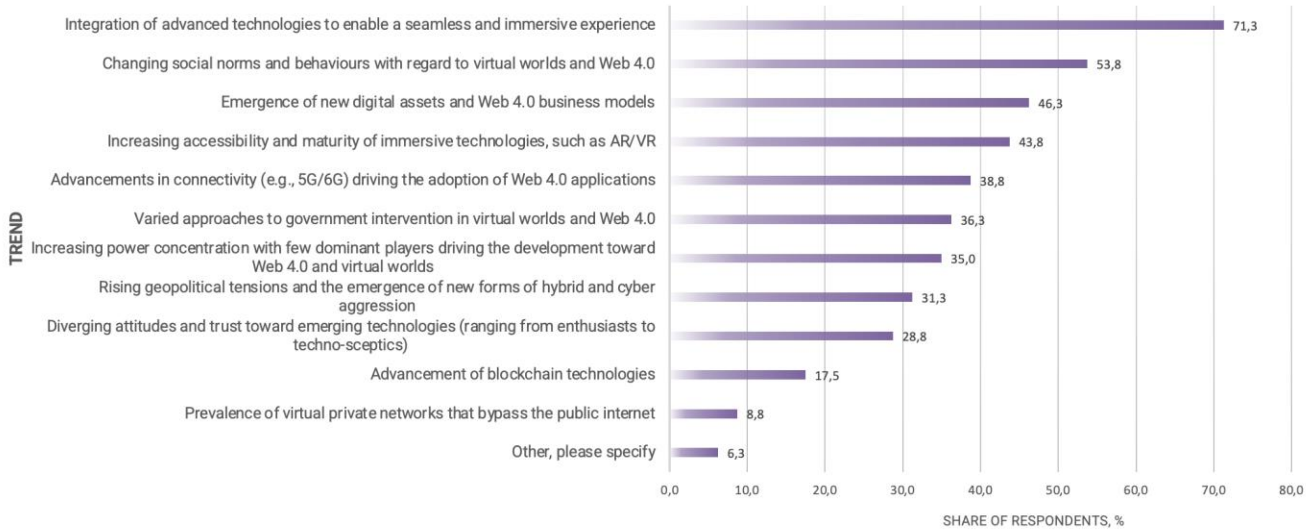
4.7.1. Technical considerations for Web 4.0

Among the **trends influencing the transition to Web 4.0**, 57 out of 80 respondents (71.3 %) identified the most impactful factor as being the integration of advanced technologies to enable a seamless and immersive experience (Figure 22). Changing social norms and behaviours related to virtual worlds and Web 4.0 were highlighted by 43 out of 80 respondents (53.8 %), while 37 out of 80 (46.3 %) noted the emergence of new digital assets and Web 4.0 business models as a key driver. The increasing accessibility and maturity of immersive technologies such as XR was emphasised by 35 out of 80 respondents (43.8 %), followed by advances in connectivity (e.g. 5G/6G) driving the adoption of Web 4.0 applications, which was selected by 31 out of 80 respondents (38.8 %). In contrast, only seven respondents (8.8 %) believed that the prevalence of virtual private networks bypassing the public internet would have a major impact.

[816] Available at: https://digital-strategy.ec.europa.eu/en/policies/web4hub

[817] Available at: https://digital-strategy.ec.europa.eu/en/library/workshop-principles-virtual-worlds-and-web-40-governance-22-october-2024; https://digital-strategy.ec.europa.eu/en/library/workshop-technology-challenges-and-solutions-web-40-and-virtual-worlds-24-october-2024; https://digital-strategy.ec.europa.eu/en/library/workshop-toward-virtual-world-and-web-40-governance-action-oriented-workshop-26-november-2024

Figure 22. Trends that will have the biggest impact on the internet's transition to Web 4.0

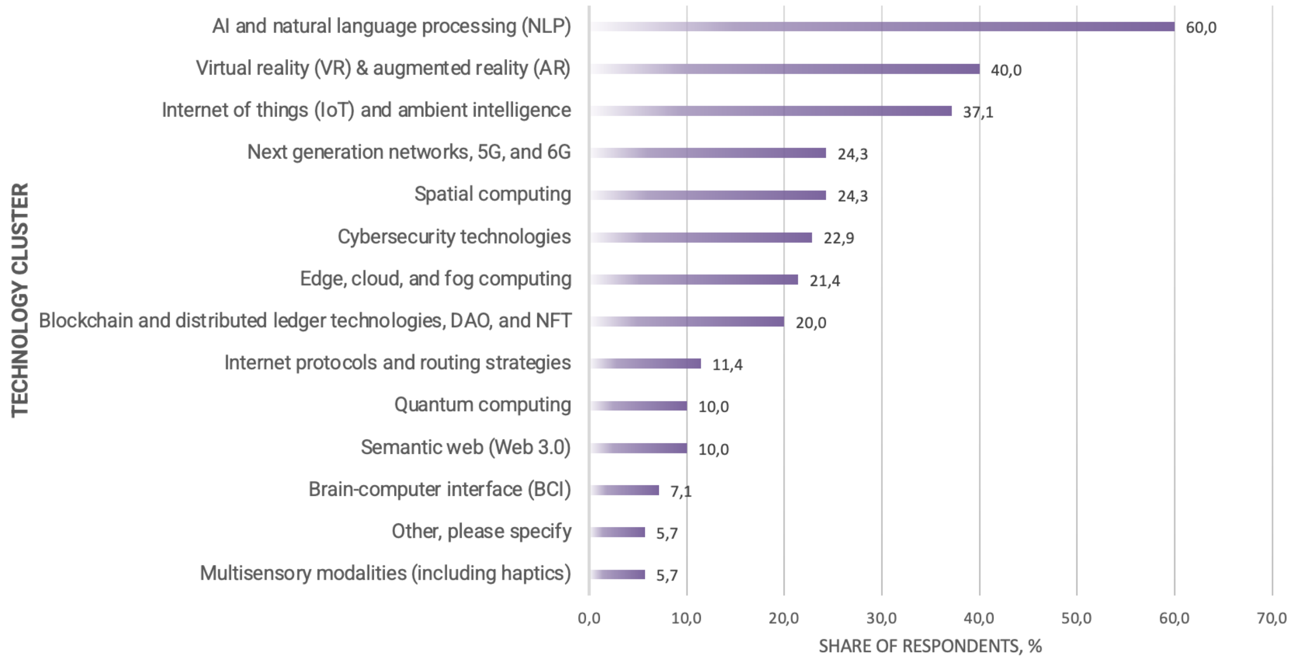


Source: online consultation; Q5 "The immersive and interactive features of virtual worlds are among the main drivers of the evolution of the internet towards Web 4.0. Which of the following trends, in your opinion, will have the biggest impact on the transition of the internet to Web 4.0? Please select up to 5 top trends".; N=80.

When asked about the **most critical technology clusters for Web 4.0 and virtual worlds**, 42 out of 70 respondents (60.0 %) highlighted AI and natural language processing (NLP) as being the most essential (). VR and AR were selected by 28 out of 70 respondents (40.0 %), while 26 out of 70 (37.1 %) pointed to IoT and ambient intelligence. Next-generation networks (5G and 6G) and spatial computing were each identified by 17 out of 70 respondents (24.3 %). In contrast, multisensory modalities, including haptics, were considered to be critical by only 4 out of 70 respondents (5.7 %). The same share selected other technology clusters, such as digital twins and wallets.

Figure 23). VR and AR were selected by 28 out of 70 respondents (40.0 %), while 26 out of 70 (37.1 %) pointed to IoT and ambient intelligence. Next-generation networks (5G and 6G) and spatial computing were each identified by 17 out of 70 respondents (24.3 %). In contrast, multisensory modalities, including haptics, were considered to be critical by only 4 out of 70 respondents (5.7 %). The same share selected other technology clusters, such as digital twins and wallets.

Figure 23. Technology clusters most critical to the evolution toward Web 4.0 and virtual worlds



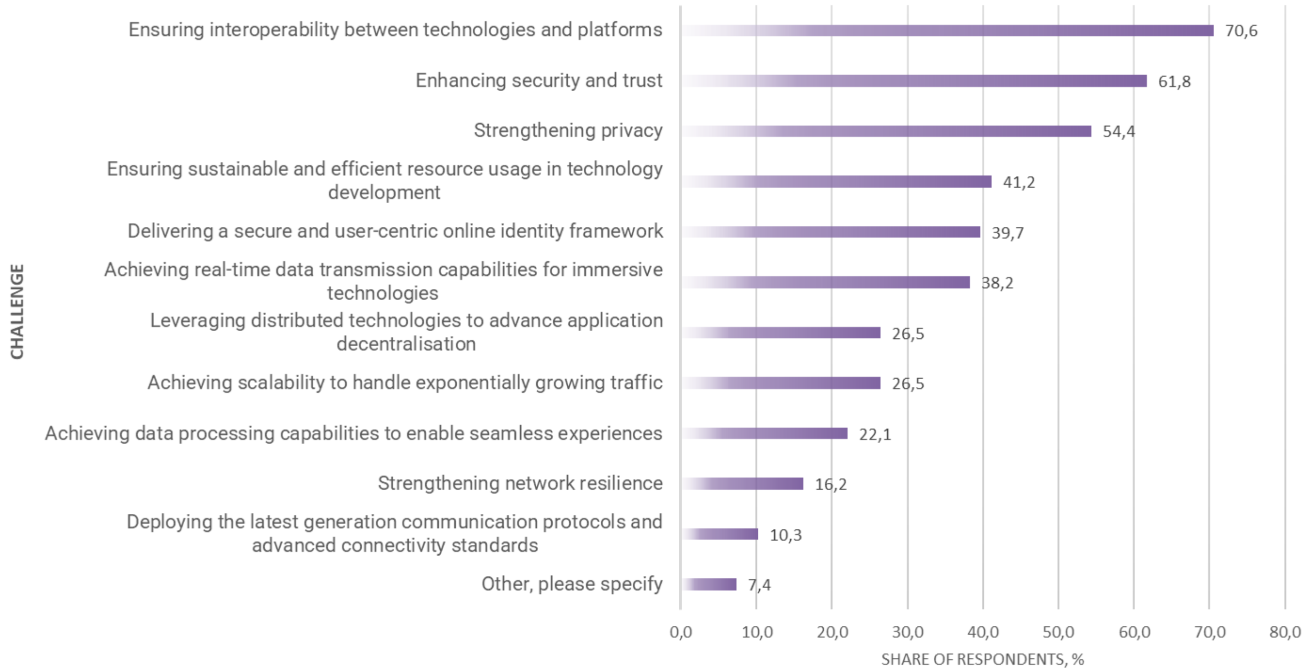
Source: online consultation; Q6 "Which Web 4.0 technology clusters are the most critical to the evolution toward Web 4.0 and virtual worlds? Please select the top 3."; N=70.

When asked to explain their choices, respondents emphasised the **interconnected nature of these technology clusters in enabling the transition to Web 4.0**. Many highlighted the way in which AI and NLP serve as fundamental enablers for creating intelligent, adaptive virtual environments and digital twins, while next-generation networks provide the essential infrastructure for real-time, low-latency experiences. In particular, respondents emphasised the crucial role of AR and VR technologies as primary interfaces for immersive experiences, noting their ability to bridge physical and digital spaces through spatial computing. Some respondents stressed that the evolution of Web 4.0 will be driven by the convergence of multiple technologies rather than isolated clusters, with IoT and ambient intelligence playing vital roles in integrating real-world data and enabling environmental interpretation.

