



Decentralisation and European sovereignty in Web 4.0

Policy brief

AUGUST 2026

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



Introduction

The transition to Web 4.0 is a rare inflection point, and **the choices the EU makes in the coming years will shape its digital ecosystem for decades**. As physical and digital environments merge, and billions of people, devices and AI agents begin to interact, the Union has an opening to shape the rules, standards and architecture of the next web rather than inherit them.

The central policy problem is whether Web 4.0 reproduces the concentration of the Web 2.0 platform economy at new layers of the stack¹. The EU enters this transition with significant dependencies on a small number of predominantly non-European providers across digital services, data infrastructure, cloud and AI capacity². AI agents could create new forms of gatekeeping over functions such as search, browsing and access to services³, while continued vertical integration could extend existing market power across several layers at once⁴. How far Web 4.0 creates genuine alternatives or reinforces these dependencies will therefore affect the EU's sovereignty, resilience and competitiveness.

Decentralising the control and delivery of Web4.0 services and data can be an opportunity to “change the rules of the game”, currently dominated by the centralised hyperscalers, and restore European sovereignty in the digital world.

This brief examines decentralisation, federation and open architectures as possible ways to reduce these dependencies and widen choice. They are not objectives in themselves. Their value depends on whether they give users and organisations viable alternatives, reduce reliance on individual providers, and keep critical services and infrastructure open to different providers and approaches.

1.1. Scope of the brief

Decentralisation is best understood at a multidimensional spectrum that encompasses technical architecture, governance arrangements and the distribution of control. Systems can be decentralised in some dimensions while remaining centralised in others. **This brief focuses on the technical and architectural dimensions**, or how data and services are organised across networks, while recognising that these technical choices carry implications for governance, market power and society.

Therefore, in this brief, **decentralisation refers to a shift of digital architectures and data governance away from single points of control**, towards systems in which functions are distributed across multiple independent participants. It can take different forms. **Distributed** architectures spread functions or resources across multiple nodes, locations or providers, while **federated** architectures connect independent organisations or systems that retain control of their own resources but operate through common rules or interfaces. In practice, most systems are hybrid, combining centralised, federated and distributed elements at different layers of the stack^{5,i}.

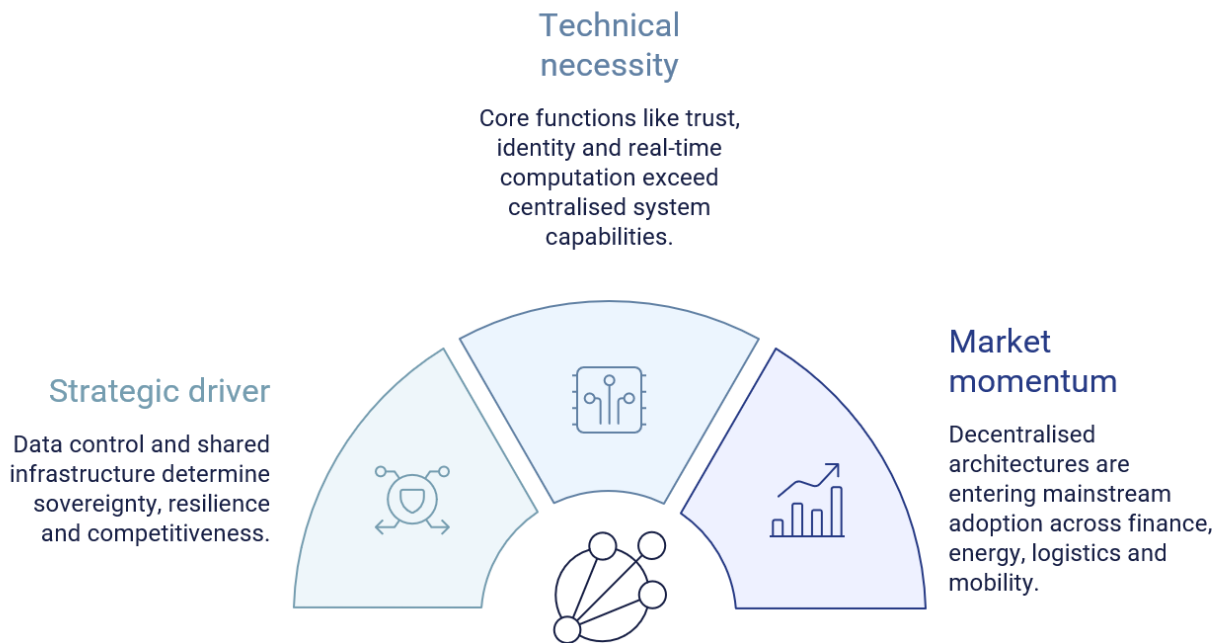
Whether this produces meaningful decentralisation also depends on the surrounding conditions. Open protocols, shared standards and digital commons – including open code, knowledge and data – can allow different providers and systems to participate without dependence on a single intermediary⁶.

