Outcome document of the conference

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

Table of contents

List of abbreviations

AI	Artificial intelligence
API	Application programming interface
AR	Augmented reality
BCI	Brain-computer interface
DePIN	Decentralised physical infrastructure network
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
FEDAPP	Federative cloud-edge architecture
HTML	Hypertext markup language
GDC	Global Digital Compact
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and communications technology
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IoT	Internet of things
ITU	International Telecommunication Union
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
PET	Privacy-enhancing technology
PTSD	Post-traumatic stress disorder
QUIC	Quick UDP internet connections
RFC	Request for comments
RPKI	Resource public key infrastructure
SDO	Standards development organisation
SME	Small and medium-sized enterprise
SSI	Self-Sovereign Identity
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UN	United Nations
VR	Virtual reality
W3C	World Wide Web Consortium
WSIS	World Summit on the Information Society
XR	Extended reality

1. Introduction

This paper is a contribution to the global debate on high-level, foundational principles for the emerging fourth generation of the web. These principles, and the resulting recommendations, emerged from a **bottom-up, open and participatory stakeholder consultation exercise** undertaken in late 2024 and early 2025. The principles and accompanying recommendations presented in this paper were discussed and subject to rough consensus[1] during the **Global Multistakeholder High-Level Conference on the Governance of Web 4.0 and Virtual Worlds** co-hosted by the European Commission and the Policy Presidency of the Council of the European Union, which took place on 31 March – 1 April.

Participants discussed the opportunities and challenges associated with Web 4.0 and virtual worlds, their potential impacts on the internet, and how these could be addressed by different stakeholder groups and internet governance institutions. Stakeholders expressed a range of ideas. The principles and recommendations presented in this document are aligned with the principles identified by the European Citizens' Virtual Worlds Panel[2]. They are intended as a contribution to stakeholder discussions in the context of the World Summit on the Information Society (WSIS) +20 process and beyond. The accompanying **Background document** provides a detailed analysis of the technologies that underpin Web 4.0 and virtual worlds, along with related challenges, needs and governance implications[3]. It also provides a detailed account of the stakeholder consultation.

This paper draws on the **definition of Web 4.0** adopted by the European Commission: namely, that through the use of advanced artificial intelligence (AI) and ambient intelligence, the Internet of Things (IoT), trusted blockchain transactions, virtual worlds and extended reality (XR) capabilities, digital and real objects and environments are fully integrated and communicate with each other, enabling truly intuitive, immersive experiences that seamlessly blend the physical and digital worlds[4]. **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"[5].

In the context of this, the essential issue that requires stakeholders' attention and action is **the maintenance of an open, distributed and interoperable global internet** that upholds human rights, rather than allowing it to fragment into disconnected "splinternets". Given the evolution toward Web 4.0 and increasingly immersive virtual worlds, such a unified foundation is critical since, in order to function effectively, these advanced digital environments will require robust cross-border data flows, increased bandwidth capacity, ultra-low latency connections, enhanced security protocols and interoperable systems. Without a cohesive global internet infrastructure, the promise of seamless virtual experiences and intelligent web services could be severely limited by technical barriers and conflicting governance frameworks, potentially leading to isolated digital ecosystems that undermine both innovation and human connection.

In view of this, the paper presents two sets of principles:

---

[1] This document reflects the prevailing sentiment which does not imply complete or unanimous agreement on all nuances of this paper among all participants.

[2] European Citizens' Panel on Virtual Worlds (2023). Documents and reports, available at https://citizens.ec.europa.eu/virtual-worlds-panel_en

[3] The Background document elaborates on challenges to internet governance that underpin the principles listed in this paper, building on both the stakeholder consultation and an extensive literature review. It presents the key issues, as well as concrete data and evidence on these challenges. Moreover, it also describes considerations with regard to internet governance, such as those relating to institutional mandates, existing and emerging governance models, multistakeholder involvement, and policy and regulatory coordination.

[4] 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, 11.7.2023. COM(2023) 442/final. Available at: https://digital-strategy.ec.europa.eu/en/library/eu-initiative-virtual-worlds-head-start-next-technological-transition

[5] Ibid.

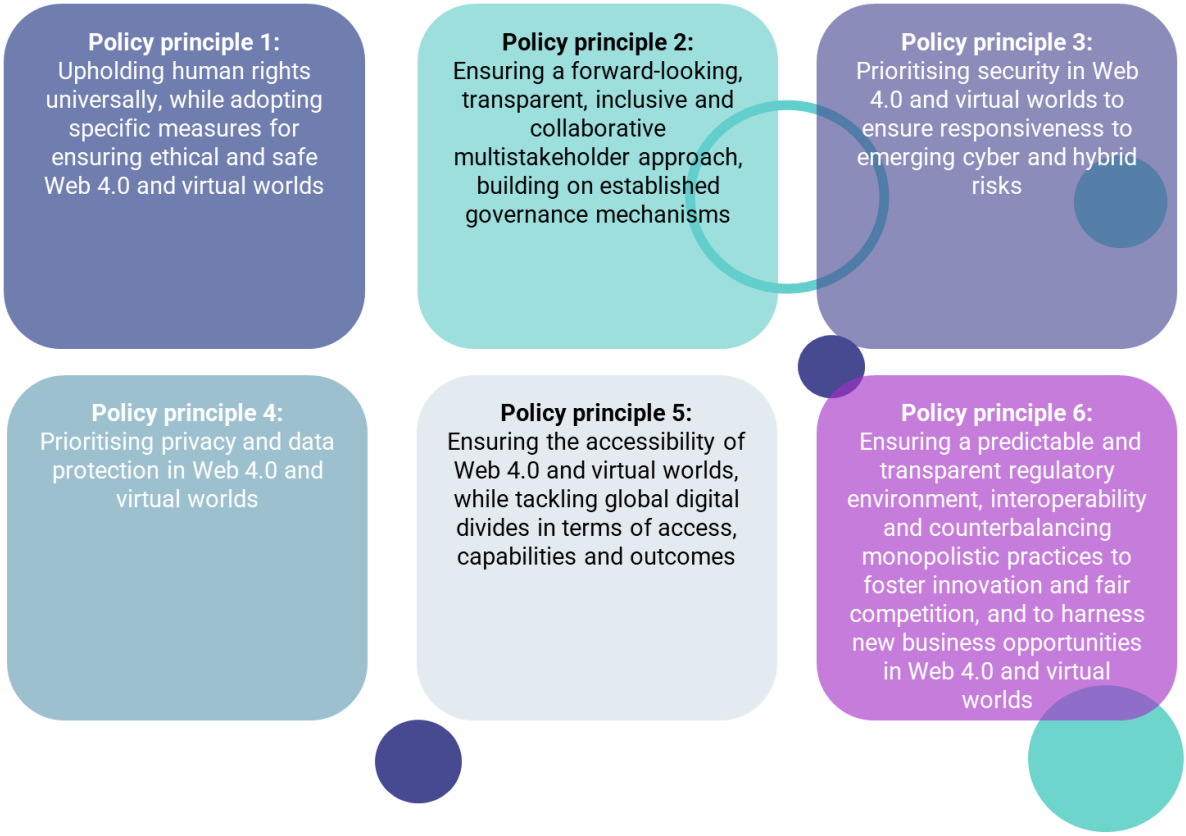
- **Policy principles.** These focus on the foundational values, rights and approaches that have so far shaped the governance of the internet, and which should be reinforced to guide it as the internet facilitates a future Web 4.0 and virtual worlds.
- **Technical principles.** These are interlinked with the policy principles and focus on the design, operational and technological features that are essential to maintaining the foundation of an open and interoperable global internet.

The **recommendations** presented in this document focus on the governance process and include measures to embed Web 4.0 and virtual worlds within a framework of the ethical, inclusive and well-coordinated governance of the internet.

2. Policy principles

The policy principles presented here outline the values, rights and approaches that have so far shaped the governance of the internet, and which should be reinforced in response to the development of Web 4.0 and virtual worlds. These principles include upholding human rights; ensuring a forward-looking, inclusive and collaborative multi-stakeholder approach; prioritising privacy and security; and ensuring accessibility, legal clarity and interoperability (see Figure 1).

Figure 1. Summary of the policy principles



The above principles build on the established foundations for internet governance and on previous initiatives. These initiatives include the World Summit on the Information Society (WSIS) – Geneva Declaration of Principles (2003) and Tunis Agenda (2005); the NETmundial Multistakeholder Statement (2014) and NETmundial+10 Multistakeholder Statement (2024); the Declaration on the Future of the Internet (2022); and the Global Digital Compact (2024). The evolution towards Web 4.0 and virtual worlds offers significant opportunities for citizens and businesses alike. However, as outlined in the Background paper[6], it is also exacerbating certain existing challenges, as well as introducing new ones. This underlines the need for the stakeholder community to reaffirm the core

[6] PPMI & TNO (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/113701

principles of internet governance and to adapt these to the evolving landscape of Web 4.0 and its related technologies, and to the future architecture of the internet.

Policy principle 1: Upholding human rights universally, while adopting specific measures for ensuring ethical and safe Web 4.0 and virtual worlds

The application of **human rights** principles to online spaces has been a cornerstone of internet governance. Commitments to uphold the Universal Declaration of Human Rights are echoed in the Tunis Agenda (2005), NETmundial (2014, 2024) and the Declaration for the Future of the Internet (2022), among other agreements[7,8,9]. Recently, the Global Digital Compact introduced a renewed and heightened commitment to respect, protect and promote human rights in the digital space[10].

Human rights are fundamental and universal, as enshrined in the Universal Declaration of Human Rights. Stakeholders who took part in the conference and the consultation preceding it broadly agreed that **the development of the Web 4.0 and virtual worlds must be anchored on international human rights law**. The international community ought to commit to upholding human rights universally when addressing emerging issues related to Web 4.0 and virtual worlds. The non-discriminatory, ethical, safe and inclusive use of technology must be ensured.