In terms of the **most pressing challenges to achieving the transition to Web 4.0, given the current internet architecture**, interoperability between technologies and platforms emerged as the top challenge, chosen by 48 out of 68 respondents (70.6 %) (). Enhancing security and trust was noted by 42 out of 68 respondents (61.8 %), while 37 respondents (54.4 %) pointed to strengthening privacy. Ensuring the sustainable and efficient usage of resources in the development of technology was selected by 28 out of 68 respondents (41.2 %), while delivering a secure and user-centric online identity framework was highlighted by 27 respondents (39.7 %). At the other end of the spectrum, only seven respondents (10.3 %) viewed deploying the latest generation of communication protocols and advanced connectivity standards as a major challenge, while five respondents (7.4 %) specified other concerns.

Figure 24). Enhancing security and trust was noted by 42 out of 68 respondents (61.8 %), while 37 respondents (54.4 %) pointed to strengthening privacy. Ensuring the sustainable and efficient usage of resources in the development of technology was selected by 28 out of 68 respondents (41.2 %), while delivering a secure and user-centric online identity framework was highlighted by 27 respondents (39.7 %). At the other end of the spectrum, only seven respondents (10.3 %) viewed deploying the latest generation of communication protocols and advanced connectivity standards as a major challenge, while five respondents (7.4 %) specified other concerns.

Figure 24. Biggest challenges to achieving the transition to Web 4.0, given the current internet architecture



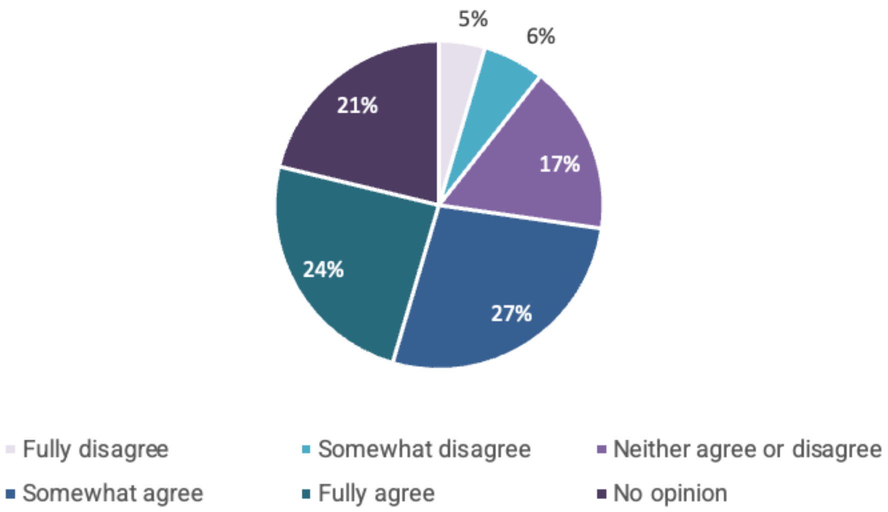
Source: online consultation; Q8 "Which of the below are the most challenging to achieve in the transition to Web 4.0, given the current internet architecture? Please select up to 5 top challenges".; N=68.

When asked for the reasoning behind their choices of top challenges, respondents emphasised that interoperability is fundamental to achieving Web 4.0's vision of a cohesive digital ecosystem, noting that it requires unprecedented collaboration among various stakeholders. They stressed that Web 4.0 **should not consist of isolated platforms, but should rather form an interconnected environment** in which users and companies can seamlessly use their data, avatars and assets across platforms. Several respondents highlighted how the increasing complexity of virtual environments raises the stakes for security and privacy concerns – especially given the quantity and sensitivity of the personal data involved in immersive experiences. On the technical front, respondents pointed to the challenges of managing exponentially growing internet traffic and ensuring sufficient infrastructure capacity, although some argued that the core challenge lies not in technical capabilities but the equitable distribution of existing resources. The need for a globally trusted identity system was also emphasised, with respondents noting that current identity frameworks are inadequate to the task of seamless navigation between virtual worlds and content. Some stakeholders underlined the importance of ensuring the sustainable and efficient use of resources, highlighting the substantial energy demands needed to run complex virtual environments and AI systems. Notably, some respondents shifted the focus to adoption challenges, arguing that the success of Web 4.0 will depend on making these technologies more accessible and user-friendly, to drive widespread engagement.

In the online consultation, 16 out of 66 respondents (24 %) fully agreed that the **TCP/IP stack and its underlying principles should be maintained to ensure continuity and stability**, while 18 respondents (27 %) somewhat agreed with this statement (). In contrast, 3 out of 66 respondents (5 %) expressed strong disagreement, whereas four people (6 %) somewhat disagreed. A total of 11 out of 66 respondents (17 %) were neutral on this topic (responding "neither agree nor disagree"), while 14 out of 66 (21 %) offered no opinion.

Figure 25). In contrast, 3 out of 66 respondents (5 %) expressed strong disagreement, whereas four people (6 %) somewhat disagreed. A total of 11 out of 66 respondents (17 %) were neutral on this topic (responding "neither agree nor disagree"), while 14 out of 66 (21 %) offered no opinion.

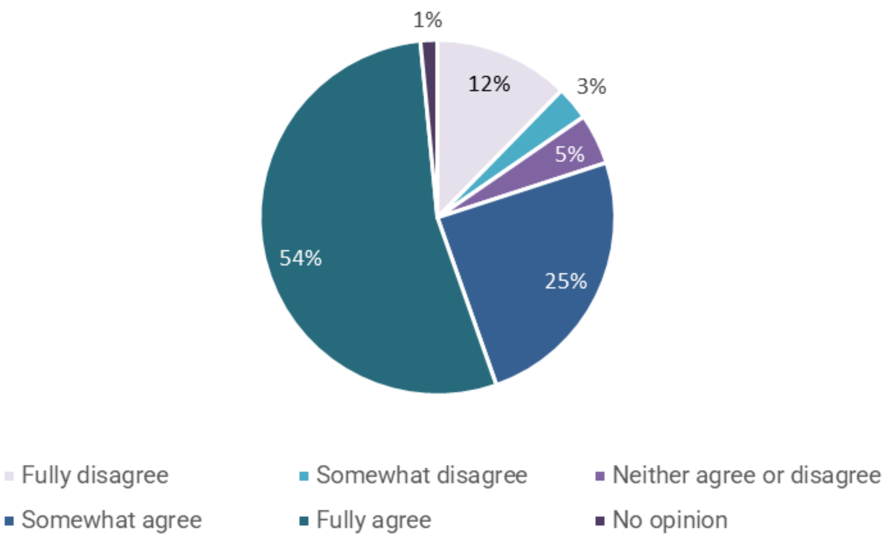
Figure 25. Opinions on whether the TCP/IP stack and its underlying principles should be maintained to ensure continuity and stability



Source: online consultation; Q10_1. "Please indicate to what extent you agree or disagree with the following statements on the transition to Web 4.0: The TCP/IP stack and its underlying principles should be maintained to ensure continuity and stability."; N=66.

The majority of respondents, 35 out of 65 (54 %), fully **supported preserving the distributed nature of the internet to ensure resilience and performance** (Figure 26). A total of 16 people (25 %) somewhat agreed with this statement. Conversely, 8 out of 65 respondents (12 %) expressed strong disagreement, while two respondents (3 %) expressed moderate disagreement. Three out of 65 respondents (5 %) were neutral (responding "neither agree nor disagree"), while 1 out of 65 (1 %) offered no opinion.

Figure 26. Opinions on whether the distributed nature of the internet should be preserved to ensure resilience and performance



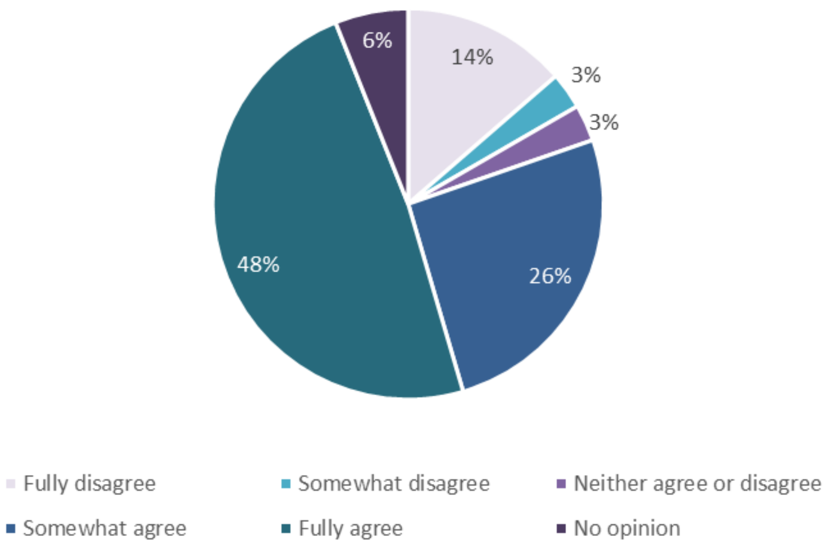
Source: online consultation; Q10_2. "Please indicate to what extent you agree or disagree with the following statements on the transition to Web 4.0: The distributed nature of the internet should be preserved to ensure resilience and performance.'"; N=65.

In the online consultation, 32 out of 66 respondents (48 %) fully agreed that **new concepts and protocols for Web 4.0 should promote openness and neutral access**, while 17 people (26 %) somewhat agreed with this statement (). Meanwhile, 9 out of 66 respondents (14 %) fully disagreed.

Only two people (3 %) somewhat disagreed with this statement. The same number of people adopted a neutral opinion (responding "neither agree nor disagree"). Four out of 66 respondents (6 %) offered no opinion.

Figure 27). Meanwhile, 9 out of 66 respondents (14 %) fully disagreed. Only two people (3 %) somewhat disagreed with this statement. The same number of people adopted a neutral opinion (responding "neither agree nor disagree"). Four out of 66 respondents (6 %) offered no opinion.