ⁱ For simplicity, this brief uses the term “decentralisation” when discussing the broader strategic direction, and “distributed” or “federated” when the specific technical or organisational model matters.

1.2. Role of decentralisation in Web 4.0

The strategic case for decentralisation is that it can help change where control over Web 4.0 sits. The EU already depends heavily on a small number of predominantly non-European providers across digital services, data and infrastructure. As new markets form around AI agents, identity, data exchange and computing capacity, decentralised and federated models can provide alternative routes and reduce dependence on individual providers. Their importance therefore comes first from their potential contribution to sovereignty, resilience and competition, reinforced by technological developments and emerging adoption.

Figure 1. Forces driving Web 4.0 decentralisation



Source: authors' elaboration

The first and most important driver is strategic. The distribution of control in Web 4.0 bears directly on the priorities of sovereignty, resilience and competitiveness highlighted in the Draghi report⁷. Where distributed or federated architectures allow users and services to move between providers, they can make markets more contestable and reduce single points of dependency.

Where the coordinating elements of distributed systems remain open and accountable, decentralisation can support shared resources that no single actor controls, such as open protocols, software and knowledge. Because the benefits of these resources are widely shared, private actors often have limited incentives to fund their long-term maintenance. Their sustainability therefore often depends on public funding, community contributions and other forms of collective support^{8,9,10}.

However, **decentralised architecture does not always disperse market powerⁱⁱ**. Control can remain concentrated in data, platforms, standards, wallets, software or other coordinating functions. Web 3.0 provides a cautionary example: distributed protocols did not prevent the emergence of new intermediaries and concentrations of control.

ⁱⁱ The two sit on different axes: a system can be architecturally distributed across thousands of independent nodes yet remain politically and economically controlled by a few actors. A blockchain network run by a single consortium spreads computation while keeping governance, access and revenue with its operators.

The lesson for Web 4.0 is therefore that decentralisation can support sovereignty only under the right conditions. Participants need to be able to interoperate, users and services need credible alternatives, and shared elements on which systems depend need to remain open and accountable. The strategic question is not how decentralised Web 4.0 becomes, but whether its architecture creates genuine choice and reduces critical dependencies.

The second reason is technical. Some Web 4.0 functions benefit from more distributed architectures. These include processing data closer to users and devices, privacy-preserving collaboration across data holders, distributed storage and mechanisms for verifying information across organisational boundaries¹¹. Distribution can improve resilience, privacy or performance in these cases, although the appropriate architecture will differ by function.

The third driver is the emerging adoption. Finance provides one of the clearest examples¹², where regulated institutions and central banks are increasingly experimenting with distributed ledgers, tokenisation and programmable settlement within accountable frameworks^{13,14} (see also Box 4). Energy provides a different example, as renewable generation, storage and flexible demand create more distributed physical assets while the digital layer coordinating them is still developing (see also Box 3). **At the network and infrastructure layer, the main strategic issue is resilience and dependence on a small number of non-European providers.** Europe relies heavily on external firms for connectivity and computing capacity, and some of this dependence is tied to physical assets. The region accounts for around 4.8 per cent of global AI supercomputer performance, compared with 74.4 per cent for the US and 14.1 per cent for China. European-owned capacity on subsea cables between Europe and North America is also limited, while US hyperscalers account for around 90 per cent of that capacity. This creates both economic dependence and potential points of vulnerability in infrastructure on which Web 4.0 services will rely.

Technically, the internet is already highly distributed. It is built on open protocols and independently operated networks, with only a limited number of shared functions, such as the naming root, requiring common coordination. The main concentration problem at this layer is therefore not the internet's basic architecture, but ownership and control of the infrastructure networks run on. Subsea cables, data centres, compute capacity and other critical assets are increasingly owned or operated by a relatively small number of firms. This means that a technically distributed network can still be highly concentrated in economic and operational control. For this brief, the relevant question is therefore whether greater distribution of infrastructure also reduces dependence on individual providers, rather than whether the network is distributed in technical terms.