Web 4.0 technologies can provide new opportunities for **self-expression and democratic engagement** by enabling individuals to reach diverse audiences, facilitating community building across physical boundaries, and providing immersive spaces for public discourse[11]. Virtual worlds already provide opportunities for diverse individuals to explore different identities, perspectives and ideas[12,13]. Several existing use cases show that immersive social learning experiences can cultivate empathy, connection, and a shared sense of community in users[14,15]. In the future, decentralised communication could enhance freedom of expression and user control through direct peer-to-peer interactions[16]. By facilitating virtual meetings, public discussions and grassroots organising, virtual worlds and digital deliberation platforms can encourage civic participation and democratic engagement, making it easier for individuals to collaborate, advocate and shape societal change. Sophisticated tools and techniques, such as fact-checking algorithms, image and video analysis tools, and AI-driven bot detection, will be essential to mitigate the spread of false information and ensure informed discourse[17]. Moreover, Web 4.0 and virtual worlds can offer personalised and immersive learning opportunities, including on topics such as immersive literacy and recognising disinformation.

The use of **vast amounts of personal data collected** in Web 4.0 environments (e.g. data on physical health, as well as neurological, behavioural and emotional data), combined with advanced AI algorithms and their predictive capabilities enables highly personalised and hyper-targeted content

[7] High Level Multistakeholder event on the Future of the Internet (2022). Available at: https://www.youtube.com/watch?v=9aGsZLxLDOY
[8] 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
[9] NETmundial (2014). NETmundial Multistakeholder Statement. Available at: https://netmundial.br/2014/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf
[10] 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
[11] DRCF (2023), Immersive technologies foresight paper, Digital Regulation Cooperation Forum.
[12] Iqbal, M. Z., & Campbell, A. G. (2023). Metaverse as tech for good: Current progress and emerging opportunities. In Virtual Worlds (Vol. 2, No. 4). MDPI.
[13] 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
[14] Ibid.
[15] OECD (2025), An immersive technologies policy primer, OECD Digital Economy Papers, No. 373, OECD Publishing, Paris, https://doi.org/10.1787/cf39863d-en.
[16] 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
[17] Lou, Q., & Xu, W. (2025). Personality modeling for persuasion of misinformation using AI agent. *arXiv*. https://arxiv.org/abs/2501.08985

and services[18,19]. Hyper-personalisation can be used to improve and tailor services and content, such as personalised health services, customised learning paths and intelligent virtual assistants that anticipate user needs. However, despite these benefits, the same data can also be exploited to influence users' behaviour and preferences (e.g. highly realistic stolen identities or fake, manipulative or coercive content highly tailored to users' preferences, behaviour and emotional states)[20]. In turn, various actors, such as the private sector, governments and malicious third parties, might leverage the capabilities of Web 4.0, such as digital identities and omnipresent visual surveillance to track and to silence dissent, algorithms to amplify certain narratives over others, or create echo chambers that distort public discourse and perpetuate harm[21,22,23]. Hyper-detailed behavioural tracking and misuse of biometric data further raise concerns of increased emotional exploitation and harassment[24,25,26]. The realistic and immersive nature of Web 4.0 and virtual worlds could significantly exacerbate harms linked to sexual harassment and violence, online sex trafficking and grooming[27,28,29]. Furthermore, in Web 4.0, the lines between "online" and "offline" harms will become increasingly blurred. For example, wearable and implantable devices or smart infrastructure could be exploited to enact actual physical harm.

To counter these risks, it is crucial to safeguard mental integrity, freedom of expression and information and human dignity[30] while promoting transparency, accountability, informed consent and user control. Those who develop, access and oversee these technologies must ensure a human-centric approach, whereby the technology development focuses on addressing the needs, preferences and well-being of the users. Developers and owners of these environments must adhere to universal human rights principles as a guiding framework. AI-assisted and other technologies could be leveraged as useful tools to detect and prevent harassment, misinformation and malicious activity[31].

By removing geographical and social barriers, future web technologies could **improve access for remote, vulnerable and marginalised populations** to experiences, services and opportunities they might otherwise lack[32]. Multimodal, personalised and XR-enabled interfaces are expected to allow for the creation of **more inclusive virtual environments** that are tailored to diverse needs. For instance, real-time captioning and translation tools, as well as voice, gesture and eye-tracking controls can

[18] 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

[19] XR4human (2023). D31; State-of-art in XR policy debates. Available at: https://xr4human.eu/wp-content/uploads/2024/10/XR4HUMAN_D3.1.pdf

[20] PPMI & TNO (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/11370.

[21] Ibid.

[22] Adams-Prassl, J. (2019). What if Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work, 41 *Comparative Labour Law & Policy. Journal,* 123, 133.

[23] 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.

[24] PPMI & TNO (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/113701.

[25] 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

[26] European Parliamentary Research Service. (2024). 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

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

[28] 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

[29] 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.

[30] European Parliamentary Research Service. (2024) 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

[31] Schulenberg, K., Li, L., Freeman, G., Zamanifard, S., & McNeese, N. J. (2023, April). Towards leveraging AI-Based moderation to address emergent harassment in social virtual reality. In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (pp. 1-17).

[32] 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

enhance accessibility, allowing users to participate fully and meaningfully in virtual environments. In addition, AI-driven bias detection systems, as well as decentralised identity solutions and zero-knowledge proofing, could increase fairness in decision-making processes, such as in recruitment practices.

While Web 4.0 technologies provide opportunities to create more inclusive virtual environments, they also raise concerns regarding **discrimination against vulnerable and marginalised populations**. The decentralisation and AI-driven nature of Web 4.0 creates an ecosystem in which bias can be deeply embedded into digital interactions. The collection of biometric and behavioural data in Web 4.0 could be used to unfairly target vulnerable groups or an individual on systematic basis, creating new forms of discrimination. In addition, the heightened sense of presence and realism could make experiences of discrimination more visceral and psychologically damaging[33]. Non-discrimination and equal treatment must be central to Web 4.0 and virtual worlds, ensuring inclusive participation for all users, regardless of background or ability, while fostering self-realisation and creativity.

Web 4.0 and virtual worlds present **a number of opportunities with respect to physical and mental health and well-being.** These include leveraging immersive environments for therapy, rehabilitation and cognitive enhancement; enabling recovery from stress; mindfulness and mood regulation; treating conditions such as anxiety and PTSD through VR-based exposure therapy; facilitating the early detection of mental health issues via eye-tracking; and enhancing rehabilitation outcomes for older adults, including stroke recovery and Alzheimer's risk detection[34].

Despite their applications for promoting health and well-being, prolonged use of virtual worlds can also present certain risks. For example, the literature highlights concerns of isolation from and the displacement of real-world connections; addiction and mental health issues; physical consequences in terms of a sedentary lifestyle and musculoskeletal disorders; and unforeseen negative impacts on children and vulnerable individuals[35,36,37]. 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[38]. Protecting physical and mental health through thoughtful design, ensuring suitability for all age groups (including children and older adults), and maintaining human oversight of applications and algorithms, are all essential to safeguarding user health and well-being.

Safeguarding children's rights should be a key consideration in the governance of Web 4.0, particularly as children are often early adopters of emerging technologies while protections remain limited. It is paramount to ensure that immersive environments and Web 4.0 uphold the best interests of the child, in line with the UN Convention on the Rights of the Child and the Charter of Fundamental Rights of the European Union. As the development of the virtual worlds technologies is largely driven by economic interests, a more inclusive and human rights-based approach is essential to ensure children can navigate the digital world safely.

The opportunities offered by Web 4.0 and virtual worlds should be harnessed to promote human rights, improve lives, and enrich experiences by expanding access to knowledge, ideas and new avenues for self-expression. To achieve this, **individuals should be more concretely and robustly protected** against discrimination, online harms, manipulation and disinformation, control and interference with access, misuse for surveillance purposes, and threats to health and well-being.

---

[33] PPMI & TNO (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/113701.

[34] Ibid.

[35] Ibid.

[36] European Parliamentary Research Service. (2024). 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

[37] XR4human (2023). D31; State-of-art in XR policy debates. Available at: https://xr4human.eu/wp-content/uploads/2024/10/XR4HUMAN_D3.1.pdf

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

Policy principle 2: Ensuring a forward-looking, transparent inclusive and collaborative multistakeholder approach, building on established governance mechanisms

The current model for internet governance is characterised by a **multistakeholder approach** that involves civil society, the technical community, academia, the private sector and governments. It has been instrumental in maintaining the internet as an open, global and interoperable environment. Through its Geneva (2003) and Tunis (2005) phases, the World Summit on the Information Society (WSIS) process established the fundamental principles of this approach, including the importance of a transparent, democratic and bottom-up process. Since then, organisations such as the Internet Governance Forum (IGF), the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), and the International Telecommunication Union (ITU) have played a key role in shaping technical standards, facilitating discussions and addressing governance challenges. The Global Digital Compact (GDC) adopted by the UN in 2024 is a framework that aims to foster an inclusive, rights-based digital future through global cooperation on the governance of AI, internet accessibility and data sovereignty. However, some stakeholders who took part in the consultation that underpins the present document, along with a broader range of civil society organisations, have noted the state-led negotiation dynamics of the GDC. They indicate that while the framework is aimed at enabling multistakeholder collaboration, the process has insufficiently integrated the perspectives of civil society.

A transparent, **forward-looking and inclusive multistakeholder approach to internet governance** that aligns with the principles of the São Paulo Multistakeholder Guidelines adopted at the NETmundial+10 conference, is essential, especially given advances in Web 4.0 and virtual world technologies[39]. In view of the current World Summit on the Information Society (WSIS) +20 process, the role of internet governance institutions needs to be reaffirmed and strengthened as central fora for anticipatory processes, discussion, reflection and the formulation of guiding principles on the future of the internet.