Figure 27. Opinions on whether new concepts and protocols enabling Web 4.0 should promote openness and neutral access

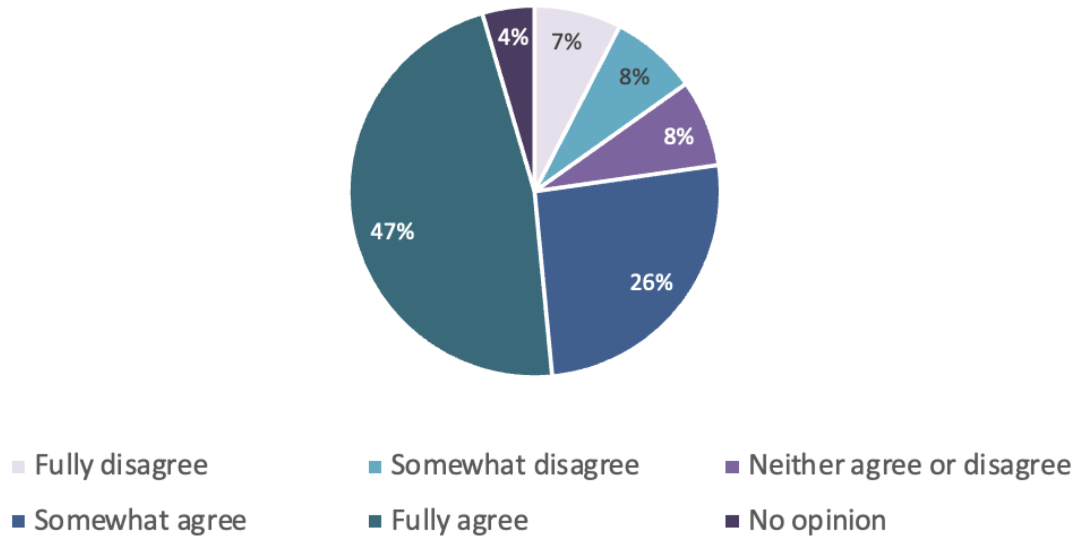


Source: online consultation; Q10_3. "Please indicate to what extent you agree or disagree with the following statements on the transition to Web 4.0: New concepts and protocols enabling Web 4.0 should promote openness and neutral access."; N=66.

The largest group of respondents, 31 out of 66 (47 %), fully agreed that **new concepts and protocols enabling Web 4.0 should promote universal accessibility**, while 17 respondents (26 %) somewhat agreed with this statement (Figure 28). Five respondents (7 %) fully disagreed with the statement, while the same number of respondents somewhat disagreed. Five respondents (8 %) expressed no strong preference regarding the statement (responding "neither agree nor disagree"), while three people (4 %) expressed no opinion at all on the issue.

Figure 28). Five respondents (7 %) fully disagreed with the statement, while the same number of respondents somewhat disagreed. Five respondents (8 %) expressed no strong preference regarding the statement (responding "neither agree nor disagree"), while three people (4 %) expressed no opinion at all on the issue.

Figure 28. Online consultation: Opinions on whether new concepts and protocols enabling Web 4.0 should promote universal accessibility, including in low-bandwidth conditions

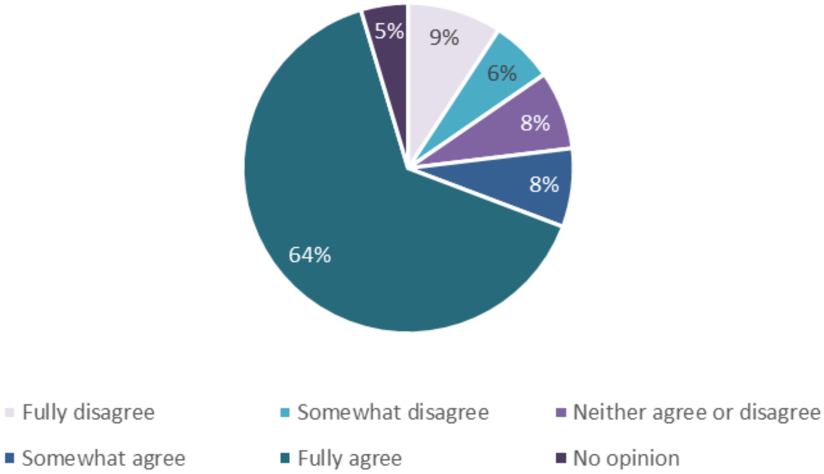


Source: online consultation; Q10_4. "Please indicate to what extent you agree or disagree with the following statements on the transition to Web 4.0: New concepts and protocols enabling Web 4.0 should promote universal accessibility, including in low-bandwidth conditions."; N=66.

The majority of respondents, 42 out of 65 (64 %), fully agreed that **network management and interactions in the development of Web 4.0 should be transparent**, while five respondents (8 %) somewhat agreed with the statement (Figure 29). Meanwhile, 6 out of 65 respondents (9 %) fully disagreed. Only four respondents (6 %) somewhat disagreed with this statement. Five respondents (8 %) expressed a neutral opinion (responding "neither agree nor disagree"), while the same number offered no opinion on the topic.

Figure 29). Meanwhile, 6 out of 65 respondents (9 %) fully disagreed. Only four respondents (6 %) somewhat disagreed with this statement. Five respondents (8 %) expressed a neutral opinion (responding "neither agree nor disagree"), while the same number offered no opinion on the topic.

Figure 29. Online consultation: Opinions on whether network management and interactions in the development of Web 4.0 should be transparent

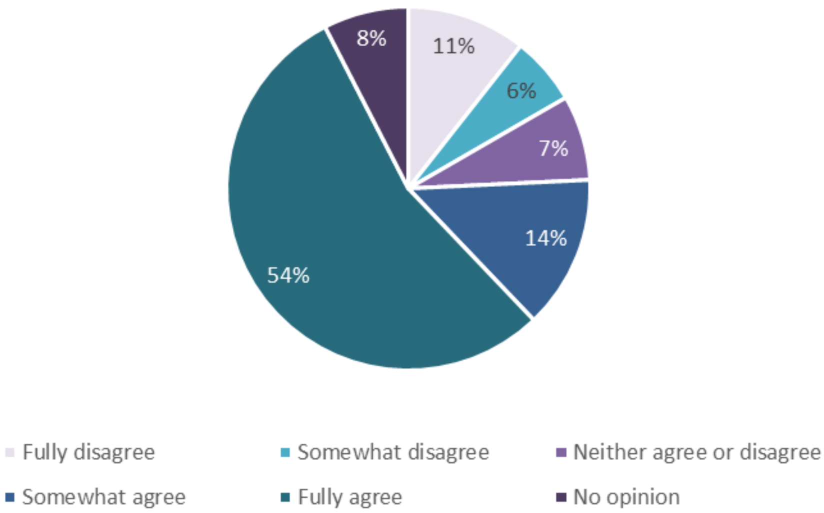


Source: online consultation; Q10_5. "Please indicate to what extent you agree or disagree with the following statements on the transition to Web 4.0: Network management and interactions in the development of Web 4.0 should be transparent."; N=65.

The majority of respondents, 36 out of 66 (54 %), fully agreed that **environmental sustainability should be a core consideration in the development of Web 4.0 infrastructure**, while nine respondents (14 %) somewhat agreed with this statement (). Seven respondents (11 %) fully disagreed with this statement, while four (6 %) somewhat disagreed. Five respondents (8 %) expressed no strong preference regarding the statement (responding "neither agree nor disagree"), while the same number offered no opinion at all on the topic.

Figure 30). Seven respondents (11 %) fully disagreed with this statement, while four (6 %) somewhat disagreed. Five respondents (8 %) expressed no strong preference regarding the statement (responding "neither agree nor disagree"), while the same number offered no opinion at all on the topic.

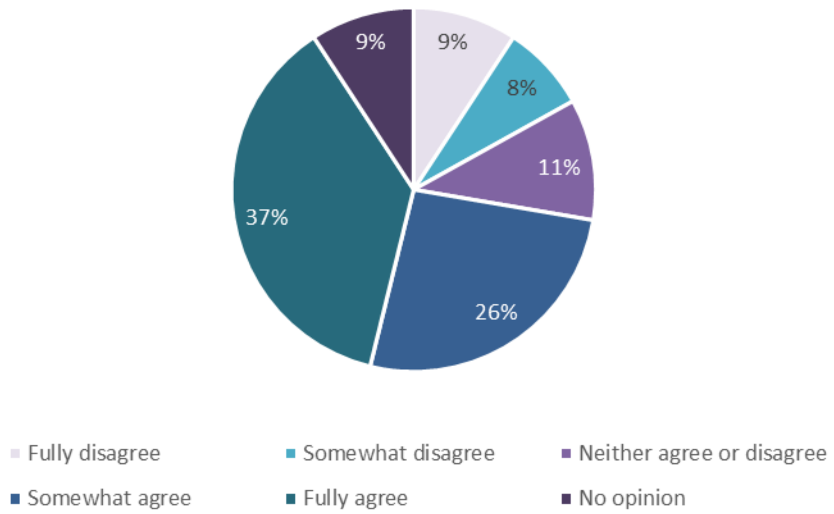
Figure 30. Online consultation: Opinions on whether environmental sustainability should be a core consideration in the development of Web 4.0 infrastructure



Source: Online consultation; Q10_6. "Please indicate to what extent you agree or disagree with the following statements on the transition to Web 4.0: Environmental sustainability should be a core consideration in Web 4.0 infrastructure development."; N=66.

The largest group of respondents, 24 out of 65 (37 %), fully supported **prioritising ease of deployment when introducing new features** (Figure 31). A total of 17 respondents (26 %) somewhat agreed with the statement. Conversely, 6 out of 65 respondents (9 %) fully disagreed, while five respondents (8 %) somewhat disagreed. A total of 7 out of 65 respondents (11 %) were neutral (responding "neither agree nor disagree"), while 6 out of 65 (9 %) offered no opinion.

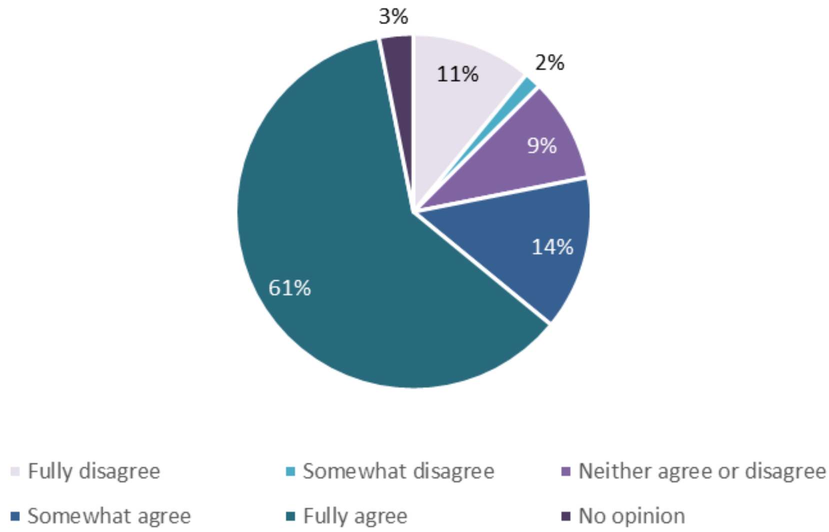
Figure 31. Online consultation: Opinions on whether ease of deployment should be prioritised when introducing new features such as APIs and protocols



Source: online consultation; Q10_7. "Please indicate to what extent you agree or disagree with the following statements on the transition to Web 4.0: Ease of deployment should be prioritised when introducing new features, such as APIs and protocols."; N=65.

In the consultation, the majority of respondents, 39 out of 64 (61 %), fully agreed that **Web 4.0 standards and protocols should be developed through a consensus-driven, inclusive and multi-stakeholder process**, while nine respondents (14 %) somewhat agreed with this statement (Figure 32). Meanwhile, 7 out of 64 respondents (11 %) fully disagreed. Only one respondent (2 %) somewhat disagreed with this statement. Meanwhile, six respondents (9 %) adopted a neutral opinion (responding "neither agree nor disagree"); 2 out of 64 respondents (3 %) expressed no opinion at all on this topic.