This concentration is increasingly reinforced by vertical integration. The same large firms can now span subsea connectivity, data centres, cloud infrastructure and services running above them. This can concentrate control over several parts of the infrastructure chain in the same companies. The EU has started to examine some of these dependencies. Under the 2025 EU Action Plan on Cable Security, for example, an expert group is mapping submarine cable infrastructure, including ownership, capacity and landing points.

More distributed infrastructure can improve resilience by spreading capacity across locations and nodes. It can also contribute to decentralisation where capacity and control are spread across independent providers rather than remaining with a single operator. Edge and peer-to-peer architectures do this by moving computing, storage or connectivity closer to where they are needed and across a wider range of nodes. DePIN is one example, using digital incentives to coordinate physical resources contributed by independent operators. But a technically distributed system can still remain concentrated in ownership or governance, for example where one platform or software provider coordinates the participating resources.

This also creates opportunities in areas where market positions are not yet fixed. The Commission's Expert Forum on Frontier AI similarly identified secure and verifiable AI infrastructure as an emerging layer of the global stack where no actor yet holds a dominant position and Europe could take leadership.

The same issue is visible in strategic sectors where physical infrastructure is becoming more distributed. Energy is the clearest case, since digitalisation is turning the grid into a network of independent nodes, and the same questions of resilience and dependence arise there directly (see Box 4). Defence and space point to a second, more forward-looking case. Modern defence systems increasingly depend on satellites, sensors, autonomous systems and edge devices that must continue operating when individual links or nodes fail. In both cases, technical distribution can support decentralisation only if it also reduces dependence on individual suppliers or coordinating platforms.

Many of the underlying technologies are also dual-use, including satellite connectivity, AI, edge computing, secure communications and distributed sensing. As European defence investment expands, this could create additional demand for European infrastructure and suppliers. EU defence and space initiatives already emphasise interoperability, modularity and systems that can work across multiple components and operators. The opportunity is therefore to use new investment to strengthen resilience and supplier diversity, rather than replacing one dependency with another.

Europe does not need to decentralise infrastructure simply because technical distribution is increasing. Web 4.0 is likely to increase demand for distributed and edge deployment, because many real-time and agentic applications benefit from processing closer to where data is generated and used. The policy question is whether this technical shift also creates greater provider choice and reduces strategic dependencies.

The key question is therefore whether more distributed infrastructure also leads to greater decentralisation of control. New capacity can still be controlled by the same firms that dominate today's cloud and digital infrastructure markets. Dependence can also move to the software and interfaces used to coordinate distributed resources. Interoperability, open interfaces and the ability to use multiple providers therefore matter as much as physical distribution itself.

The **energy sector illustrates this particularly clearly** because its physical assets are becoming more distributed while the digital coordination layer is still taking shape. Defence and space offer a more forward-looking case, where distributed communications, sensing and edge processing can increase resilience and reduce dependence on individual infrastructure nodes or suppliers.

These examples do not imply that every sector should follow the same model. Rather, they show that different combinations of centralised, federated and decentralised architectures are already emerging, and that the EU still has scope to influence who controls their critical components.

Box 1. Three models of a decentralised transaction layer: examples from US, EU and China

The **US is promoting privately issued dollar stablecoins, which hold about 99.8 per cent of the global market**¹⁵, under legislation that requires issuers, including foreign ones serving US customers, to be able to freeze or block tokens on lawful order¹⁶. **China is scaling a state-operated digital yuan**¹⁷. This sits within a far larger national data effort. Under the 2025 National Data Infrastructure Construction Guidelines, China aims to complete a nationally coordinated data infrastructure by 2029. The National Data Administration preliminarily estimates it will attract around CNY 400 billion (USD 54.5 billion) in direct investment annually^{18,19}. That figure covers the national data infrastructure, from data circulation to computing and network facilities, within which blockchain-based capabilities such as trusted data circulation, smart contracts and cross-chain interoperability are one component of the investment²⁰. Ultimately, in each case, control can remain concentrated even where parts of the architecture are technically distributed.