Stakeholders who took part in the conference and the consultation leading up to it emphasised that the existing internet governance frameworks need to continuously evolve in order to address the issues emerging from Web 4.0 and virtual worlds. A key concern is the **risk of fragmentation** in approaches to Web 4.0 and virtual worlds technologies. Uncoordinated policy approaches or divergent standards could lead to siloed virtual worlds, as well as having adverse unintended effects on internet infrastructure and undermine the global, interconnected nature of the internet. Building safe and interoperable future web and virtual worlds requires enhanced global coordination in both **institutional and non-institutional settings**[40] between governments, internet governance institutions, businesses, including virtual worlds creators, civil society, academia and end users.

Since its inception, the multistakeholder internet governance model **has achieved several notable milestones** in the technical, institutional and developmental spheres. The 2016 IANA transition, which shifted oversight from the US government to global stewardship, stands out as a landmark achievement, building on the earlier work of Regional Internet Registries and reinforcing bottom-up policy development[41,42]. The multistakeholder approach has promoted inclusive policies to expand access in developing regions, to boost local content creation and strengthen capacity-building programmes. While consensus-driven decision-making can be slow and the digital divide remains a

[39] The term "multistakeholder governance" is defined in the 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.

[40] Improving institutional cooperation entails the establishment and maintenance of formal mechanisms for policy coordination and internet governance, as well as ensuring an open and inclusive dialogue, while non-institutional cooperation covers more flexible mechanisms for knowledge sharing, dialogue and capacity building.

[41] More information is available at: https://www.icann.org/en/announcements/details/stewardship-of-iana-functions-transitions-to-global-internet-community-as-contract-with-us-government-ends-1-10-2016-en

[42] Authentic Web (no date). *The Challenges of Deploying DNSSEC*. Available at: https://authenticweb.com/domains-dns-and-tls-certificates/the-challenges-of-deploying-dnssec/

persistent challenge, **the multistakeholder approach has played a pivotal role** in fostering a stable, secure and ever-evolving global internet infrastructure that balances the interests of diverse stakeholders.

Internet governance must therefore continue to rely on a proactive, transparent and inclusive **multistakeholder approach**, while additional efforts are needed to ensure meaningful and accountable participation in the governance of Web 4.0 and virtual worlds by civil society, businesses, governments, the technical community, academia and end users. **Meaningful inclusion** requires the recognition of different cultural norms and perspectives and the active participation in internet governance institutions and processes of under-represented groups, including those from the Global South, SMEs, civil society, end-users, indigenous communities and marginalised populations, as well as new stakeholder groups relevant to Web 4.0 (e.g. virtual world developers, decentralised communities, immersive tech startups, open-source communities, and companies specialising in quantum computing and advanced networking). It is important to ensure an approach that is inclusive to the relevant stakeholder community. Such participation will involve the overcoming of barriers such as geographical imbalances, language limitations and resource constraints through capacity-building initiatives, inclusive consultation processes and mechanisms that ensure equitable participation and the reflection of diverse cultural, social and economic perspectives in decision making[43].

The integration of an **anticipatory approach** in governance is essential, due to the rapid pace of technological advances in Web 4.0 and virtual worlds. Internet governance institutions should engage with diverse stakeholders to proactively identify emerging challenges and opportunities in relation to technological advances and their impact on the internet and its governance. Multistakeholder governance sandboxes[44], used to co-create and test solutions to specific issues related to Web 4.0 could be harnessed for this purpose.

Policy principle 3: Prioritising security in Web 4.0 and virtual worlds to ensure responsiveness to emerging cyber and hybrid risks

Ensuring stability, security and safety has been central to internet governance. In its Declaration of Principles, the World Summit on the Information Society (WSIS) stated the need to "ensure a stable and secure functioning of the internet"[45]. The Global Digital Compact (2024) notes the need for a secure digital space, including "safe, secure and trustworthy emerging technologies" as well as safe and secure network coverage[46]. The Compact also highlights the need to ensure that "people can meaningfully and securely use the internet and safely navigate the digital space"[47]. Therefore, **security must be a cornerstone of Web 4.0 and virtual worlds**, ensuring resilience against cyber threats, safeguarding sensitive data, and fostering trust in digital environments.

The evolution of Web 4.0 and virtual worlds **not only amplifies existing cybersecurity and cybercrime challenges, but also introduces new ones**. These include, for example, risks due to the proliferation of technologies that are capable of collecting sensitive data (e.g. emotional and behavioural data); the increased interconnectedness of devices and systems in which the lines between "online" and "offline"

[43] PPMI & TNO (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/113701.

[44] Environments within existing governance institutions to innovate and test approaches tackling cross-cutting issues that require input from diverse stakeholder groups. Those environments can provide a structured setting for experimentation, which enables the testing of different policy approaches, innovative solutions and consensus building by involving diverse and appropriate stakeholders

[45] 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

[46] UN (2024). Global Digital Compact. Available at: https://www.un.org/global-digital-compact/en

[47] Ibid.

harms become increasingly blurred[48]; the exploitation of virtual marketplaces and smart contracts; AI-powered cyberattacks (e.g. AI-enabled impersonation and adaptive botnets) and other malicious misuse of advanced technologies[49,50]. Another persistent threat concerns the targeting of critical infrastructure, such as undersea cables, satellite networks and cloud infrastructure[51,52]. The current networks face challenges in handling the complexity and scale of Web 4.0-related threats, leaving critical infrastructure at risk. A distinct challenge arises from the advancement of **quantum computing**, which threatens to undermine foundational encryption algorithms[53]. Even if post-quantum cryptography standards are achieved before this happens, a "catch now, exploit later" situation, in which actors collect currently unreadable data in order to decrypt it afterwards, remains a threat[54].

In terms of opportunities, Web 4.0 and its associated technologies **have the potential to enable practical approaches** to enhancing cybersecurity and addressing digital risks through multiple layers of protection. **Currently, however, these are separate technologies with different levels of maturity**. For example, by leveraging AI and machine learning, systems can detect and respond to threats in real time. Advanced authentication mechanisms, including biometrics and behavioural analytics, can provide continuous identity verification[55], while blockchain technology can ensure transparent and tamper-proof record keeping[56]. The integration of IoT devices and digital twins enables both physical and virtual infrastructure to be better monitored. Self-healing networks will automatically isolate and repair compromised sections. Smart contracts and automated incident response systems can execute security protocols instantly, while AI-driven predictive analytics can forecast and prevent potential breaches before they occur. If integrated into a symbiotic ecosystem, these technologies could create a more resilient security environment that adapts to emerging threats while ensuring privacy and regulatory compliance.

Given the close link between cybersecurity, national security and the resilience of the internet infrastructure, **international collaboration between governments, within multistakeholder settings**, is essential to address transnational cyber threats[57]. Such collaboration should focus on implementing comprehensive security measures across critical internet infrastructure, promoting the widespread adoption of crucial security standards such as DNS Security Extensions (DNSSEC) and Resource Public Key Infrastructure (RPKI). It should also focus on strengthening supply chain integrity through robust verification processes, and establishing coordinated incident response mechanisms to effectively combat evolving cyber threats that transcend national boundaries. At the same time, it is important to strike a balance between security needs and the risks of over-surveillance or the misuse of cybersecurity tools that could infringe civil liberties. Moreover, the role of private sector service providers in ensuring a secure and human-centric web should also be emphasised.

[48] PPMI & TNO (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/113701.

[49] 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.

[50] PPMI & TNO (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/113701.

[51] IGF (2024). Riyadh Messages. Available at: https://intgovforum.org/en/filedepot_download/305/28526

[52] PPMI & TNO (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/113701.

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

[54] Vermeer, M.J.D., &Peet, E.D. (2020). *Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption*. Santa Monica, CA: RAND Corporation. Available at: https://www.rand.org/pubs/research_reports/RR3102.html .

[55] More information is available at: https://www.edps.europa.eu/press-publications/publications/techsonar/biometric-continuous-authentication_en

[56] Devlane (no date) *The role of blockchain in secure online transactions*. https://www.devlane.com/blog/the-role-of-blockchain-in-secure-online-transactions.

[57] IGF (2024) Riyadh Messages. Available at: https://intgovforum.org/en/filedepot_download/305/28526

Policy principle 4: Prioritising privacy and data protection in Web 4.0 and virtual worlds

Privacy has served as a guiding principle for the governance of the internet since its very outset. The Tunis Agenda for the Information Society (2005) emphasised that respecting privacy and protecting personal data are crucial[58]. The signatories to the Global Digital Compact (2024) have committed to protecting privacy, freedom of expression and access to information while addressing harms[59].

Stakeholders who took part in the conference and the consultation leading up to it noted that **the right to privacy should be fundamental** to Web 4.0 and virtual worlds. The future web offers opportunities to strengthen privacy by giving users more control over their personal data through advanced technological solutions. These include privacy enhancing technologies, consent automation, decentralised and secure transactions using blockchain. Moreover, quantum-secure encryption (when it becomes available) will enhance privacy by protecting against data breaches and ensuring that personal information, communications and transactions remain secure.

The scale and complexity of the data collection, behavioural tracking and biometric analysis enabled by technologies related to Web 4.0 also create significant risks for individuals and organisations[60,61]. A key feature of this trend is the **depth and granularity** of the data collected using immersive technologies, IoT devices and AI analytics. This can allow facial recognition, voice analysis, gaze tracking, haptics and the tracking of real-time physiological responses, as well as neurological and health data[62,63,64,65]. Moreover, the collection of behavioural and movement data in virtual environments can enable individuals to be identified across multiple sessions, regardless of other identifiers (e.g. username, avatar), thereby posing new challenges to anonymity and privacy online[66,67].

The stakeholders consulted indicated that **users should be empowered to decide** when and how their data is used. While personal data relating to identified or identifiable natural persons enjoy specific legal protections in many jurisdictions[68], data generated through user activities is often subject to more flexible regulation, and the relevant legal framework is still evolving in many cases. All stakeholders, including governments, businesses and developers, have a responsibility to manage user data securely and ethically. Overall, given the vast amount of personal data collected through immersive technologies, it is crucial to limit data collection only to that which is absolutely necessary.