Figure 32. Online consultation: Opinions on whether Web 4.0 standards and protocols should be developed through a consensus-driven, inclusive and multi-stakeholder process

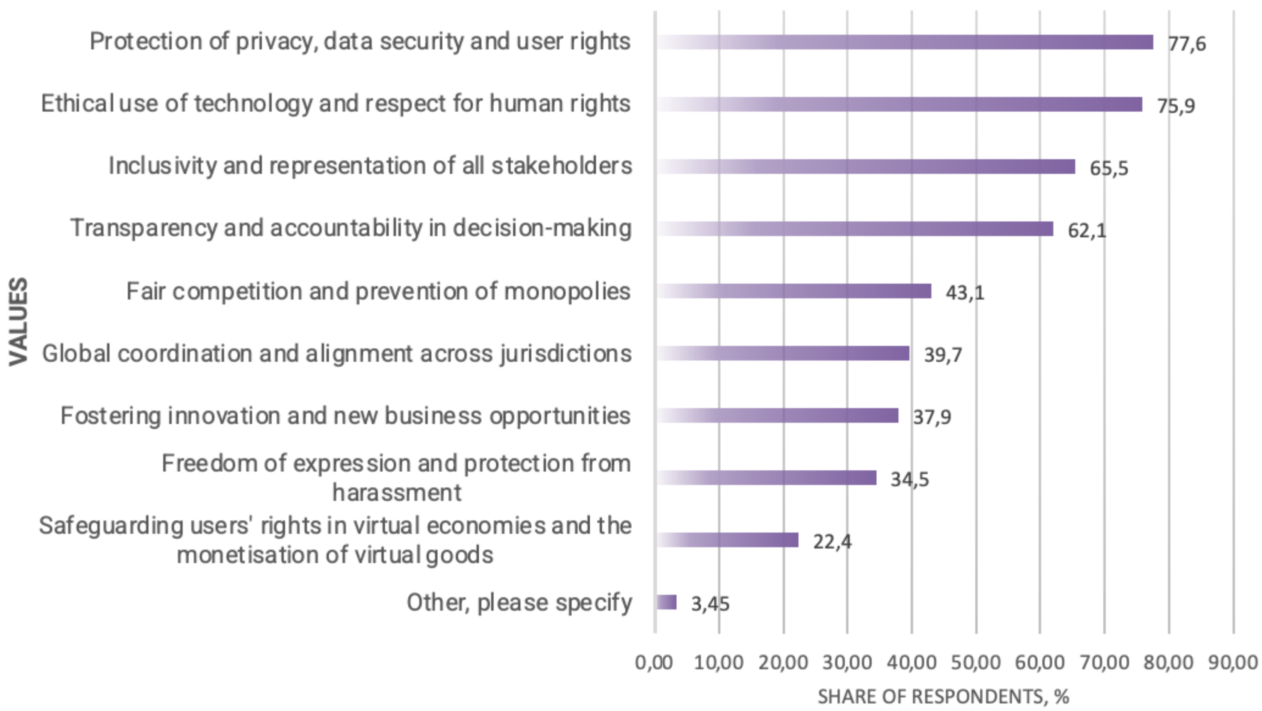


Source: online consultation; Q10_8. "Please indicate to what extent you agree or disagree with the following statements on the transition to Web 4.0: Web 4.0 standards and protocols should be developed through a consensus-driven, inclusive, and multi-stakeholder process."; N=64.

4.7.2. Values and principles for the development of Web 4.0

Among **the foundational values and principles that should underpin the governance of virtual worlds and Web 4.0**, 45 out of 58 respondents (77.6 %) identified the protection of privacy, data security, and user rights as the most impactful factor (Figure 33). Ethical use of technology and respect for human rights was highlighted by 44 out of 58 respondents (75.9 %), while 38 out of 58 (65.5 %) indicated inclusivity and the representation of all stakeholders. Transparency and accountability in decision-making was emphasised by 36 out of 58 respondents (62.1 %), followed by fair competition and the prevention of monopolies, which was selected by 25 out of 58 respondents (43.1 %). In contrast, only 13 out of 58 respondents (22.4 %) chose safeguarding users' rights in virtual economies and the monetisation of virtual goods as a major principle, while 2 out of 58 (3.4 %) indicated other values such as free speech and consideration of the psychological, social and political impacts of viewing and recording technologies.

Figure 33. Online consultation: Foundational values and principles that should underpin the governance of virtual worlds and Web 4.0.

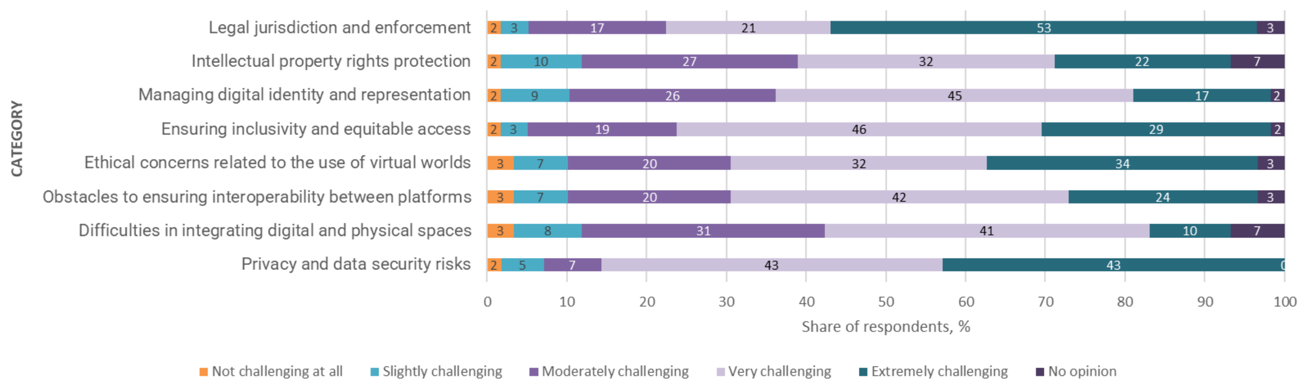


Source: online consultation; Q13. "What foundational values and principles should underpin the governance of virtual worlds and Web 4.0? Please select up to 5 principles that you think are most important."; N=58.

When asked to explain their choices of foundational values, respondents emphasised that **human rights principles should be the primary foundation for Web 4.0 governance**. Privacy and data security emerged as the top priority, with respondents stressing the critical importance of protecting user data in increasingly immersive and interconnected environments. Several respondents highlighted that Web 4.0 will not be a parallel virtual world, but rather a technology that closely links the physical and virtual realms – making it crucial that it applies the same values and protection mechanisms that apply in the physical world. Respondents stressed that transparency and accountability in decision-making are essential to building and maintaining user trust, while inclusivity will ensure that all voices – particularly those that are traditionally underrepresented – have a say in how these digital spaces evolve. Several respondents pointed to the European context, arguing that proactive involvement in shaping Web 4.0 from the outset is crucial to safeguarding European values in these emerging digital environments. On the economic front, respondents emphasised that the principles of fair competition are key to preventing monopolies that could stifle innovation. In particular, they highlighted the importance of creating opportunities for smaller players. Respondents also noted that while protecting core values such as privacy and ethical use is paramount, this should be balanced against the need to foster innovation and new business models. In addition, respondents emphasised the need for global coordination across jurisdictions to ensure consistent governance standards, to stimulate international participation and exchanges, and to effectively address challenges such as cybercrime, in an increasingly interconnected digital landscape.

The consultation also examined **governance and ethical challenges associated with virtual worlds**. Privacy and data security risks emerged as the most significant concern, with 48 out of 58 respondents (86 %) identifying it as either "very" or "extremely" challenging (Figure 34). Legal jurisdiction and enforcement followed closely, with 43 out of 58 respondents (74 %) rating it among the most serious levels of challenge. Obstacles to interoperability between platforms were also seen as a major issue, with 39 out of 58 respondents (66 %) finding these "very" or "extremely" challenging. Ensuring inclusivity and equitable access, as well as ethical concerns related to virtual worlds, were also highly rated, with 44 out of 58 respondents (75 %) and 39 out of 58 respondents (66 %) respectively highlighting them as major challenges. Managing digital identity and representation was considered "very" or "extremely" challenging by 36 out of 58 respondents (62 %), while the protection of intellectual property rights was ranked slightly lower, with 32 out of 58 respondents (54 %) identifying it as among the most serious levels of challenge. Difficulties in integrating digital and physical spaces were perceived as the least challenging aspect, with only 30 out of 58 respondents (51 %) choosing it as "very" or "extremely" challenging.

Figure 34. Online consultation: How challenging do you expect the following governance and ethical issues to be in managing virtual worlds and their integration with real-world systems?



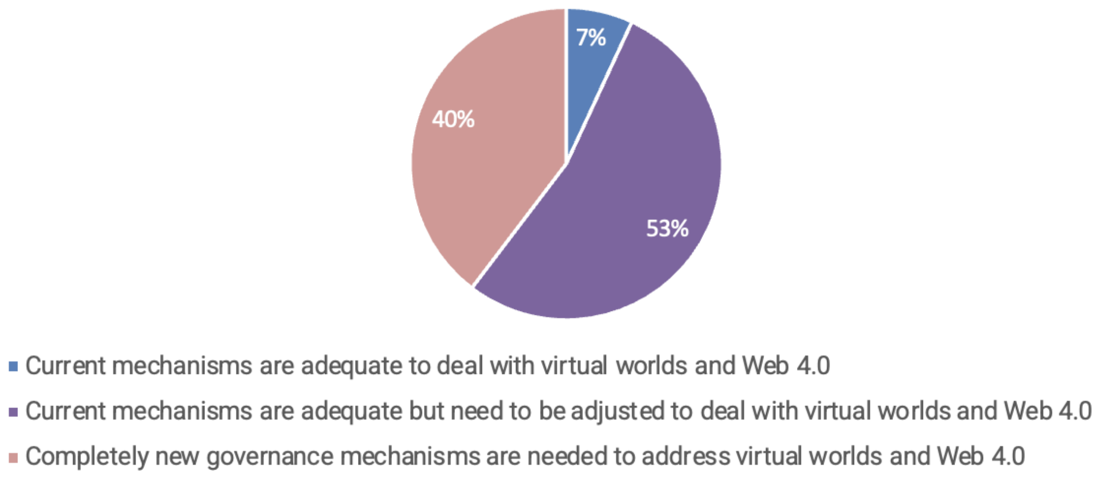
Source: online consultation; Q15. "As Web 4.0 evolves, how challenging do you expect the following governance and ethical issues to be in managing virtual worlds and their integration with real-world systems?"; N=58.