The EU is charting a third path. It pairs public settlement anchors under accountable governance with regulated private assets on open rails, anchored by central bank money, as the Eurosystem sets out in its Comprehensive Payments Strategy²¹. Set against the other two, what separates them is not how decentralised each is, but where legal authority sits. A dollar stablecoin is architecturally open, but it embeds foreign legal authority in the transaction layer, since its issuers must enforce US law on the network. China's model distributes operation while embedding state control in the architecture itself. The European hybrid distributes operation on open rails while anchoring legal authority in accountable European institutions, seeking to combine distributed operation with accountable European governance. This is why the European model can

serve as a reference for other sectors, though the transaction layer is far from settled and sectors may legitimately reach different balances depending on what they need from settlement.

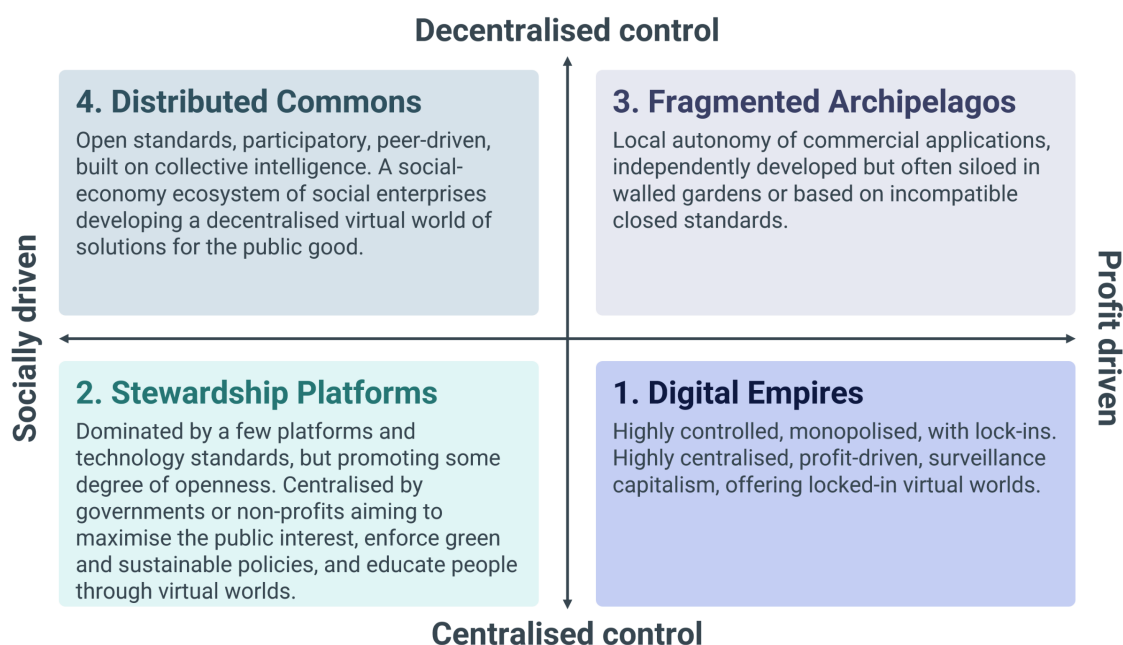
The EU already has important policy levers to influence this transition. Its strengths in standards, open-source development and interoperability are being reinforced by instruments including the Open Source Strategy²², Cloud and AI Development Act (CADA) and major investments in European digital infrastructure^{23,24}. These measures address different parts of the problem, but they do not by themselves ensure that new capacity and services remain contestable or that alternatives reach sufficient scale.

The gap is therefore in how existing instruments are used together. Open standards remain important, but they need to be complemented by practical implementations, sustained digital commons, public investment and demand-side measures that preserve interoperability, portability and choice between providers. The chapters that follow examine this challenge from the web layer, through the data layer, to the network and infrastructure layer, where the underlying dependencies ultimately sit.

1.3. Scenarios for Web 4.0

This policy brief sets out **four plausible future scenarios** for how the Web 4.0 ecosystem could develop, mapped along two axes: the degree of control and what drives the ecosystemⁱⁱⁱ.

Figure 2. Four future scenarios^{iv} for Web 4.0, by degree of control and dominant driver



The **Digital Empires** scenario is the closest to today, whereby a few dominant, mostly non-EU platforms control infrastructure and data, with limited interoperability and diminished user autonomy. Meanwhile, **Fragmented Archipelagos** is close to where permissionless blockchain ecosystems sit now.

ⁱⁱⁱ For a more detailed analysis of the four scenarios, consult the paper 'Decentralised data and service architectures' developed by PMO and TNO as part of the Web4Hub project.