---

[58] World Summit on the Information Society (2005).

[59] 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

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

[61] 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

[62] European Parliamentary Research Service (EPRS) (July 2024). 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

[63] 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

[64] 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

[65] 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

[66] 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

[67] XR4human (2023). D31; State-of-art in XR policy debates. Available at: https://xr4human.eu/wp-content/uploads/2024/10/XR4HUMAN_D3.1.pdf

[68] For example, see Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

It is essential to achieve a careful balance between protecting user privacy and anonymity (in relevant contexts) and broader societal interests. Safeguarding users' control over their data must be weighed against the need to support a thriving data economy and drive innovation in virtual worlds and other Web 4.0 applications. Similarly, ensuring strong privacy and data protection while enabling law enforcement to combat cybercrime requires a well-calibrated approach. Lawful access to data for crime prevention must be strictly governed by the principles of necessity, fairness and legality.

Policy principle 5: Ensuring the accessibility of Web 4.0 and virtual worlds, while tackling global digital divides in terms of access, capabilities and outcomes

Internet access has become an essential part of life for much of the world. Recognising its importance, the United Nations declared in 2016 that it considers internet access a human right[69]. The World Summit on the Information Society (WSIS) states that "the ability for all to access and contribute information, ideas and knowledge is essential in an inclusive Information Society"[70]. The recent Global Digital Compact (2024)[71] contains a commitment to connect all persons to the internet, as well as to "refrain from internet shutdowns and measures that target internet access"[72]. According to the conference participants, accessibility of future Web 4.0 technologies requires both an interoperable internet architecture and the adaptation of the application and content layers to diverse user needs.

While some populations remain focused on simply gaining reliable internet access and safeguarding their human rights, others are poised to leverage these emerging technologies for rapid advancement, potentially deepening existing inequalities. According to many of the stakeholders who took part in the conference and the consultation leading up to it, **the opportunity to participate in the Web 4.0 and virtual worlds** – including affordable and equitable access to the hardware, software, digital identity services[73] and connectivity required to participate fully in digital environments – should be available to all, regardless of background or abilities. A fundamental principle is that the economic and societal benefits of Web 4.0 and virtual worlds should be shared fairly around the globe. To ensure this, coordinated action on an international level in terms of investment in digital infrastructure, promotion of inclusive design and strengthening of user and advanced specialised digital literacy and skills are needed, especially in underserved areas and for vulnerable populations.

When they are coupled with affordable access, inclusive design and the development of digital skills, advances in Web 4.0 technologies offer opportunities to bridge the digital divide and ensure that individuals can participate fully in digital environments regardless of location, socio-economic status or ability. By leveraging decentralised communication, multimodal interfaces and AI-driven accessibility tools, the future web could reduce barriers to participation and enable the more equitable distribution of economic and societal benefits among diverse communities[74].Inequalities can be addressed in terms of three critical dimensions: access, capabilities and outcomes[75].

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. In recent years, gaps in terms of internet speed and data have grown between high-income

[69] Article 19 (2016). Internet statement adopted. Retrieved from https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

[70] 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

[71] 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

[72] More information is available at: https://www.accessnow.org/internet-shutdowns-2023/

[73] Around 850 million people in the world do not have an official ID at all, with 220 million more living without a digital record of their identity, 400 million more people lack a digitally verifiable identity document, according to the World Bank (2024) 'Digital Progress and Trends Report 2023'.

[74] OECD (2025), An immersive technologies policy primer, OECD Digital Economy Papers, No. 373, OECD Publishing, Paris, https://doi.org/10.1787/cf39863d-en.

[75] 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.

and low- and medium-income countries[76]. Emerging virtual world and Web 4.0 technologies will require high upload speeds and ultra-low latency, thus necessitating the widespread deployment of 5G/6G networks, additional fibre rollout as well as specialised hardware and software[77,78,79]. Beyond network coverage, meaningful connectivity requires addressing the usage gap, as 2.2 billion people within network reach remain unconnected[80].

Web 4.0 technologies offer opportunities to reduce barriers to access virtual environments for a wide range of people. Their multimodal, personalised and AR-enabled interfaces can be adapted to differing needs. These technologies could also improve the accessibility of physical environments – for example, by providing object recognition and navigation assistance to individuals with visual impairments or intellectual disabilities[81,82].

However, currently available XR technologies are comfortable to wear for only around half of the population[83]. For example, many current VR and AR devices are not designed for children or older adults, and are not suitable for users with visual, vestibular or cognitive impairments[84,85,86]. It is important that this access gap be closed, which will ensure that all individuals and societies can benefit from the opportunities offered by Web 4.0 and virtual worlds. Achieving this will require coordinated efforts from the international community to advance accessible digital infrastructure, affordable hardware and software, and inclusive design.

The **capability divide** refers to differences in digital skills, technological literacy and the ability to use digital tools effectively. Intuitive and immersive interfaces may reduce barriers to accessing Web 4.0 by rendering some current digital skills obsolete over time. However, new skills will gain importance, such as in the use of devices that support immersion (e.g. headsets, haptic devices), as well as AI collaboration skills, data literacy, cybersecurity skills and the ability to identify increasingly sophisticated disinformation and manipulation[87]. For instance, the novelty of immersive experiences and lack of awareness of best practices for secure usage, can lead to increased threats for data misuse and digital security[88]. This shift runs the risk of further disadvantaging those with limited access to emerging devices and training resources. Investments in digital skills and digital literacy are urgently needed to ensure that people can navigate and harness the benefits of Web 4.0 and virtual worlds meaningfully, responsibly and safely[89]. Opportunities to develop and improve these skills should be made available to persons of all ages and backgrounds, taking into account their cultural, social, economic and linguistic needs.

---

[76] World Bank (2024). Digital progress and trends report 2023. Washington, DC: World Bank. https://doi.org/10.1596/978-1-4648-2049-6

[77] 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

[78] OECD (2025), An immersive technologies policy primer, OECD Digital Economy Papers, No. 373, OECD Publishing, Paris, https://doi.org/10.1787/cf39863d-en.

[79] Connect Europe. (2025). State of digital communications 2025. Available at: https://connecteurope.org/sites/default/files/2025-01/State%20of%20Digital%20Communications%20%282025%29.pdf

[80] Ibid.

[81] European Commission: Directorate-General for Communications Networks, Content and Technology, Boel, C., Dekeyser, K., Depaepe, F., Quintero, L. et al., Extended reality – Opportunities, success stories and challenges (health, education) – Final report, Publications Office of the European Union, 2023, https://data.europa.eu/doi/10.2759/121671

[82] Maran, P. L., Daniëls, R., & Slegers, K. (2022). The use of extended reality (XR) for people with moderate to severe intellectual disabilities (ID): A scoping review. Technology and Disability, 34(2), 53-67.

[83] 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

[84] 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.

[85] 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

[86] 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.

[87] 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

[88] OECD (2025), An immersive technologies policy primer, OECD Digital Economy Papers, No. 373, OECD Publishing, Paris, https://doi.org/10.1787/cf39863d-en.

[89] PPMI & TNO (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/113701.

Lastly, the **outcome divide** refers to disparities in the benefits derived from digital technologies. These include economic opportunities, educational progress and access to information, a lack of which can result in unrealised potential for societal or personal development and missed opportunities for businesses. It is therefore important to counter the risk of uneven adoption, which could deepen existing digital divides and negatively affect regional competitiveness and development and ensure fair benefit-sharing and participatory governance.

Policy principle 6: Ensuring a predictable and transparent regulatory environment, interoperability and counterbalancing monopolistic practices to foster innovation and fair competition, and to harness new business opportunities in Web 4.0 and virtual worlds

The 2003 declaration of principles by the World Summit on the Information Society (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"[90]. The Global Digital Compact (2024) acknowledges that the advancement of meaningful inclusion requires the laying of groundwork 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[91].

Web 4.0 and virtual worlds **can unlock significant economic value** by favouring the emergence of new business models and transforming various sectors of the economy such as financial services, manufacturing, agriculture, healthcare and others. 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[92,93].

However, realising the potential of Web 4.0 and virtual worlds will require a predictable regulatory environment, interoperability, and the countering of monopolistic practices.

Web 4.0 and related technologies aim to provide highly immersive experiences and to mimic real-life experiences within digital spaces. The creation of and trade in new, virtual assets raises distinct questions about ownership, taxation and intellectual property that need to be addressed in order to ensure that innovation can occur within a clear regulatory environment.

It is essential that fair competition is ensured by tackling the **concentration of market and technological power** and preventing the emergence of closed digital ecosystems in Web 4.0 and virtual worlds. **Interoperability** must be a fundamental principle underpinning Web 4.0 and virtual worlds. By facilitating seamless interactions across platforms and ensuring the ability of users to transfer digital assets, avatars, identities and experiences, interoperability is a key pre-condition for competitive markets. However, full interoperability depends not only on the adoption of appropriate technical standards and protocols, but also on economic incentives that can either facilitate or hinder such interoperability, as well as the broader regulatory framework. It is important that governments, the technical community, academia, the private sector and civil society organisations collaborate to

[90] 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

[91] 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

[92] 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

[93] Vigkos, A., Bevacqua, D., Turturro, L., & Kuehl, S. (2022). The Virtual and Augmented Reality Industrial Coalition: Strategic paper.

discuss, adopt and implement common standards and broader regulatory frameworks aimed at creating technical and economic incentives for interoperability[94].

The development of Web 4.0 and virtual worlds requires a **predictable and transparent environment**, supported by global coordination of policies, legal and regulatory frameworks. Clear rules are essential to provide businesses with the certainty they need to address cross-border challenges such as intellectual property rights, data governance and platform monetisation[95]. Multistakeholder governance sandbox environments can act as collaborative spaces to test and refine these technologies, providing a mechanism to assess their impact and foster open, transparent dialogue prior to full implementation[96]. Stakeholders in the conference and the consultation leading up to it also highlighted that determining the applicable legal jurisdiction in virtual worlds remains a challenge. The application of different rules in different jurisdictions create costs for businesses and opportunity costs for innovation. Thus, coordination between governments to resolve issues stemming from differences in legal frameworks and jurisdiction questions in virtual worlds is needed.