When asked to elaborate on the above challenges, respondents provided insights into why they regarded these issues as particularly complex in virtual worlds. They emphasised that privacy and data security concerns are heightened, due to the unprecedented volume and sensitivity of personal data these environments will collect, making them attractive targets for breaches. On the legal front, respondents highlighted that existing frameworks might struggle to adapt to these new "territories", with particular concerns being expressed with regard to cross-border jurisdiction and enforcement. The challenge of ensuring inclusivity and equitable access was highlighted as particularly crucial, with respondents expressing concerns about the development of immersive technology being concentrated in more developed countries, potentially deepening the digital divide. Respondents also noted specific regional challenges, such as the potential for authoritarian governments to exploit these technologies at the expense of human rights. With regard to interoperability, respondents emphasised that while seamless integration across platforms is essential for Web 4.0's success, achieving this would require unprecedented levels of collaboration between competing platforms, as well as the development of open standards. Ethical dimensions were described as being particularly complex, encompassing concerns about user treatment, risks of addiction, exploitation in the virtual economy as well as broader impacts on mental health and social dynamics. Some respondents stressed that addressing these challenges effectively would require not only the robust enforcement of existing legislation, but also new regulatory frameworks supported by adequately resourced oversight bodies.

The online consultation also explored the **suitability of current internet governance mechanisms for the future of Web 4.0 and virtual worlds**. The majority of respondents, 31 out of 58 respondents (53 %), indicated that while existing mechanisms are adequate, they require adjustments in order to effectively address emerging challenges (). Meanwhile, 23 out of 58 respondents (40 %) believed that entirely new governance mechanisms are necessary to regulate virtual worlds and Web 4.0. Only four respondents (7 %) considered current governance frameworks to be sufficient without any modifications.

Figure 35). Meanwhile, 23 out of 58 respondents (40 %) believed that entirely new governance mechanisms are necessary to regulate virtual worlds and Web 4.0. Only four respondents (7 %) considered current governance frameworks to be sufficient without any modifications.

Figure 35. Online consultation: The suitability of current internet governance mechanisms for the future of virtual worlds and Web 4.0

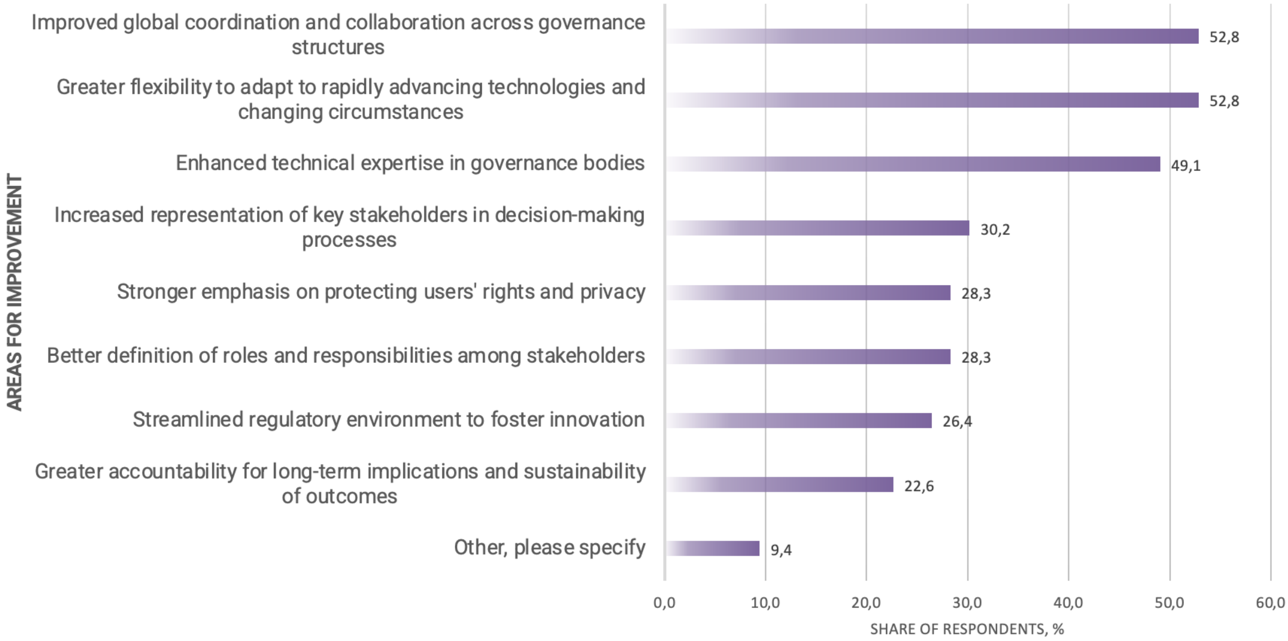


Source: online consultation; Q17. “Reflecting on the above challenges, how suitable are the current internet governance mechanisms for future virtual worlds and Web 4.0?”; N=58.

4.7.3. Governance of Web 4.0 and virtual worlds

Survey respondents highlighted the key adjustments they believed are required to **enhance internet governance mechanisms in light of the evolution towards Web 4.0**. The most commonly cited need was improved global coordination and collaboration between governance structures, with 28 out of 53 (52.8 %) of respondents supporting this (Figure 36). An equal proportion (also 52.8 %) stressed the importance of greater flexibility in adapting to advancing technologies and changing circumstances. Enhancing the technical expertise of governance bodies was also seen as a critical area for improvement, with 26 out of 53 (49.1 %) of respondents indicating that this believed this was necessary. In addition, 16 out of 53 respondents (30.2 %) called for the increased representation of key stakeholders in decision-making processes. A stronger emphasis on protecting users’ rights and privacy was supported by 15 out of 53 respondents (28.3 %), while the same percentage highlighted the need for roles and responsibilities to be better defined among stakeholders. Streamlined regulatory environments to foster innovation were backed by 14 respondents (26.4 %), and greater accountability for long-term implications and the sustainability of outcomes was supported by 12 respondents (22.6 %).

Figure 36. Online consultation: Adjustments needed to current internet governance mechanisms for a successful transition to virtual worlds and Web 4.0

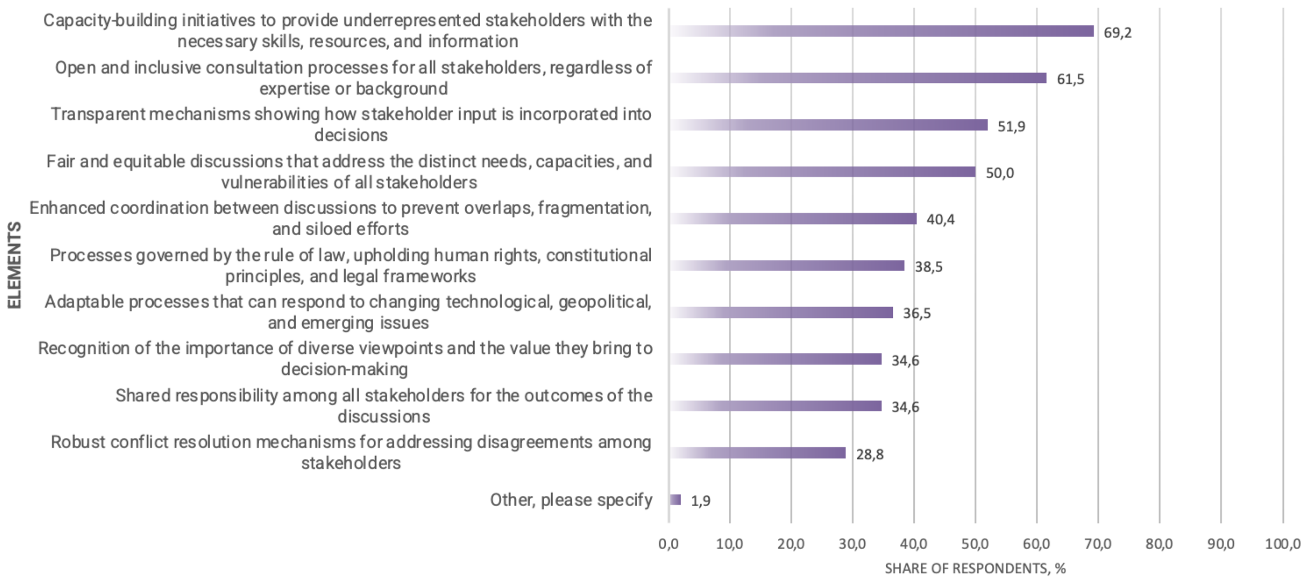


Source: online consultation; Q18. "With the above challenges in mind, what adjustments are needed to the current internet governance mechanisms for a successful transition to virtual worlds and Web 4.0? Please select the top 3 areas where improvements are necessary."; N=53.

When elaborating on these adjustments, respondents provided their perspectives on how internet governance mechanisms should evolve. They emphasised that decision-making processes must become more flexible and inclusive, ensuring that all stakeholders – especially those from underrepresented regions and sectors – have a meaningful voice in Web 4.0 governance. Many respondents highlighted the need for enhanced coordination through multiple channels, suggesting increased points of contact between government, market actors and NGOs. Indeed, one stakeholder specifically proposed the use of DAOs (decentralised autonomous organisations) as potential governance tools. On the technical front, respondents broadly agreed on the importance of developing standards and protocols for interoperability, security and digital identity to address the complexities of virtual worlds. Particular emphasis was placed on developing robust frameworks for decentralised identifiers and real-time data transmission. With regard to institutional arrangements, respondents suggested that existing internet governance organisations might need to expand their mandates to account for the specificities of Web 4.0, while also acknowledging that new governance bodies specifically focusing on Web 4.0 challenges might be necessary. Some respondents emphasised the need to foster stronger collaboration between such institutions to avoid the duplication of efforts and ensure a more cohesive approach to governance. Several respondents highlighted the importance of strengthening privacy and data protection policies for increasingly immersive and data-rich environments, suggesting enhancements to existing legal frameworks to account for new digital environments.

The survey also explored the most important elements in **ensuring adequate stakeholder representation in internet governance**. The highest priority was given to capacity-building initiatives to provide underrepresented stakeholders with the necessary skills, resources and information, as identified by 36 out of 52 respondents (69.2 %) (Figure 37). Open and inclusive consultation processes for all stakeholders were deemed important by 32 out of 52 respondents (61.5 %). Transparent mechanisms showing how stakeholder input is incorporated into decisions were identified by 27 out of 52 respondents (51.9 %), while fair and equitable discussions that address the distinct needs and vulnerabilities of stakeholders were supported by 26 respondents (50 %). Enhanced coordination between discussions to prevent overlaps and fragmentation was cited by 21 out of 52 respondents (40.4 %), followed by governance processes based on the rule of law and human rights principles, chosen by 20 out of 52 respondents (38.5 %). Adaptable processes that respond to geopolitical, technological, and emerging issues were highlighted by 19 out of 52 respondents (36.5 %). The recognition of diverse viewpoints in decision-making, as well as shared responsibility for discussion outcomes, were each supported by 18 out of 52 respondents (34.6 %). Lastly, robust conflict resolution mechanisms were considered important by 15 out of 52 respondents (28.8 %).

Figure 37. Online consultation: Most important elements in adequately representing stakeholders in internet governance processes



Source: online consultation; Q20. "How can stakeholders (users, governments, private sector, technical sector, small businesses, civil society, the public) be adequately represented in internet governance processes? Please select up to 5 most important elements."; N=52.