^{iv} These scenarios may coexist in different sectors and regions, and each carries a distinct mix of benefits and drawbacks for different beneficiaries – large industry, SMEs, civil society and citizens – and for different purposes, from economic growth to democratic resilience and sovereignty.

Stewardship Platforms and Distributed Commons are the alternatives – the first reachable by binding today's dominant platforms to public-interest rules, the second only by building open, commons-based infrastructure from a much earlier stage. Distributed Commons also relies on collective intelligence, with users and communities contributing to and governing the knowledge, data and other commons on which digital services depend.

Out of this analysis, a combination of **Distributed Commons and (European) Stewardship Platforms is the approach most aligned with the EU's goals of sovereignty, openness and shared value.** Reaching it would require more than open standards. Without deliberate intervention involving substantial public funding, long-term commitment and strong regulatory support, incumbents are likely to deploy first and convert existing advantages into durable positions in the next web. The policy challenge is therefore to change the conditions under which deployment takes place: sustain digital commons across software, infrastructure, data and shared knowledge; use public procurement and first-customer demand to give open alternatives a route to scale; and attach interoperability, portability and multi-provider conditions to publicly supported infrastructure before new concentrations become entrenched.

1.4. Structure of the policy brief

This brief examines three layers in the order in which control becomes visible and then traces it down to the foundations on which it depends: the web layer, the data governance layer, and the network and infrastructure layer. The web layer who mediates the services through which users and AI agents interact; the data layer asks who controls the data, credentials and trusted reference points those services depend on; and the network and infrastructure layer asks who owns and coordinates the physical and logical capacity on which the other two layers run. These layers are necessarily simplified, and some functions span more than one: settlement, for example, is experienced through wallets and agent interfaces at the web layer, while the settlement asset, ledger and legal authority sit at the data layer.

The three layers therefore present different forms of the same strategic problem. At the web layer, the immediate risk is gatekeeping and value capture by incumbent platforms. At the data layer, it is control over data and trusted authority. At the network and infrastructure layer, it is dependence on concentrated physical capacity and the coordinating mechanisms that make distributed infrastructure work. The chapters move downward through these dependencies to show where decentralisation, federation and openness can create genuine alternatives and where they cannot.

Two sectoral examples are examined more closely: finance at the data layer, where distributed settlement is already being deployed under supervision, and energy at the network and infrastructure layer, where physical assets are increasingly distributed while the digital coordination layer is still taking shape. They illustrate how the wider transition is already unfolding rather than forming separate subjects of the brief.

Cross-cutting takeaways are summarised in Chapter 5 'Conclusions'.

2. Web layer: changing the value model for Web 4.0 services

At the web layer, the immediate sovereignty risk is gatekeeping: who mediates access to information, services, users and markets. This is the layer users interact with directly, through search and discovery, virtual environments and, increasingly, AI agents acting on their behalf. If these functions consolidate around a small number of incumbent platforms, existing network effects and control over user relationships could extend into the next generation of the web.

At this layer, decentralisation is mainly about reducing dependence on a single platform or intermediary. In practice, **this will often take the form of federated services**, where independent providers remain separate but interoperate through shared protocols. Open protocols and code can support such alternatives, but openness alone does not mean that control is decentralised.

The risk is already becoming visible. Stakeholders at the Global Multistakeholder High-Level Conference on the governance of Web 4.0 and Virtual Worlds identified potential consequences of platform concentration, including hyperpersonalisation, where content and advertising are tailored using far richer behavioural data than today's platforms capture, and self-preferencing, where a platform favours its own services within the environment it controls²⁵. The structural drivers of concentration are also expected to strengthen rather than weaken in Web 4.0: richer data can amplify network effects, new services enable bundling that raises switching costs, and established firms can shape emerging markets in ways that make entry harder for competitors and decentralised alternatives²⁶. Access to information produced or mediated by centralised social networks is also a growing risk for society, ranging from children addiction to geopolitical and democracy twists.

The Web4Hub project's work on agentic AI suggests that this is already happening in specific functions²⁷. In discovery, 2% of cited domains, 185 of the more than 9,000 analysed, account for almost half of citations across leading generative AI services²⁸. At the device level, the firms designated as gatekeepers under the Digital Markets Act²⁹ (DMA) are building agentic action into their operating systems and can decide which agents and services these reach by default³⁰. In commerce, an agent's choice of provider can follow its operator's commercial partnerships rather than the user's preference³¹. Platform power could therefore deepen in Web 4.0 as gatekeeping moves into the agents and interfaces acting on users' behalf. At the same time, these markets are not yet settled, leaving room for alternatives to scale.