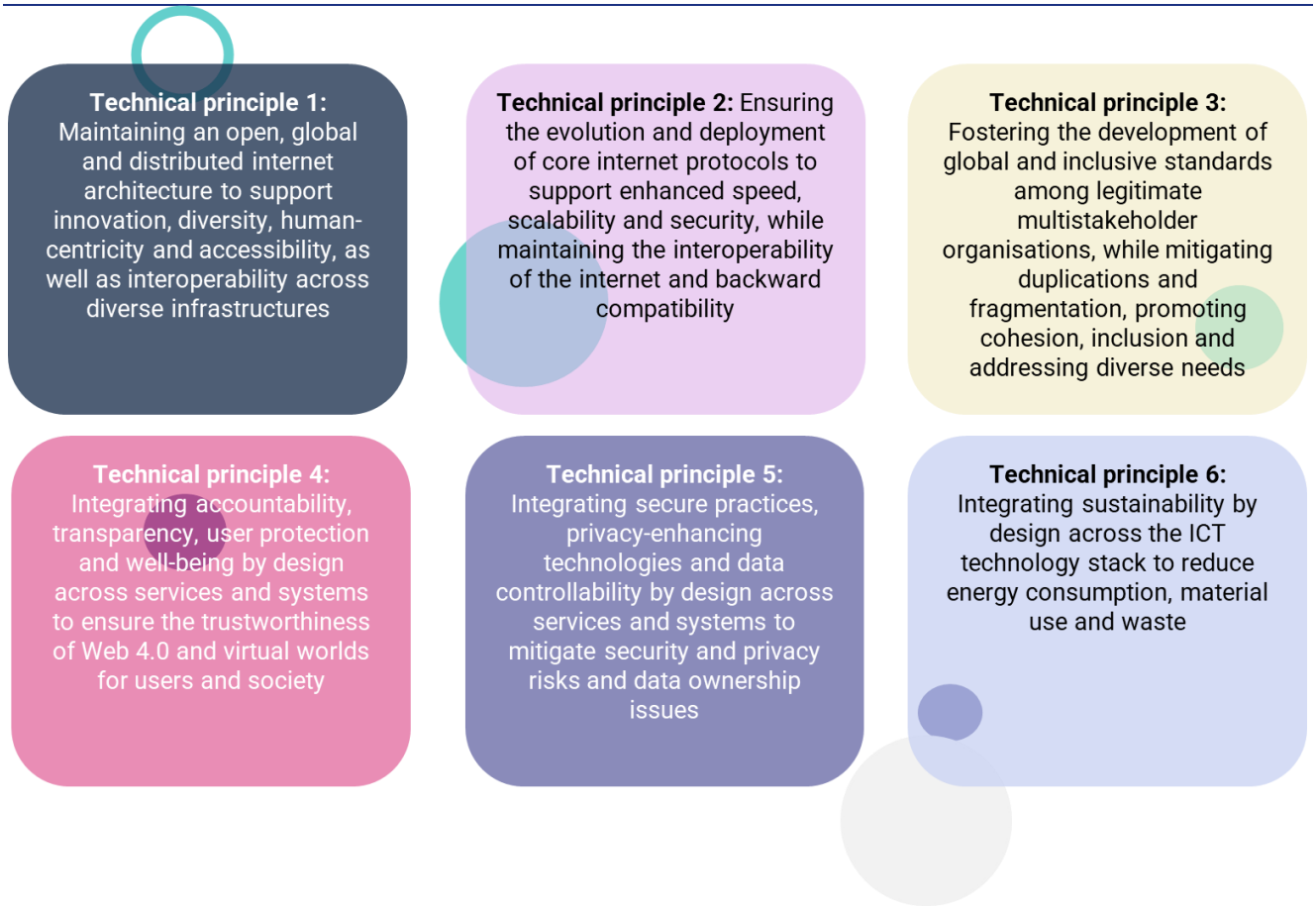
Global trade and data ownership are the foundational pillars of the digital economy. An open, interoperable and inclusive global ecosystem is essential for the exchange of goods, services and data. International cooperation within multistakeholder settings is critical to creating a predictable and transparent framework that supports fair trade practices, respects data rights and promotes sustainable economic growth in the evolution towards Web 4.0 and virtual worlds.

[94] OECD (2025), An immersive technologies policy primer, OECD Digital Economy Papers, No. 373, OECD Publishing, Paris, https://doi.org/10.1787/cf39863d-en.
[95] PPMI & TNO (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/113701.
[96] More information available at: https://www.metaversedialogues.org/

3. Technical principles

The technical principles outlined in this chapter **are intertwined with the policy principles.** They are instrumental for upholding the values and rights that underpin a fair, transparent and accountable digital ecosystem, particularly in light of technological advances in relation to Web 4.0 and virtual worlds. These principles include maintaining open and distributed internet architecture; ensuring the evolution and deployment of core internet protocols to maintain interoperability; fostering the development of global and inclusive standards; integrating accountability, transparency, user protection and well-being by design; integrating secure practices and privacy enhancing technologies; and integrating sustainability by design (see Figure 2).

Figure 2. Summary of the technical principles



An analysis of developments in technology and the related governance challenges that underpin the evolution towards Web 4.0 and virtual worlds are presented in the accompanying **Background document**.

Technical principle 1: Maintaining an open, global and distributed internet architecture to support innovation, diversity, human-centricity and accessibility, as well as interoperability across diverse infrastructures

Several stakeholders who participated in the consultation activities emphasised that technological advances in relation to Web 4.0 and virtual worlds should build upon the existing internet, leveraging decades of experience, technical expertise and operational know-how from the technical community, civil society, businesses and the public sector. This aligns with recommendations and guidance from various organisations, including the Internet Society's *Global Internet Report*[97], the OECD's *Principles for Internet Policy Making*[98], ITU guidance on inclusive connectivity[99], and the World Economic Forum's call for resilient, future-proof digital infrastructure[100]. **It is essential to ensure that the internet remains an open and distributed global network.** Technological advances in relation to Web 4.0 and virtual worlds should be integrated in a technically sound and feasible manner to enhance and upgrade the existing internet. This would foster innovation, diversity and accessibility, ensuring the internet can serve as a resilient and trustworthy foundation for digital ecosystems in the future, as it has done in the past.

At present, there is **a risk that the internet will shift away from its original vision** of a single, open, distributed and globally connected network of networks. The term "splinternet" refers to the increasing fragmentation of the global internet into separate, nationally or regionally controlled or technologically siloed networks. This includes the creation of national firewalls, content restrictions and the development of parallel digital ecosystems. It also encompasses **diverging technical standards and protocols** between different countries or regions – for example, in relation to mobile communications, encryption, the exchange of personal and business data, and payments. Therefore, **it is crucial to build on current internet architecture** in order to maintain a digital ecosystem that remains open, global and unfragmented.

Furthermore, the dominance of certain browser vendors – whereby a handful of major companies control the most widely used web browsers – has concentrated power over web standards and user experience. The growing prevalence of app-based ecosystems, particularly the rise of mini-apps within super-apps, has created **closed digital environments** that operate outside the open web. These parallel developments put at risk the internet's founding vision of an open, universally accessible network in which content and services can be accessed via standard protocols rather than being controlled by individual platforms. To preserve an open and universally accessible internet, major browsers and app platforms should adhere to the principles of open standards, ensure data portability, and maintain APIs that enable third-party access and integration.

The evolution towards Web 4.0 and virtual worlds is ushering in **a new generation of platforms and services** that blend physical and digital realities through advanced technologies. By maintaining **openness and flexibility**, these new platforms and services are able to integrate seamlessly with existing ones. Openness is the key to preventing ecosystem "lock-in", and encourages fair competition.

Interoperability must be ensured across the infrastructure of the internet, including high-speed terrestrial fibre networks and next-generation mobile technologies such as 6G, as well as satellite-based systems. But while interoperability can enable immersive, seamless Web 4.0 experiences, if not properly managed it can also create complex dependencies that undermine resilience. Special care

[97] Internet Society (ISOC) (2019). *Global Internet Report*. https://www.internetsociety.org/globalinternetreport/
[98] Organisation for Economic Co-operation and Development (OECD) (2011). *Principles for Internet Policy Making*. OECD Publishing. https://www.oecd.org/internet/innovation/49258588.pdf
[99] International Telecommunication Union (ITU) & United Nations Educational, Scientific and Cultural Organization (UNESCO) (Annual). *The State of Broadband*. Broadband Commission for Sustainable Development. https://www.broadbandcommission.org/
[100] World Economic Forum (WEF). (2023). *The Global Risks Report 2023*. World Economic Forum. https://www.weforum.org/reports/global-risks-report-2023/

should be taken to maintain efficiency and security by incorporating scalability and adaptability by design in order to accommodate for future needs and threats. **Resilience** is also essential in order to withstand disruptions, to safeguard the integrity of data, and to advance equitable digital inclusion.

Net neutrality is a key principle in preserving an open and equitable internet. This requires internet service providers to treat all data traffic equally, without discrimination on the basis of content, user, platform, application or device. This principle prevents ISPs from creating "fast lanes" for preferred content providers or throttling access to competing services, essentially ensuring that small startups have the same opportunity to reach users as established tech giants. By prohibiting practices such as paid prioritisation and content blocking, net neutrality fosters innovation, protects consumer choice, and maintains the internet as a level playing field.

The continuous evolution of network architectures and digital infrastructures should support **future-proof connectivity and enable enhanced scalability, adaptability and sustainability**[101,102]. For instance, a federative cloud-edge architecture (FEDAPP) provides the basis for decentralised and distributed processing, ensuring data can be managed closer to its point of origin[103]. In addition, support for AI within federated and distributed ecosystems should be established in a way that aligns with data sovereignty, sustainability and local regulatory frameworks.