Turning to the **future of users' rights in Web 4.0**, respondents emphasised several critical areas in the evolution. Privacy and data protection emerged as a fundamental concern, with respondents envisaging more granular control over personal data through enhanced privacy settings and decentralised storage solutions. They stressed that the increasing merger of users' digital and physical lives should be safeguarded by stronger data protection standards, with privacy-by-design principles embedded from the earliest stages of development. Universal access was highlighted as another crucial dimension, with respondents emphasising the need to ensure that Web 4.0 technologies remain accessible and affordable across all regions. In particular, they noted the importance of including actors from the Global South, who have historically been excluded from digital governance processes. With regard to digital identity and self-expression, one respondent outlined a vision in which users could maintain multiple self-managed virtual identities with robust privacy protections, while also having greater control over their digital assets through blockchain-enabled ownership tracking. The complexity of freedom of expression in immersive environments was also addressed, with respondents suggesting the need for balanced approaches that combine user freedom with protection against harassment, potentially through decentralised moderation systems. Some respondents emphasised the need for transparent – potentially AI-driven – systems that protect users from algorithmic bias and discriminatory practices, while ensuring that users remain informed about how AI systems interact with and affect their digital experiences.

4.8. Annex 3: Results of the interview programme

Between 9 October 2024 and 13 January 2025, the study team conducted a total of 50 interviews. These interviews followed a semi-structured approach, and were adapted to the expertise and experiences of different stakeholder groups. The interviewees focused on three main areas: an overview of Web 4.0 technologies and their impact; technical considerations and principles for the development of Web 4.0 and virtual worlds; as well as key policy considerations and values. The interview questionnaire is provided in Annex 5.

Unless explicitly stated otherwise, the views expressed in the interviews reflect the personal perspectives of individual stakeholders and should not be interpreted as representing the official positions of their respective organisations.

All evidence from the interviews was incorporated into the Background and Prescriptive papers. A summary of the findings from the interview data is presented below[818].

4.8.1. Web 4.0 as an evolution of the internet

A key theme emerging from the interview programme was the perception that **Web 4.0 represents an incremental evolution of the current internet architecture, rather than a disruptive change**:

- Stakeholders emphasised that existing internet systems **are capable of enabling Web 4.0** technologies.
- For most use cases, stakeholders believed the architecture of the internet can adapt without the need for fundamental restructuring.
- Interviewees highlighted the importance of maintaining compatibility with legacy protocols and ensuring the accessibility of new technologies for all users.

When it comes to the definition of Web 4.0, some experts expressed mixed views on the concept, with some questioning its distinctiveness as a technological phase. Most interviewees agreed that Web 4.0 technologies primarily represent the convergence of multiple emerging technologies, including virtual worlds and XR experiences, ambient intelligence, IoT and the seamless blending of the physical and digital worlds.

4.8.2. Overview of technical considerations

Interviewees outlined some unique technical challenges and considerations presented by virtual worlds and Web 4.0 technologies. Among the issues most often mentioned as being critical to enabling immersive experiences were **bandwidth and latency**. Most stakeholders highlighted the significance of ensuring connectivity for the widespread adoption of Web 4.0 technologies, especially from a global perspective. Some stakeholders pointed to the potential of satellite integration to improve global connectivity, particularly in underserved areas. **Scalability** also emerged as a recurring theme, with stakeholders highlighting that while network evolution is underway, it must be able to accommodate increasing traffic demands. Some interviewees pointed to the adoption of IPv6, routing stability and domain name system (DNS) security as areas requiring further development.

Identity management emerged as another contentious issue, particularly in the context of cross-border regulation. Differences in approaches to end-user privacy and identity management are seen as critical areas in which a harmonised policy approach is needed to avoid fragmentation and abuses of end users' rights.

Interviewees stressed that **the integration of IoT and other connected devices requires improved local networking solutions**. Stakeholders noted that a shift towards more localised networking – less reliant on the broader internet – might be necessary in order to effectively manage the scale and diversity of IoT ecosystems.

The **immersive nature of Web 4.0** was identified as a key area requiring further exploration. Stakeholders raised concerns about the cognitive and health impacts of persistent virtual

[818] Disclaimer: this summary should be regarded solely as a summary of the contributions made by the interviewed stakeholders. It cannot in any circumstances be regarded as the official position of the Commission or its services. These interview responses cannot be considered as a representative sample of the views of the EU population.

environments and technologies, such as brain–computer interfaces – in particular, impacts associated with prolonged interaction and heightened immersiveness.

In addition, stakeholders discussed **hardware limitations**, in particular the size and wearability of VR and AR devices for the realisation of virtual worlds and Web 4.0. Many noted that miniaturisation, improvements in battery technology and enhanced sensor capabilities would be crucial in making Web 4.0 technologies more user-friendly. Some interviewees pointed to the limited processing capacity of wearables as a big bottleneck.

On a broader level, interviewees noted that questions remain regarding how the potential **decentralised governance models** for virtual worlds will interact with existing regulatory frameworks. Some interviewees argued that safeguarding against centralisation will be crucial. Even within blockchain ecosystems, some stakeholders warned that a small number of companies are beginning to dominate the space, leading to potential monopolisation within so-called decentralised networks. On a similar note, some interviewees highlighted the importance of considering how open-source technologies and frameworks enable and shape the evolution towards Web 4.0 technologies.

When it comes to the **suitability of current internet protocols**, most interviewees agreed that existing internet protocols are able to accommodate Web 4.0 technologies. While some argued that the existing protocols should be upgraded, most agreed that TC/IP is an important starting point. A few stakeholders argued for the need for new protocols to accommodate emerging technical demands, particularly for monitoring autonomous systems. Some interviewees raised concerns about the potential cross-border splitting of IP addresses, viewing this as one of the most pressing concerns for internet connectivity.

4.8.3. Overview of technical principles

When discussing the main technical principles that should be considered in the development of Web 4.0 and virtual worlds, interviewees highlighted **ensuring interoperability** as being central. Some interviewees cautioned that there is currently no unified interoperability framework or widely agreed-upon standards for virtual worlds and Web 4.0 technologies, raising concerns about fragmentation across different virtual world platforms.

Several interviewees pointed out that historically, major battles over technology standardisation have eventually led to industry convergence around a single standard. Some argued that Web 4.0 may follow a similar trajectory, with industry-driven standardisation emerging over time. However, others emphasised that pre-emptive action should be taken to establish open, transparent and interoperable standards in order to prevent dominant corporations from defining proprietary standards.

Most interviewees identified **identity management, digital asset management and connectivity standards** as key areas requiring standardisation. Open standards and open-source technology were highlighted as potential enablers of a more inclusive and decentralised Web 4.0 ecosystem.

4.8.4. Policy considerations

Most interviewees agreed that **existing internet governance structures provide a solid foundation for governing Web 4.0 technologies**. Nonetheless, interviewees highlighted some key areas of consideration in relation to Web 4.0 technologies. The complexity and scale of Web 4.0 raises significant questions about data privacy, accessibility, regulatory fragmentation, economic competition and geopolitical tensions. Importantly, stakeholders agreed that these topics are cross-cutting and should be discussed in joint forums rather than through isolated initiatives.

One of the most frequently mentioned concerns concerned **the volume and variety of data that would be collected and used by Web 4.0 technologies.** Many interviewees argued that this issue poses **new challenges for data governance, as well as user privacy and safety**. Questions remain about the use of behavioural, biometric and other sensitive types of data, especially in conjunction with AI systems.

The potential for algorithmic manipulation, commercial exploitation and the misuse of biometric identifiers adds to these concerns, making data protection frameworks a central issue for governance.

A related challenge stems from the **blurring of lines between virtual and real-world environments**. Interviewees noted that this introduces heightened concerns over manipulation and polarisation. Moreover, the enhanced hyper-personalisation that is possible under Web 4.0 could further exacerbate issues such as echo chamber effects, and could reduce exposure to diverse perspectives.

Accessibility and inclusion were also key considerations, with some interviewees warning that Web 4.0 could exacerbate inequalities by further entrenching differences between those who are able to access immersive environments, and those who cannot. This raises questions about who will be able to access and shape virtual environments, and whether new technologies will be designed with inclusivity in mind. A few interviewees stressed that ensuring equitable access to Web 4.0 technologies requires proactive governance measures such as affordability initiatives, inclusive design standards and regulatory interventions that prevent digital exclusion.

Interviewees pointed to **the use and application of AI** in virtual worlds and Web 4.0 as another significant area for consideration. Content generated by AI systems – in particular as it relates to AI-driven avatars – raises questions over transparency, control, ownership and accountability. In addition, the role of AI in moderating content, enforcing rules and shaping user experiences requires further examination.

Given the highly immersive nature of Web 4.0 technologies and the increased volume and sensitivity of the data collected, **an important consideration has emerged with regard to the concentration of power over technology infrastructure.** Interviewees saw this as a potential area of vulnerability requiring attention. They raised concerns about reliance on foreign-owned infrastructure, noting that such dependence is especially pronounced in the Global South. On a related note, some interviewees expressed concerns that non-democratic governments or large technology corporations could gain disproportionate control over the next iteration of the internet by acting as first movers in setting standards and launching initiatives in relation to virtual worlds. To this end, several interviewees stressed the importance of ensuring that discussions on the development of Web 4.0 and virtual worlds take place in multistakeholder settings.

Concerns were also raised about potential **regulatory fragmentation** and the risks of silos. Differences in regulatory priorities between global jurisdictions could lead to the development of incompatible legal frameworks, posing challenges for virtual worlds. Some interviewees questioned whether certain virtual spaces might become inaccessible to users in specific countries, due to regulatory restrictions. Furthermore, some interviewees raised concerns as to whether national regulations would be able to adapt to decentralised Web 4.0 infrastructures, particularly when identity frameworks, taxation rules, liability concerns and intellectual property protections vary significantly between regions.

From the perspective of market competition, interviewees highlighted concerns over the **concentration of power** and the dominance of Big Tech companies, which risks limiting market access for smaller players. Some expressed concerns that dominant corporations could shape Web 4.0 technology landscapes to benefit their own interests, making it harder for new entrants and decentralised initiatives to compete. Interviewees noted that while regulation is necessary, **overregulation** could also present a challenge – particularly for countries with limited regulatory capacity. Some interviewees pointed out that large firms often favour stricter regulation as a way to block smaller competitors, reinforcing the need for balanced policy approaches that protect innovation, competition and consumer rights.

Lastly, interviewees raised concerns about the **environmental impact of Web 4.0 technologies**, particularly in relation to the energy consumption of data centres, blockchain networks and hardware manufacturing. Some stakeholders noted the need for sustainability measures to mitigate these effects.

4.8.5. Policy principles and values

From a governance perspective, one of the policy principles expressed by interviewees was **the importance of leveraging existing policy frameworks to address the risks posed by Web 4.0 technologies**:

- Particularly within the EU, some stakeholders viewed existing legislation as well-positioned to manage these risks, while others stressed the need to assess whether current EU policy frameworks are sufficient to address the challenges of these emerging technologies.
- On a global scale, the focus remained on building upon ongoing internet governance efforts.
- However, some stakeholders underlined the challenge of ensuring these frameworks are applied effectively and consistently. Stakeholders advocated for enhanced monitoring of risks, ensuring compliance and reinforcing existing commitments.