Many of the building blocks for such alternatives already exist. Open protocols, shared code and knowledge resources allow services to interoperate without being controlled by a single platform and were central to the development of the open web³². Federated services continue to rely on shared protocols, while open knowledge resources such as Wikipedia provide common resources that many digital services depend on³³. Neither open protocols nor digital commons are themselves forms of decentralisation, but both can make decentralised or federated alternatives easier to build and sustain.

Digital commons are particularly important to this challenge. Because no single organisation captures all the benefits from maintaining open protocols, software and knowledge resources, they are often underfunded and depend heavily on communities and philanthropy³⁴. AI is increasing this pressure. AI services draw heavily on open knowledge, while summaries and other AI interfaces can reduce visits and contributions to the sources that provide it³⁵. Supporting digital commons therefore means supporting not only open-source software, but also the knowledge and other shared resources on which Web 4.0 services depend (see also the paper 'Agentic AI, trust and architecture'³⁶ developed as part of this project).

Europe already uses several open and federated alternatives. Matrix supports secure communications for public-sector organisations in Europe³⁷, while the Commission operates its own Mastodon service³⁸. The same logic is being extended to personal data itself. The Solid protocol, developed by web inventor Tim Berners-Lee³⁹ and piloted by European public administrations including the Flanders government, stores users' data in personal pods under their own access control, decoupling data from the applications that use it⁴⁰. Commercial ventures are now building on open protocols too. **W Social**⁴¹ is a European social network launched in 2026 on the open AT Protocol, with data hosted in Europe and a separate privacy-preserving identity service that verifies users and stores their verified identity attributes on their own devices. These examples show that alternatives exist across public, community and commercial settings. The remaining challenge is not that much about technical feasibility as it is about whether these alternatives can attract enough users and sustained support to become viable choices.

EU programmes already support the creation and maintenance of some of this infrastructure. The Next Generation Internet programme has funded open-internet projects across areas such as identity, federated communication and decentralised infrastructure⁴², while the Digital Commons EDIC⁴³ and the 2026 Open Source Strategy are beginning to strengthen longer-term maintenance⁴⁴. The European EDIC aims to deploy public and other services leveraging decentralised technologies. **These initiatives support openness and shared infrastructure, but they do not by themselves decentralise the web layer.** What remains less developed is support for adoption. Public bodies still face practical costs when moving away from incumbent services, including migration, integration and training. The proposed CADA's "open source first" principle is a step in this direction⁴⁵, but open-source funding needs to be complemented by measures that make adoption easier and create demand for open alternatives^{46,47}.

Agentic AI creates a second issue at the web layer: how agents transact with services. Agents may need to discover a service, agree terms and make payments without direct human involvement. Existing payment systems were not designed for large volumes of automated, small and real-time transactions^{48,49}, while tokenised and programmable settlement may make these transactions easier and cheaper⁵⁰. This is not inherently a decentralisation question. At the web layer, the relevant issue is whether agents can choose between interoperable payment and service providers rather than becoming tied to proprietary interfaces. The settlement assets and governance underneath those payments are considered at the data layer.

Agentic AI also increases the importance of provenance and traceability. As agents generate content and carry out actions on behalf of users, it becomes more important to establish where content came from and which actor performed an action⁵¹. This information should not depend on the records of a single platform. Provenance should instead travel with the content or action and be independently verifiable. Open standards such as C2PA already provide ways to attach verifiable provenance information to digital content. This allows recipients to check information about its origin without relying on one platform. Technologies underpinning the tracing of agent actions are less mature. Full visibility into an agent's internal reasoning may not be feasible, but recording its outputs and externally visible actions is more realistic. One expert consulted for this project also noted that distributed records can make it easier to separate and attribute the actions of different participants⁵².

The EU already has a basis for acting in this area. Article 50 of the AI Act requires machine-readable marking of certain AI-generated or manipulated content from 2 August 2026⁵³. Open provenance standards can help turn such transparency requirements into practical tools that work across services and providers. The objective is interoperability and independent verification, rather than decentralisation for its own sake.