Creating programmable, **elastic digital infrastructures** that can adapt to application demands in real time requires common stable application programming interfaces (APIs) for both transport and compute resources. Such interfaces provide standardised methods for resource allocation and management, enabling operations to be carried out consistently and efficiently. AI capabilities, when properly integrated into cloud infrastructures, can enhance resource optimisation and predictive scaling, potentially improving both operational control and system efficiency.

The move towards cloud-native and AI-native architectures further blurs the lines between cloud, edge and device, treating them all as nodes for computing and transport functions. This approach not only improves **performance and scalability,** but also encourages **resilience and flexibility** across heterogeneous digital ecosystems[104].

Technical principle 2: Ensuring the evolution and deployment of core internet protocols to support enhanced speed, scalability and security, while maintaining the interoperability of the internet and backward compatibility

The TCP/IP stack[105] **is a hierarchical set of protocols** that enable data to be broken into packets, addressed, transmitted across networks and reliably reassembled at its destination. It forms the fundamental communication architecture of the internet. Stakeholders who took part in the conference discussions and the consultation agreed that maintaining and evolving the TCP/IP stack, alongside other protocols and infrastructure improvements, helps to ensure that the global network remains robust and able to meet increasing demands for low latency, higher speeds and increases in the volume of both personal data as well as data generated by connected machines.

[101] Organisation for Economic Co-operation and Development (OECD) (2019). *Artificial Intelligence in Society*. OECD Publishing. https://doi.org/10.1787/eedfee77-en

[102] World Economic Forum (WEF) (2023). *The Global Risks Report 2023*. World Economic Forum. https://www.weforum.org/reports/global-risks-report-2023/

[103] NIST (2020). *NIST Big Data Interoperability Framework*. NIST Special Publications. https://www.nist.gov/programs-projects/big-data-interoperability-framework

[104] IEEE Standards Association (IEEE SA) (2022). IEEE P2874 - Standard for Virtual Reality and Related Technologies Interoperability. https://standards.ieee.org/

[105] The term "internet protocol stack" is also relevant, especially with the development of the QUIC transport protocol, which coexists with TCP. However, "TCP/IP stack" remains the more traditional term, and is still widely used in technical literature, education and industry.

The core internet protocols face **multiple interconnected risks** that threaten their stability and universality. Technical challenges include the exhaustion of available IPv4 addresses, routing system scalability issues, and protocol ossification (a lack of flexibility and extensibility of protocols). These are compounded by the risk of fragmentation resulting from nation-state initiatives such as alternative DNS systems and regional governance creating inconsistent implementations, potentially leading to a "splinternet". Security vulnerabilities in legacy protocols, along with operational challenges from the uneven deployment of IPv6 and the growing complexity of infrastructure, have placed further strain on the system. The fundamental challenge lies in evolving these protocols to address upcoming needs, as well as to facilitate developments towards Web 4.0, while maintaining global interoperability and preventing network fragmentation.

These **risks are amplified** by emerging Web 4.0-related technologies and usage patterns, which place new demands on internet infrastructure. The growing number of connected devices, both physical (IoT, smart homes, sensor networks) and virtual (metaverse objects, digital twins), challenges existing addressing schemes. To ensure ownership, control, and security of digital assets, they will need unique identifiers Real-time applications that require ultra-low latency, such as haptic interfaces and brain-computer interfaces, are pushing the limits of current internet protocols. Meanwhile, the distributed nature of modern computing architectures spanning cloud, edge and fog computing increases the attack surface and the complexity of security protocols.

The mitigation of risks to core internet protocols **must be guided by principles** of careful evolution rather than radical change. Protocol development should prioritise backward compatibility and incremental improvements, allowing new features to be introduced without disrupting existing infrastructure. Standards development organisations (SDOs) play a crucial role in this process by anticipating future requirements even during the early phases of a technology's adoption, ensuring that protocol extensions and enhancements are standardised in a coordinated manner. This evolutionary approach helps to maintain the internet's fundamental stability while enabling it to adapt to emerging needs.

A forward-looking but measured approach to protocol development **must balance innovation with the preservation of core principles of internet architecture**. This means designing protocol improvements that can accommodate emerging technologies without compromising the internet's basic functions and interoperability. Such development should follow a systematic process of testing, validation and phased deployment, allowing organisations to adopt new capabilities at their own pace while maintaining operational stability. The goal is to enhance protocol capabilities incrementally, ensuring that each change strengthens rather than fragments the internet's foundational infrastructure, while providing clear migration paths for existing systems and services.

Technical principle 3: Fostering the development of global and inclusive standards in legitimate multistakeholder organisations, while mitigating duplications and fragmentation, promoting cohesion, inclusion and addressing diverse needs

Internet standards are developed and maintained by organisations such as the IETF and W3C. They provide broad technical specifications and guidelines that ensure consistency and interoperability across the internet ecosystem. These standards encompass everything from HTML and CSS specifications, which define how web content should be structured and styled, to security standards such as TLS, which specify how data should be encrypted during transmission. Standards are typically

documented in RFCs (Requests for Comments by IETF) and other documents[106] and undergo rigorous review and testing processes before being adopted. Standards provide the overarching framework that guides how protocols and other internet technologies should be designed and implemented to ensure they work together seamlessly across the global network.

The evolution of the internet has been driven by the collaborative efforts of teams and companies pursuing innovation, creating a dynamic foundation for technological advancement in which openness and flexibility are key. While flexibility fosters innovation, the maturation and broader deployment of technologies within the ecosystem often require well-designed standards to ensure interoperability across different implementations and systems. However, for user-facing applications further up the technology stack, proprietary solutions may prove more profitable, limiting incentives for interoperability. In addition, for these applications, standardisation is likely to be driven by industry consortia rather than traditional internet standards bodies.

The rapid evolution of technologies associated with Web 4.0, such as IoT, AI, virtual worlds and brain-computer interfaces, **poses significant challenges to internet standardisation**. These include the massive scale and heterogeneity of devices, rigorous real-time performance demands, the need to ensure robust privacy and security, and the mismatch between rapid innovation and the traditionally deliberative process of standards development. Cross-domain integration adds another layer of complexity, as these technologies blur traditional boundaries, while resource constraints in IoT devices create a tension between comprehensive standards and practical implementation.

Differences in regulation between states and across regions – for example, in areas such as AI and data privacy – make it harder to develop standards that can be applied globally. Maintaining backward compatibility with existing infrastructure becomes more difficult as new technologies introduce fundamentally different paradigms. Testing and verification become more complex too, with AI systems exhibiting emergent behaviours and IoT deployments spanning millions of devices. In addition, given that that the deployment of standards developed by most organisations mentioned here are voluntary, their implementation can depend on market forces, industry acceptance and perceived benefits. Commercial pressures sometimes lead to competing proprietary standards, particularly in emerging fields, risking market fragmentation and reduced interoperability across the internet ecosystem.

The stakeholders consulted indicated that internet governance institutions and stakeholders - including countries - **must embrace** a truly global, collaborative approach in order to adapt to technological change, while allowing each country to act in its own domestic realm of responsibility. Such an approach would include ensuring a comprehensive global perspective in the development of standards. This is particularly crucial in the case of Web 4.0 and virtual worlds, where interoperability is paramount. The process should be anchored in legitimate multistakeholder organisations that involve diverse actors and prevent the duplication of efforts. Organisations such as the IETF and W3C and have earned credibility and recognition through established processes and transparent operation. Liaison officers[107] play an important role in this ecosystem, serving as bridges between standardisation bodies, civil society and governments. However, a lack of technical expertise and resources within civil society organisations limits their participation in the process of standards development.

The governance framework **must ensure fair participation** in the development of standards for emerging technologies by all stakeholders. This will entail the establishment of mechanisms that prevent any single country or major market player from advancing proposals without broad consensus from the global community. Standards development should be guided by principles of inclusivity, transparency and technical merit. At the same time, inclusive standards must consider **diverse needs**, respecting community autonomy, different age groups (e.g. youth and older adults) and cultural

[106] Internet and web technology standards are documented across various authoritative sources and organisations: RFCs (Requests for Comments) published by the IETF define core Internet protocols and systems; W3C recommendations establish web standards and technologies; IEEE standards cover hardware and networking specifications; ISO/IEC standards address broader information technology requirements; and ITU-T recommendations provide global telecommunications specifications through the work of the UN specialised agency, the ITU.

[107] Designated representatives who facilitate communication and coordination between different standards organisations, technical bodies, and stakeholder groups involved in internet governance.

diversity. Collaboration across industries is essential to creating standards that support open competition and user choice. Multi-stakeholder organisations involved in standards development must aim to build consensus while remaining agile enough to keep pace with rapid advances in technology. This balanced approach will help to ensure that standards serve the global public interest while fostering innovation and maintaining the Internet's fundamental character as an open, interoperable system.

Technical principle 4: Integrating accountability, transparency, user protection and well-being by design across services and systems to ensure the trustworthiness of Web 4.0 and virtual worlds for users and society

Trust and trustworthiness are fundamental to the development of Web 4.0 and virtual worlds because these technologies represent an unprecedented integration of digital systems into our daily lives. Users must have confidence that their information, digital assets and interactions are secure and authentic across these environments. This involves protecting privacy and verifying digital identities, (e.g. making sure that a given digital identity is not in fact a deep fake), ensuring the trustworthiness of AI-driven interactions and maintaining safe community spaces.

Trust requires **robust technical infrastructure and effective security measures** to protect against threats such as identity theft and the loss of digital assets.