Stakeholders emphasised the need for **coordinated international governance of Web 4.0 and virtual worlds**, warning against the risks of fragmented or competing initiatives. Experts stressed the importance of conducting Web 4.0 governance discussions within **multistakeholder settings**. Interviewees from various backgrounds highlighted the need to further uphold and strengthen existing multistakeholder frameworks. A collaborative approach involving governments, the private sector, civil society, academia and technical communities was viewed as essential for addressing the complexities of Web 4.0 effectively.

Some interviewees suggested that a global governance framework should be established, outlining the foundational governance principles for Web 4.0, including a focus on:

- Engaging **diverse stakeholders** to ensure that governance processes are inclusive.
- Fostering **collaboration and knowledge sharing** between regulatory bodies, industry and technical communities.
- Ensuring **transparency and accountability** in governance mechanisms.

The evolving roles of governance institutions were a key discussion point. Experts noted that emerging technologies often require an **"accommodation phase",** during which institutional mandates are reassessed and redefined. Strengthening inter-organisational dialogue and cooperation will be key to ensuring the coherence of governance across regulatory domains.

When discussing internet governance in light of Web 4.0 and virtual worlds, interviewees stressed the importance of enhancing coordination and adopting forward-looking perspectives in the multistakeholder approach. To this end, some interviewees advocated for the need to reinforce **an issues-based approach** to internet governance. This approach envisages a central "hub" as a platform for discussion and exchange, with dedicated workstreams led by the most appropriate organisations. The **IGF** was mentioned by interviewees as a potential central hub for shaping discussions on virtual worlds and Web 4.0 governance. Interviewees recognised the IGF's unique role in convening diverse stakeholders including governments, the private sector, civil society and technical communities, to engage in open dialogues on global internet governance.

However, a few interviewees raised concerns about whether the IGF's current structure is fit for purpose in addressing the emerging governance challenges posed by immersive technologies. Some interviewees suggested that the IGF should evolve to better align with the needs of stakeholders working with emerging technologies, ensuring that discussions move beyond traditional internet governance topics. While some emphasised the need for the IGF to expand its scope and focus on emerging regulatory gaps, others warned that overburdening the IGF with additional mandates could undermine its effectiveness.

To **enhance the IGF's role in Web 4.0 governance**, interviewees recommended strengthening regional IGF initiatives, ensuring that national and regional discussions feed into global processes, and developing clearer linkages between IGF discussions and policy implementation efforts. In addition, some interviewees proposed the creation of dedicated IGF working groups or subforums focusing on virtual worlds and immersive technologies, which would provide structured spaces for in-depth engagement on Web 4.0 governance challenges.

While some interviewees debated whether a separate multistakeholder forum should be created for Web 4.0 governance, several interviewees stated that the IGF remains one of the most inclusive platforms for discussions on digital governance. Most interviewees agreed that if the IGF is adapted to reflect the evolving digital landscape, it could play a significant role in coordinating governance approaches, fostering cooperation and bridging regulatory gaps in Web 4.0 governance.

Interviewees outlined several gaps or important considerations within the multistakeholder approach that should be addressed in light of the evolution towards Web 4.0:

- **Communication** is identified as a challenge, particularly in ensuring ongoing dialogue between all parties. A lack of consistent stakeholder definitions, as well as frequent turnover within technical communities, are cited as contributing factors.
- **The concentration of power** in the hands of private players is also identified as a critical risk. Stakeholders express concerns about the increasing influence of private companies, especially Big Tech companies, which could undermine accountability and reduce equitable participation in governance processes. A lack of redress mechanisms and enforced self-regulation further exacerbates this issue. Some stakeholders advocated for increased public involvement in oversight processes and the development of enforcement mechanisms that go beyond litigation. Technological tools could play a role in ensuring compliance and transparency without overburdening public authorities.
- Ensuring the **flexibility and ability of internet governance frameworks** to match the rapid pace of technological development was also highlighted. Stakeholders emphasised the need for anticipatory governance that is agile enough to respond to emerging challenges. Enhanced agility is critical to ensuring that governance structures remain relevant as Web 4.0 technologies continue to evolve.
- **Limited technical knowledge** represents a considerable barrier to participation, particularly for representatives of **civil society**. Stakeholders noted that a lack of technical knowledge and skills in relation to Web 4.0 technologies often limits meaningful engagement, especially in early-stage discussions that are often dominated by corporate actors. In addition, civil society groups frequently receive draft initiatives at later stages, reducing their ability to provide meaningful input. Time and resource constraints further limit their engagement, with civil society representatives often lacking the budgets to attend international forums. Stakeholders recommended improving outreach efforts to ensure broader and more equitable participation in governance discussions.
- While not specific to Web 4.0, **underrepresentation of the Global South** within established multistakeholder governance institutions continues to be a challenge. The hurdles faced by stakeholders from the Global South include travel costs, visa issues and limited access to international forums, preventing many from participating fully in governance processes. Virtual consultations have provided some relief, but stakeholders stress the need for localised approaches to governance. One interviewee also highlighted the issue of ensuring Global South or indigenous perspectives and values being reflected in major technologies.
- Interviewees also stressed the importance of collaboration in ensuring **human rights protections** in the governance of Web 4.0 technologies. Calls were made for strong safeguards and governance mechanisms to protect users from potential exploitation and ensure safe participation in digital environments.
- Some stakeholders noted that **blockchain governance** is not adequately addressed within current frameworks.
- Some stakeholders also called for **internet impact assessments** to evaluate how Web 4.0 technologies might affect core internet infrastructure and protocols.

In addition, concerns were raised about **overregulation** stifling emerging technologies. While governance is essential, stakeholders emphasised that regulation should not be so restrictive that it prevents companies from innovating, especially smaller players.

4.9. Annex 4: Survey questionnaire

4.9.1. Introduction

Thank you for taking part in shaping the future governance of Web 4.0 and virtual worlds!

While the governance of the internet is a rather stable although evolving environment, with established international institutions and a strong anchor in the multistakeholder model, the governance of the new frontier for the internet is still an unchartered territory. In its Communication on Web 4 and Virtual Worlds, the Commission acknowledged the need to engage internationally with the multistakeholder community on a broad scope of issues of technical and content nature. It also emphasised that this technological shift may involve new forms of governance, which require a reflection on the mandates of the current internet governance institutions and about whether other (existing or to be built) institutions should be involved.

The results collected through the form below will feed into the development **of guiding principles for the governance of virtual worlds and Web 4.0.** The draft principles will be discussed at the **global and multistakeholder** High Level Conference on Governance for Web 4.0 and virtual worlds, hosted by the European Commission and the Polish Presidency of the Council on 31 March–1 April 2025.

The form is divided into **three sections**: the concept of Web 4.0; the technical aspects of the transition to Web 4.0; and the governance principles for Web 4.0 and virtual worlds. Please note that the questions in the form **are not mandatory**. You can choose to answer the questions that are most relevant to you and fit your expertise. You can save your answers and come back to finish the form later. For more information about how we handle your data, please consult our privacy statement.

Before you start, we outline some working definitions of key concepts below.

- **Web 4.0:** the expected fourth generation of the World Wide Web. Using advanced artificial and ambient intelligence, the internet of things, trusted blockchain transactions, virtual worlds and XR capabilities, digital and real objects and environments are fully integrated and communicate with each other, enabling truly intuitive, immersive experiences, ***seamlessly blending the physical and digital worlds***[819].
- **Virtual worlds**: persistent, immersive environments, based on technologies including 3D and extended reality (XR), which make it possible to blend physical and digital worlds in real time for a variety of purposes such as designing, making simulations, collaborating, learning, socialising, carrying out transactions or providing entertainment[820].
- **Internet governance** refers to the institutions, rules, policies, standards, and practices that coordinate and shape the global internet's technical architecture and operation. Due to the internet's inherently distributed nature, governance involves a diverse range of actors who collaborate to address key issues related to the internet's infrastructure, usage and impact on society. This includes managing protocols, identifiers, routing, standardisation, security, privacy, and addressing broader societal impacts[821].
- **The multistakeholder approach** to internet governance: refers to the bottom-up, multistakeholder processes, ensuring the meaningful and accountable participation of all stakeholders alongside governments such as the private sector, civil society organisations, the technical community, academia and users. Core institutions that reflect the multistakeholder approach of internet governance are for example the Internet Governance

[819] The European Commission's communication on the EU initiative on Web 4.0 and virtual worlds
[820] Ibid.
[821] https://www.internetgovernance.org/what-is-internet-governance/

Forum (IGF), the Internet Corporation for Assigned Names and Numbers (ICANN) or the Internet Engineering Task Force (IETF).[822]

4.9.2. Online form questionnaire

Registration questions

1. Do you represent one or more organisations or act in your personal capacity (e.g. independent expert)?
    - I represent an organisation
    - I respond in a personal capacity
2. [*If answering in professional capacity*] Organisation that you represent
3. [*If answering in personal capacity]* Your affiliation
4. Full name
5. Email address
6. Which stakeholder group best represents you?
    - Academic or research institution
    - Civil society or NGO, including user rights, data privacy, ethics
    - Government
    - International organisation
    - Internet governance organisation or standards body
    - Private sector
    - Professional association
    - Sectoral association
    - Technical community
    - Other, please specify
7. [*If answering in a personal capacity*] In which country are you based?
8. [*If answering in a professional capacity*] In which country are the headquarters of your organisation located?
9. Why are the topics of virtual worlds and Web 4.0 governance relevant to you?
10. Would you like to be informed about study updates and pertinent events, including the High Level Conference on Governance for Web 4.0 and virtual worlds? [Y/N]

Main questions

On Web 4.0 and the general evolution of the internet

1. What does Web 4.0 mean for you? What are the key functions, benefits and pitfalls of Web 4.0 that you envisage?
2. The immersive and interactive features of virtual worlds are among the main drivers of the evolution of the internet towards Web 4.0. Which of the following trends, in your opinion, will have the biggest impact on the transition of the internet to Web 4.0? Please select the top 5.
    a. Integration of advanced technologies to enable a seamless and immersive experience
    b. Emergence of new digital assets and Web 4.0 business models

[822] https://netmundial.br/2014/netmundial-multistakeholder-statement/

   c. Increasing power concentration with few dominant players driving the development toward Web 4.0 and virtual worlds
   d. Diverging attitudes and trust toward emerging technologies (ranging from enthusiasts to techno-sceptics)
   e. Varied approaches to government intervention in virtual worlds and Web 4.0
   f. Changing social norms and behaviours with regard to virtual worlds and Web 4.0
   g. Rising geopolitical tensions and the emergence of new forms of hybrid and cyber aggression
   h. Advancement of blockchain technologies
   i. Increasing accessibility and maturity of immersive technologies, such as AR/VR
   j. Prevalence of virtual private networks that bypass the public internet
   k. Advancements in connectivity (e.g. 5G/6G) driving the adoption of Web 4.0 applications
   l. Other, please specify

On Web 4.0 technologies and internet architecture

3. Which Web 4.0 technology clusters are the most critical to the evolution toward Web 4.0 and virtual worlds? Please select the top three.
   a. AI and natural language processing (NLP)
   b. Spatial computing
   c. Internet of Things (IoT) and ambient intelligence
   d. Edge, cloud, and fog computing
   e. Next generation networks, 5G and 6G
   f. Blockchain and distributed ledger technologies, DAO, and NFT
   g. Semantic web (Web 3.0)
   h. Brain–computer interfaces (BCIs)
   i. Quantum computing
   j. Virtual reality (VR) & augmented reality (AR)
   k. Multisensory modalities (including haptics)
   l. Cybersecurity technologies
   m. Internet protocols and routing strategies
   n. Other, please specify

4. *[Follow up]* Please explain your reasoning for the selection of the top three technology clusters.