Overall, the market is unlikely to deliver viable alternatives to incumbent platforms at sufficient scale on its own. Incumbent platforms benefit from large existing user bases and network effects, while the protocols and commons on which alternatives depend upon often receive only limited private or public

investments⁵⁴. The policy challenge is therefore to combine **substantial** support for open infrastructure with stronger demand for its use, so that users have viable alternatives before new Web 4.0 gatekeepers become established.

EU policy response:

Current EU instruments address some of the conditions needed for a more contestable web layer, but none directly aims to decentralise it. The DMA addresses the market power of large platforms, including through interoperability requirements for some services⁵⁵. Separately, the 2026 Open Source Strategy and initiatives such as the Digital Commons EDIC and Open Internet Stack support open-source software, protocols and shared digital infrastructure⁵⁶. These can reduce lock-in and make alternatives easier to build, but openness, interoperability and decentralisation are not the same thing. Whether control is actually dispersed depends on whether independent providers can enter, interoperate and attract users at meaningful scale.

More specific action is therefore needed to help open and federated alternatives reach scale. **Three gaps stand out.** First, support for digital commons should extend beyond software to shared knowledge and data resources such as Wikipedia and OpenStreetMap, which are increasingly important inputs to digital and AI services⁵⁷. Second, short-term project funding should be complemented by longer-term support for protocols and services that are already in use but remain under-resourced⁵⁸. Third, public procurement and other demand-side measures should help create users and markets for open alternatives, including through requirements on interoperability, portability and open protocols where appropriate.

These actions should also remain connected to international open-source and digital-commons communities, since many of the protocols and resources used in Europe are maintained globally⁵⁹. The objective should not be to create separate European versions of every open resource, but to ensure that the EU can contribute to, rely on and deploy open infrastructure without becoming dependent on a small number of commercial gatekeepers.

Open services alone, however, cannot deliver sovereignty if the data, identities and settlement systems beneath them remain controlled elsewhere. The next layer, therefore, turns to who controls those underlying data and trust functions.

Recommendations:

- **Develop and deploy “EU Stewardship Platforms” at scale and over a stable timeframe, as viable decentralised alternatives to incumbent Web 4.0 platforms.** Use existing and future EU programmes to support open and federated social networks and virtual environments, with sustained support for their operation, protocols and shared components. Promote wider adoption of such services notably by SMEs and the general public, paired with demand-side incentives for firms building solutions on decentralised approaches⁶⁰.
- **Complement this with support for open-source development and maintenance of digital commons with stronger demand-side measures.** Incentivise bottom-up development of commons and use public procurement to create demand for open alternatives, including through interoperability, portability and open-protocol requirements where appropriate. Procurement and support measures should also address practical barriers to adoption, such as migration, integration and training costs.
- **Extend support for digital commons beyond software, nurturing new collective intelligence mechanisms.** Open knowledge and other shared resources on which Web 4.0 and AI services depend should receive more sustained support alongside open-source code. This should include resources built and maintained through collective contributions, helping preserve and expand a strong base of human-created and human-validated knowledge.

Developing this vision requires strong research and regulatory support for portable and independently verifiable provenance of content, including AI-generated content and agent actions. Article 50 of the AI Act and open standards such as C2PA provide a basis for enabling provenance information to travel with content and be checked across services without relying on a single platform. For AI agents, development should focus first on traceability of outputs and externally visible actions, where technical solutions are more mature.

3. Data governance layer: who controls the trust infrastructure?

At the data layer, the main sovereignty risk is concentration of control over data and the systems used to verify it. Web 4.0 services will depend on growing volumes of data generated by people, AI agents, devices and virtual environments⁶¹. This creates two related questions around who stores, processes and controls that data, and who can verify the identities, credentials and claims on which services rely.

Europe already depends heavily on a small number of non-EU cloud providers, who hold around 70 per cent of the cloud market in the region⁶². This matters not only because of market concentration, but because data held by foreign providers may remain subject to foreign law even when it is stored in the EU^{63,64} (see also Box 3 below). This creates a risk that the same providers become the main route through which Web 4.0 data is stored, accessed and exchanged.

EU policymakers have begun to address this concentration from two directions. The Data Act works on the demand side⁶⁵, making it easier for users to switch between providers or combine several, while the CADA⁶⁶ works on the supply side, building European capacity and explicitly referring to distributed and decentralised cloud and edge approaches among its priorities^v. These measures can increase choice and reduce lock-in, but they do not by themselves ensure that new capacity remains interoperable or that control is spread across several providers.