A robust technical infrastructure for Web 4.0 and virtual worlds is likely to consist of **multiple interconnected systems working together** to deliver secure, reliable and high-performance digital experiences. At its core, such a system includes high-performance computing systems for real-time data processing, decentralised physical infrastructure (DePIN) models, and scalable cloud solutions with redundant backup systems. The integration of neuromorphic computing and energy-efficient optical neural networks enables more sophisticated processing capabilities, while multi-modal interface support incorporating brain-computer interfaces (BCI) and haptics creates more immersive user experiences. The necessary **security architecture** for these systems leverages advanced encryption as well as distributed, self-healing systems that make use of swarm intelligence. Performance is maintained through load balancing, edge computing and efficient data storage solutions, while standardised protocols and APIs enable the seamless integration together of different virtual environments.

Stakeholders who participated in the conference and the consultation leading up to it emphasised that trust among users, businesses, and society is essential for the development of Web 4.0 and virtual worlds. To foster this trust, **transparency and accountability** must be embedded by design across products and services. Users must be able to clearly differentiate between real and virtual environments, with virtual entities readily recognisable (i.e. identifiable), thereby ensuring an intuitive and understandable experience. **User protection and well-being** should be prioritised at every level of service design, from privacy-preserving infrastructure to proactive safeguards against digital harassment. These norms should be upheld through standardised protocols that ensure cross-platform interoperability, the identifiability of responsible human actors (system developers and users), as well as robust security measures and fair economic practices.

Technical principle 5: Integrating secure practices, privacy-enhancing technologies and data controllability by design across services and systems to mitigate security and privacy risks and data ownership issues

Web 4.0 technologies are fundamentally data-driven. When data is aggregated across multiple connected devices, users face increased privacy and security risks. The environments of virtual worlds and immersive technologies can thus be vulnerable to misuse, making robust security measures and comprehensive user protections essential. For example, the growing adoption of IoT devices and the development of emotional recognition systems are creating new categories of sensitive personal data that require strict protection. Another future risk is that the advanced processing power of quantum computers – especially cryptographic-relevant quantum computers (CRQC) – may eventually enable them to break many of the public-key encryption algorithms used at present, including those used in digital signatures (such as DNSSEC) and secure communications (such TLS)[108]. To mitigate this risk, post-quantum cryptography (PQC) has been an active field of research and development[109,110,111,112]. These algorithms do not require quantum computers but can be run on existing computers while being resistant to quantum attacks. The IETF[113] has recognised the importance of developing cryptographic standards that are resistant to quantum attacks and has been working on updating existing protocols and developing new ones that incorporate PQC algorithms.

From a technical perspective, new technologies for **privacy protection and personal data control** in immersive environments can provide solutions that safeguard personal information. Examples of these include self-sovereign identities (SSIs), which empower users to control their own identity and data without relying on centralised authorities. Privacy-enhancing technologies (PETs) are another significant advance. These protect personal data using techniques such as differential privacy, which adds noise to data to prevent the identification of individuals. Meanwhile, AI-driven privacy enforcement is also emerging. This utilises real-time monitoring and consent automation to ensure compliance with privacy regulations and user preferences.

Alongside the protection of personal data, a framework is needed for creating, protecting, securing, publishing and ultimately monetising **personally created assets**. For example, in virtual world platforms such as Second Life or Roblox, users can create their own content – e.g. avatars, shops and games– and can provide these to other users. Ultimately, ownership and protection of IP and usage rights should be well defined, and a fair balance should be struck between the platform provider and the user, in order to provide a viable business model for the monetisation of such assets by their creators.

Several participants of the conference and the stakeholder consultation pointed out that **users require robust, reliable systems that protect privacy and security**. Ensuring such protection demands that continuous improvements are made to cybersecurity and data protection practices. To build user trust and respect autonomy, organisations should provide transparent information about the data they store, including retention periods, the types of data collected, and its intended uses. Data collection and sharing should be limited only to what is necessary for service provision. While users should

[108] ICANN Office of the Chief Technology Officer (2022). *Quantum* Computing and the DNS. Available at: https://www.icann.org/en/system/files/files/octo-031-11feb22-en.pdf
[109] NIST PCQ standardisation project involving researchers around the globe. Available at: https://csrc.nist.gov/Projects/post-quantum-cryptography
[110] NIST (2024), NIST Releases First 3 Finalized Post-Quantum Encryption Standard. Available at: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
[111] ETSI Quantum-Safe Cryptography (QSC) focusing on the practical implementation of quantum safe primitives. Available at: https://www.etsi.org/technologies/quantum-safe-cryptography
[112] AIVD, CWI and TNO publish renewed handbook for quantum-safe cryptography. Available at https://www.tno.nl/en/newsroom/2024/12/renewed-handbook-quantum-safe-crypto/
[113] IETF Post-Quantum Use in Protocols (pquip) working group to the corresponding work across the organisation. Available at: https://datatracker.ietf.org/wg/pquip/about/

maintain meaningful authority over their personal data, this must be balanced against the potential benefits of creating comprehensive datasets that combine together information from different individuals in order to advance scientific research, foster innovations in healthcare, improve public services or develop more effective AI systems.

Developers and companies working on Web 4.0 technologies must follow the "**security by design" paradigm**. Embedding cybersecurity measures from the outset not only protects computing infrastructure from attacks but also ensures that computing is secure without compromising privacy. Robust AI and data management practices, reinforced by strict security protocols, can safeguard sensitive information and minimise vulnerabilities. Secure identity verification and management methods are essential to fostering trust, recognisability (identifiability), of virtual entities preserving user autonomy, and preventing impersonation or identity theft. **Privacy-enhancing technologies** should be integrated into system design, respecting cultural diversity, regulatory requirements and global ethical principles. Finding a balance between identity verification and anonymity is crucial to maintaining user privacy while upholding security and system integrity.

Technical principle 6: Integrating sustainability by design across the ICT technology stack to reduce energy consumption, material use and waste

Sustainability is essential to the future of Web 4.0 and virtual worlds. The computational demands of AI, immersive environments and blockchain networks together with the vast amount of data storage required translates into **substantial energy consumption and water usage** for cooling systems, as well as **electronic waste** resulting from rapidly obsolete hardware. Moreover, the production of digital technologies, particularly semiconductors, relies heavily on **rare materials**, contributing to environmental degradation and ethical issues surrounding the extraction of raw materials, including human rights violations, further complicating the sustainability of Web 4.0 technologies.

Importantly, Web 4.0 technologies can enable innovative use cases that will become even more prominent in the future. By leveraging AI-assisted resource management, digital twins, digital product passports, smart grids and environmental monitoring systems, these technologies could help to reduce energy consumption, material use and waste. These technologies provide data-driven insights and facilitate behavioural changes, empowering individuals and organisations to make more sustainable choices.

Stakeholders who took part in the conference discussions and the consultation leading up to it noted that Web 4.0 technologies and the future internet must be developed with **a strong focus on enhancing resource efficiency and minimising its carbon footprint**. Developers and companies should adhere to the principles of sustainability at every layer of digital infrastructure, from electricity grids to data centres, application development and end-user devices. This includes minimising the use of materials and the production of waste through the adoption of sustainable practices such as hardware recycling and the re-use of components. Solutions such as digital product passports could be used to increase transparency by tracking materials, ethical sourcing and carbon footprints, ensuring accountability in technology supply chains. The development of Web 4.0 technologies and the underlying internet infrastructure requires significant investment and resources. This includes the extraction of raw materials such as cobalt, lithium, selenium and nickel. It is essential to minimise the harm associated with the production of technology, including in its supply chains. Given the technical complexity of achieving the required efficiencies and the policy support that will be needed, an explicit multi-stakeholder approach is essential.

4. Recommendations

Internet governance must adapt to the significant advances in immersive technologies, AI, IoT, future communication networks and other developments. To achieve this, it is crucial to take a multistakeholder approach that brings together contributions from governments, businesses, the technical community, academia, civil society and users. Such an approach combines the values, experience and expertise needed to navigate the complexity and rapid evolution of emerging technologies. The present document proposes **six policy principles and six technical principles** that should guide internet governance in view of the evolution towards Web 4.0 and virtual worlds. These principles focus on foundational values, rights and approaches, as well as on design, operational aspects and technological characteristics.

This chapter **presents recommendations** for areas of action to support the effective governance of the future internet and foster adherence to the policy and technical principles. The principles and recommendations proposed have emerged from an open, bottom-up stakeholder consultation process. While stakeholders expressed a diverse range of opinions, the recommendations have been designed to reflect the direction of the discussion.

The underlying issue that requires attention and action from internet governance institutions and the stakeholders **is maintaining an open, distributed and interoperable global internet** that upholds human rights, rather than allowing it to fragment into disconnected splinternets. In this process, it is essential to rely on the existing internet governance institutions and to support their adaptation to address technologies related to Web 4.0 and virtual worlds.

Adhering to the policy and technical principles outlined in this paper requires action across multiple domains. The recommendations and areas for action are aimed at a broad audience, including internet governance institutions, civil society, the technical community, academia, developers, businesses and governments. Each of these groups of stakeholders will contribute to shaping the future of the internet, from technical standard-setting and policymaking to the discussion of ideas, monitoring, oversight and user advocacy.

Recommendation 1: Develop guidance documents to ensure human rights-based, ethical and coherent global internet governance as Web 4.0 and virtual worlds emerge

Stakeholders should act to uphold human rights, privacy, security and accessibility, and to ensure predictable and transparent regulatory environment, ensuring that individuals are protected from exploitation, abuse or harm in increasingly immersive digital environments. Governments and businesses should avoid actions that undermine the dignity and autonomy of individuals. Human rights should be protected through ethical design, regulatory oversight and accountability mechanisms.

Various stakeholders, including technology providers, technical experts, end-users, children's rights advocates, youth, indigenous communities and human rights organisations, need to be meaningfully involved in the development of guidelines for ethical conduct in the context of technological developments related to Web 4.0. Guidance documents such as guidelines, codes of conduct, codes of practice, toolkits and best practices can facilitate dialogue, promote common understanding and foster collective commitments in a horizontal, open and multi-stakeholder environment. Such documents are essential for coordinated action in support of a human rights-based, ethical and coherent global future internet. The development of guidance documents would also serve as a framework for raising awareness, improving technological literacy and skills, and widening access to technology – all of which are critical to fostering public acceptance and long-term engagement.