5. Looking at the current internet architecture, which of the below are the most challenging to achieve in the transition to Web 4.0? Please select the top 5.
   a. Achieving scalability to handle exponentially growing traffic
   b. Ensuring interoperability between technologies and platforms
   c. Enhancing security and trust
   d. Strengthening privacy
   e. Ensuring sustainable and efficient resource usage in technology development
   f. Delivering a secure and user-centric online identity framework
   g. Achieving data processing capabilities to enable seamless experiences
   h. Deploying the latest generation communication protocols and advanced connectivity standards
   i. Leveraging distributed technologies to advance application decentralisation
   j. Achieving real-time data transmission capabilities for immersive technologies
   k. Strengthening network resilience
   l. Others, please specify

6. [*Follow up*] Please explain your reasoning for the selection of the top 5.

7. Please indicate to what extent you agree or disagree with the following statements on the transition to Web 4.0, with 1 indicating "Fully disagree" and 5 indicating "Fully agree".
    a. The TCP/IP stack and its underlying principles should be maintained to ensure continuity and stability
    b. The distributed nature of the internet should be preserved to ensure resilience and performance
    c. New concepts and protocols enabling Web 4.0 should promote openness and neutral access
    d. New concepts and protocols enabling Web 4.0 should promote universal accessibility, including in low-bandwidth conditions
    e. Network management and interactions in the development of Web 4.0 should be transparent
    f. Environmental sustainability should be a core consideration in Web 4.0 infrastructure development
    g. Ease of deployment should be prioritised when introducing new features, such as APIs and protocols
    h. Web 4.0 standards and protocols should be developed through a consensus-driven, inclusive, and multi-stakeholder process
    i. Other, please specify

8. *[Follow up for principles ranked 1 – fully disagree; or 2 – somewhat disagree]* For the statements that you disagree with, please explain your reasoning.

9. What are the key steps that need to be taken to facilitate the transition to Web 4.0 in multi-stakeholder settings?

On the governance of VW and Web 4.0

10. What foundational values and principles should underpin the governance of virtual worlds and Web 4.0? Please select up to 5 principles that you think are most important.
    a. Transparency and accountability in decision-making
    b. Inclusivity and representation of all stakeholders
    c. Protection of privacy, data security, and user rights
    d. Ethical use of technology and respect for human rights
    e. Fair competition and prevention of monopolies
    f. Global coordination and alignment across jurisdictions
    g. Safeguarding users' rights in virtual economies and the monetisation of virtual goods
    h. Freedom of expression and protection from harassment
    i. Fostering innovation and new business opportunities
    j. Other, please specify

11. [*Follow up*] Please explain your reasoning for the selection of the top five.

12. [*Likert scale]* As Web 4.0 evolves, how challenging do you expect the following governance and ethical issues to be in managing virtual worlds and their integration with real-world systems? Please rate each on a scale of 1 to 5, where 1 is "Not challenging at all" and 5 is "Extremely challenging".
    a. Privacy and data security risks
    b. Difficulties in integrating digital and physical spaces
    c. Obstacles to ensuring interoperability between platforms
    d. Ethical concerns related to the use of virtual worlds
    e. Ensuring inclusivity and equitable access
    f. Managing digital identity and representation

g. Intellectual property rights protection
h. Legal jurisdiction and enforcement
i. Other, please specify

13. [*Follow up*] Please explain your reasoning for the most important challenges indicated above.

14. Reflecting on the above challenges, how suitable are the current internet governance mechanisms for the transition to virtual worlds and Web 4.0?
    a. Current mechanisms are adequate to deal with virtual worlds and Web 4.0.
    b. Current mechanisms are adequate but need to be adjusted to deal with virtual worlds and Web 4.0.
    c. Completely new governance mechanisms are needed to address virtual worlds and Web 4.0.

15. [*If "b" or "c" selected in Q14]* With the above challenges in mind, what adjustments are needed to the current internet governance mechanisms for a successful transition to virtual worlds and Web 4.0? Please select the top three areas where improvements are necessary.
    a. Better definition of roles and responsibilities among stakeholders
    b. Increased representation of key stakeholders in decision-making processes
    c. Enhanced technical expertise in governance bodies
    d. Greater flexibility to adapt to rapidly advancing technologies and changing circumstances
    e. Greater accountability for long-term implications and sustainability of outcomes
    f. Improved global coordination and collaboration across governance structures
    g. Stronger emphasis on protecting users' rights and privacy
    h. Streamlined regulatory environment to foster innovation
    i. Other, please specify

16. In relation to the top three areas of improvement you selected, what should change in the internet governance model to make it fit for the transition to virtual worlds and Web 4.0?
    a. In terms of the governance processes? (i.e. with respect to accessibility, fairness, effectiveness and efficiency of decision-making)
    b. In terms of the technical questions that need to be addressed? (i.e. with respect to standards and protocols, identifiers, security)
    c. In terms of policies? (i.e., with respect to privacy and data protection policies, and data access)
    d. In terms of existing institutions and platforms? (i.e. with respect to the sufficiency of their mandate)
    e. Other, please elaborate.

17. How can stakeholders (users, governments, private sector, technical sector, small businesses, civil society, the public) be adequately represented in such discussions? Please select the top 5 most important elements.
    a. Open and inclusive consultation processes for all stakeholders, regardless of expertise or background
    b. Capacity-building initiatives to provide underrepresented stakeholders with the necessary skills, resources, and information
    c. Enhanced coordination between discussions to prevent overlaps, fragmentation, and siloed efforts
    d. Transparent mechanisms showing how stakeholder input is incorporated into decisions
    e. Shared responsibility among all stakeholders for the outcomes of the discussions
    f. Recognition of the importance of diverse viewpoints and the value they bring to decision-making

   g. Robust conflict resolution mechanisms for addressing disagreements among stakeholders
   h. Processes governed by the rule of law, upholding human rights, constitutional principles, and legal frameworks
   i. Adaptable processes that can respond to changing technological, geopolitical, and emerging issues
   j. Fair and equitable discussions that address the distinct needs, capacities, and vulnerabilities of all stakeholders
   k. Other, please specify

18. Looking from the user perspective, how could users' rights (e.g. privacy and data protection, universal access, freedom of expression) change or evolve in Web 4.0/virtual worlds?
19. Are you aware of any existing initiatives or practices that are pertinent to the development of virtual worlds and Web 4.0 governance? These can be local, national or international. Examples can include coordination mechanisms, voluntary or mandatory obligations in relation to virtual worlds or Web 4.0.
20. [*question for file upload]* If you would like to upload any supporting files to the answers above, please do so.

4.10. Annex 5: Interview guide

4.10.1. Introduction

This **interview guide** contains information on the approach and content of interviews conducted for the purpose of exploring the topic of virtual worlds and Web 4.0 as part of the "Space for the Metaverse – Virtual World and the transition to Web 4.0" initiative (henceforth – "the initiative") implemented by PPMI and TNO for DG CNECT of the European Commission. The guide contains the following information:

- a description of the broader context
- a description of interview objectives and data protection measures
- interview topics
- contact information.

1. Broader context – virtual worlds governance and enabling 4.0 technologies

In line with EU's **strategy on Web 4.0 and virtual worlds**, the European Commission has launched the Pilot Project "A Space for the Metaverse – Virtual World and the transition to Web 4.0". Our objective is to assess the main developments in internet technologies that are relevant for Web 4.0 and virtual worlds. Furthermore, it will lay the groundwork for a global debate on the different aspects of the global governance of Web 4.0 and virtual worlds.

As part of this initiative, we are researching both policy and technological aspects of the Web 4.0. The interviews will play a vital role in that matter.

The results of this work will feed into the High Level Conference on the Governance of Web 4.0 and virtual worlds, co-organised by the European Commission and the 2025 Polish Presidency of the Council of the EU.

2. Interview objective & data protection

The interviews will serve as inputs for the technical and policy papers on the governance of Web 4.0 and virtual worlds.

The interviews aim to gather stakeholder positions to feed paper development. The target audiences include governments, technical community, civil society, academia and the private sector.

Please read our privacy statement for more information on how we handle your data for the purpose of this work.

3. Interview topics

The interview will cover the following topics:

- Understanding of Web 4.0 and virtual worlds
- Potential governance approaches for Web 4.0 and virtual worlds
- Risks associated with different governance approaches of Web 4.0 and virtual worlds
- Trends impacting the evolution toward Web 4.0 and virtual worlds (including technological and technical, market and economic, demographic and societal, political and geopolitical)
- The potential impacts of Web 4.0 and virtual world developments on internet architecture
- Key technologies enabling Web 4.0 and virtual worlds
- Synergies and potential conflicts of technology convergence for Web 4.0 and virtual worlds
- The appropriateness of existing standards and protocols for Web 4.0 and virtual worlds
- Key considerations and risks for realising Web 4.0 and virtual worlds (technological and technical, market and economic, demographic and societal, political and geopolitical)
- Principles for the development of Web 4.0 and virtual worlds

4. Key definitions

To ensure we are speaking about the same concepts, we share some guiding definitions below:

- **Web 4.0:** the expected fourth generation of the World Wide Web. Using advanced artificial and ambient intelligence, the Internet of Things, trusted blockchain transactions, virtual worlds and XR capabilities, digital and real objects and environments are fully integrated and communicate with each other, enabling truly intuitive, immersive experiences, ***seamlessly blending the physical and digital worlds***[823].
- **Virtual worlds**: persistent, immersive environments, based on technologies including 3D and extended reality (XR), which make it possible to blend the physical and digital worlds in real time for a variety of purposes such as designing, making simulations, collaborating, learning, socialising, carrying out transactions or providing entertainment[824].
- **Internet governance** refers to the institutions, rules, policies, standards, and practices that coordinate and shape the global internet's technical architecture and operation. Due to the internet's inherently distributed nature, governance involves a diverse range of actors who collaborate to address key issues related to the internet's infrastructure, usage and impact on society. This includes managing protocols, identifiers, routing, standardisation, security, privacy and addressing broader societal impacts[825].
- **The multistakeholder approach** to internet governance refers to bottom-up, multistakeholder processes that ensure the meaningful and accountable participation of all stakeholders alongside governments. Such stakeholders include the private sector, civil society organisations, the technical community, academia and users. Examples of core institutions that reflect the multistakeholder approach to internet governance include the

[823] European Commission's communication on the EU initiative on Web 4.0 and virtual worlds.
[824] Ibid.
[825] Available at: https://www.internetgovernance.org/what-is-internet-governance/

Internet Governance Forum (IGF), the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF)[826].

[826] Available at: https://netmundial.br/2014/netmundial-multistakeholder-statement/