Table 1. Recommendation 1: areas for action

Area for action	Stakeholders involved
Develop ethical guidelines that consider the unique needs and risks faced by different communities and stakeholder groups in view of the evolution towards Web 4.0 and virtual worlds. In particular: • Such guidelines should cover risks to human rights, children's rights, digital exclusion, algorithmic bias and online exploitation, and should propose concrete mitigation measures. • When developing the guidance documents, it is crucial to consider security, privacy, sustainability, data ownership and user protection across the entire value chain, while also accounting for their impact on other layers, systems and the distributed architecture of the internet. • The guidelines should include specific measures to protect vulnerable and marginalised groups.	Civil society and human rights organisations, the end-user community, youth organisations, governments, other public authorities, academia. The national and regional IGFs could be involved in the facilitation mapping of culturally and regionally specific risks and good practices in the safeguarding of human rights in virtual spaces.
Companies developing virtual worlds and Web 4.0 technologies should develop and adopt ethical codes of conduct with regard to user protection, paying particular attention to vulnerable groups, privacy rights and the prevention of algorithmic bias. These should include: • Self-assessment tools, transparency/reporting principles, standards and methodologies for inclusive design, development and implementation. • Commitment to the use of technology impact assessments and due diligence processes, with a view to identifying negative impacts on human rights and freedoms online. • Codes of conduct for high-risk sectors such as healthcare.	Companies providing virtual worlds and Web 4.0 related technologies, the technical community, civil society organisations.
Engage in awareness raising about the human rights considerations and risks involved in virtual worlds, in relation to data collection, misinformation, identity theft, etc.	Civil society and human rights organisations, the end-user community, youth organisations, IGF regional chapters, governments, academia.

Recommendation 2: Involve diverse stakeholders from different regions in the development of standards for the future internet in collaboration with the appropriate standards development organisations

The development of Web 4.0 and virtual worlds should be based on open, widely adopted standards and protocols that promote interoperability and security across platforms and networks. Given the global and multi-faceted nature of the internet, the development of standards for Web 4.0-related technologies also requires a multi-faceted, issue-based approach. It is essential that the process of

developing standards remains inclusive, open and multi-stakeholder to ensure that the future internet continues to function as an open, distributed and interoperable global internet.

Although SDOs typically work together and complement each other, overlap and fragmentation sometimes occur. It is therefore essential to foster cooperation and liaison between technical standards bodies, policy and governance organisations, and industry.

SDOs should ensure that new or improved standards do not compromise interoperability and backward compatibility. A forward-looking but measured approach to the development of standards and protocols must balance innovation with the preservation of the core principles underpinning the architecture of the internet. The standards developed by SDOs are open but remain voluntary and are only effective if they are widely adopted by the global community.

The development of standards for Web 4.0 and virtual worlds should be based on a global, multistakeholder process to ensure coherence, avoid fragmentation and address the needs of the Global South.

Currently, the standards developed by SDOs are often treated as recommendations rather than binding requirements. However, the implementation of new or improved standards – especially those relating to security and privacy – should be strongly encouraged.

Standards can either promote or restrict human rights, depending on how they are applied. Therefore, it is necessary to adopt and apply standards in a way that provides a strong basis for the protection and promotion of human rights. When developing standards, it is essential to incorporate the principles of accountability, transparency, security, privacy, sustainability, data ownership and user protection throughout the end-to-end value chain. Despite the distributed architecture of the internet, it is essential to maintain a comprehensive understanding of its end-to-end functioning and the potential impact of new standards on other layers or systems. This holistic approach will ensure that standards are robust and effective.

Table 2. Recommendation 2: areas for action

Area for action	Stakeholders involved
Support the active participation of all stakeholders in the global standardisation process: • Provide funding for experts to participate in the standardisation process in established organisations, including participants from less developed regions. • Reduce fees and barriers to entry into SDOs, specifically for representatives from the Global South, members of marginalised communities, civil society organisations and SMEs. • Enable online and hybrid consultation in different languages. • Provide capacity-building initiatives to ensure all stakeholders concerned can participate in the standardisation process. Ensure all stakeholder groups (including vulnerable and minority groups) are represented.	SDOs, companies, civil society organisations, governments.
Foster communication and collaboration between SDOs and other actors involved in the development of standards for the future internet: • Devise structured mechanisms for coordination between standards bodies while maintaining space for innovation. Focus on efficient, inclusive processes for standards development. • Foster the participation of and collaboration between stakeholders to develop practical guidelines for implementing standards effectively. Such fora act as bridges between industry players, SDOs and other organisations, ensuring proper coordination and consistent implementation of technical standards.	SDOs, liaison officers, companies, civil society organisations.
Integrate human rights considerations into the development of standards for the future internet: • Make human rights an integral part of the standardisation process by increasing awareness among stakeholders and systematically assessing human rights. • Make standard-setting processes transparent, open and inclusive, ensuring that all relevant documentation is free and publicly available.	SDOs, companies, civil society organisations.
Take action to facilitate the adoption and implementation of standards developed by SDOs in relation to Web 4.0 and virtual worlds technologies: • Provide clear, comprehensive implementation guidelines and documentation, and develop reference implementations and open-source tools. • Ensure backward compatibility where possible, provide clear migration paths from legacy systems, and support interoperability testing. • Ensure alignment between standards and regulatory requirements. • Build communities of practice for knowledge sharing, facilitate peer-to-peer learning, experimenting and experience sharing, and create feedback loops between implementers and standards developers.	SDOs, companies, civil society organisations, regulatory bodies within state governments.

Recommendation 3: Proactively assess the risks and related governance needs associated with Web 4.0, virtual worlds and related technologies

Internet governance institutions should continue employing a multistakeholder approach, engaging diverse stakeholders to proactively identify emerging risks and opportunities and their impact on the internet, while harnessing multistakeholder governance sandboxes to co-create solutions for cross-cutting issue areas. In the context of the forthcoming World Summit on the Information Society (WSIS) +20 review, stakeholders should take steps to strengthen the role of internet governance institutions in taking a forward-looking approach. The IGF should remain the main forum for the exchange of ideas, coordination and policy-relevant messages. Stakeholders within the IGF and other internet governance institutions (ICANN and the ITU, IETF, W3C and other SDOs) should within the bounds of their evolving responsibility for the technology stack coordinate their actions, adopt an issue-based approach, and avoid the duplication of efforts.

Table 3. Recommendation 3: areas for action

Areas for action	Stakeholders involved
Incorporate workstreams (into the operation of the organisations) that focus on the implications for the future internet of Web 4.0 and virtual worlds • Anticipate risks to the maintenance of an open, distributed and interoperable global internet • Prioritise sustainability, resilience and inclusivity, ensuring that the internet remains a valuable and equitable resource for generations to come • Engage technology developers, venture capitalists and innovators in multistakeholder discussions about the future of the internet	IGF, ICANN, the ITU, IETF other internet governance organisations, industry bodies, civil society organisations, national governments, public authorities.
Adopt multistakeholder governance sandboxes within existing governance institutions to innovate and test approaches tackling cross-cutting issues requiring input from diverse stakeholder groups. Those environments can provide a structured setting for experimentation, which enable the testing of different policy approaches, innovative solutions and consensus building by involving diverse and appropriate stakeholders.	Depending on the issue areas being discussed, stakeholders involved in internet governance bodies, civil society organisations, the technical community, industry, academia, national governments, other public authorities.
Conduct impact assessments to determine the impact of new policies, initiatives and regulatory measures on the operation of the internet.	Stakeholders involved in internet governance bodies, civil society organisations, the technical community, industry, academia, national governments, other public authorities.
Conduct risk assessments in relation to the technologies associated with Web 4.0 and virtual worlds, to ensure that internet governance frameworks can proactively address the challenges identified and remain resilient.	Stakeholders involved in internet governance bodies, civil society organisations, the technical community, industry, academia.

Recommendation 4: Facilitate policy coordination between governments, including the involvement of multistakeholder institutions, to address the impacts on the internet of Web 4.0 and virtual world technologies

National governments, regional governments and international institutions have already adopted (or are working on) guidelines, policies and regulations on issues that are relevant to the evolution towards

Web 4.0 and virtual worlds. These include policies on privacy, security, innovation, transparency and accountability. Without proper information sharing, cooperation and coordination, the application of different rules in different jurisdictions would create costs for businesses and opportunity costs for innovation, and could weaken interoperability, hinder user access and exacerbate the digital divide.

Policy coordination requires a global approach that includes the active involvement of diverse actors in multistakeholder institutions. Such coordination entails creating conditions that enable stakeholders (policy actors, businesses, civil society organisations, the technical community, users and others) operating under different legal frameworks and jurisdictions to effectively exchange ideas, and to collaborate and align regulatory approaches as far as possible. Internet governance institutions should work transparently and monitor the adherence of stakeholders to principles such as those presented in this document, with the aim of ensuring effective governance.

Table 4. Recommendation 4: areas for action

Areas for action	Stakeholders involved
Foster a global policy coordination dialogue with regard to virtual worlds and Web 4.0 technologies: • Discuss policy alignment on issues pertinent to virtual worlds and Web 4.0 technologies within dedicated multistakeholder fora. • Prioritise global coordination in high-risk areas such as identity management, accessibility, abuse prevention, and sustainability. • Encourage exchanges concerning best practices and policy lessons. • Discuss adherence to policy and technical principles, review existing principles, and introduce new ones as needed.	Stakeholders involved in internet governance bodies, civil society organisations, the technical community, industry, academia, end users, national governments, other public authorities.
Ensure the inclusion of diverse underrepresented groups to tackle digital divides and prevent regulatory biases • Introduce capacity-building initiatives to ensure that all stakeholders are well equipped to take part in policy coordination dialogues.	Stakeholders involved in internet governance bodies, civil society organisations, the technical community, industry, academia, end users, national governments, other public authorities.