A second challenge concerns the trusted information on which Web 4.0 services depend⁶⁷. Identity systems will increasingly need to verify not only people, but also AI agents, devices and digital assets⁶⁸. Concentrating these functions in a small number of systems could create new dependencies and security risks. The credentials and other trust mechanisms introduced today will also need to remain secure over time, including through the transition to post-quantum cryptography⁶⁹.

These concentration risks create a case for reducing reliance on single providers and points of control. Decentralised and federated approaches can contribute to this, but not every trust function can be fully decentralised. A credential can be stored or verified through technically distributed systems, but an accountable organisation still needs to confirm many of the facts behind it. This includes whether an identity is genuine, whether a qualification was issued legitimately or who owns an asset^{70,vi}. Identity and credential systems therefore often use hybrid architectures: technical functions may be distributed, while trusted issuers or registries retain responsibility for confirming real-world claims^{vii}. This need does not disappear as the technology matures, because someone must remain accountable for the facts being certified and for deciding which issuers and claims are recognised⁷¹.

The sovereignty question is therefore not simply whether a system is decentralised, but **whether reducing technical dependence also reduces concentration of control, and who governs the trusted**

^v Here, “distributed” refers to capacity spread across multiple locations or nodes, while “decentralised” refers more broadly to reducing dependence on a single point of control.

^{vi} This is known as the “oracle problem”: a distributed system can cryptographically prove that a claim was made and by which key, but cannot itself verify whether the claim is true of the real world – that verification always resolves to some external, accountable source. Its identity-specific form contributed to the collapse of the Sovrin network in 2025, when credentials issued without recognised, accountable issuers found no relying parties willing to accept them.

^{vii} This applies to trust functions such as identity, credentials and asset ownership. It does not apply in the same way to all decentralised approaches at the data layer. As discussed below, functions such as data storage and privacy-preserving computation can be distributed without relying on the same type of trusted authority.

functions that remain⁷². Web 2.0 showed how widely used login services could give a small number of platforms visibility across many other services and strengthen their existing market position⁷³. In Web 4.0, similar verification functions will extend to AI agents, devices and digital assets^{74,75,76}. It is, therefore, important that these trusted functions do not become another concentrated point of control.

The EU is already developing hybrid and federated approaches that combine greater user or organisational control with accountable governance. The European Blockchain Services Infrastructure (EBSI) and its continuation through EUROPEUM-EDIC provide publicly governed infrastructure for verifiable credentials⁷⁷. The EUDI and Business Wallets allow credentials to be held by users while relying on an agreed European trust framework⁷⁸. Common European data spaces use federated arrangements in which data can remain with different holders while being shared under common rules⁷⁹. These examples show that decentralisation can coexist with clear institutional accountability.

Finance provides a further example of a hybrid model at scale. Distributed ledgers and tokenised assets are increasingly being used alongside regulated institutions and public settlement infrastructure. The technical infrastructure can therefore be distributed while responsibility for issuance, settlement and supervision remains institutionally concentrated and accountable. The box below shows why the governance of these functions matters for sovereignty and what this may mean for other Web 4.0 services.

Box 2. Finance as an early example of hybrid architecture

Finance shows how distributed technology can operate alongside regulated institutions. Tokenised assets and stablecoins are increasingly being used within existing financial frameworks, including under MiCA in the EU⁸⁰. The Eurosystem's Pontes⁸¹ and Appia⁸² initiatives illustrate one approach, combining new forms of tokenised settlement with central-bank and regulated financial infrastructure. This allows parts of the technical operation to be distributed, while keeping responsibility for key functions, such as issuance and settlement, with accountable institutions. For the data layer, the key question is who governs these trusted functions and the rules that make transactions final.

This issue is becoming more important as AI agents begin to transact. Much of the emerging infrastructure for agent payments is being developed by non-EU technology and payments companies. Some important emerging protocols also rely on dollar-denominated stablecoins⁸³. The concern at the data layer is not the payment interface itself, but the settlement asset and rules underneath it. If dollar-based systems become widely used, European agentic commerce could become dependent on settlement arrangements governed outside the EU^{viii,84}. Finance therefore shows that the sovereignty implications of distributed systems depend not only on their technical design, but also on who governs their key trust and settlement functions.

Hybrid models can also support public interest uses. UNHCR has used a regulated stablecoin on an open blockchain to deliver assistance to people displaced by the war in Ukraine⁸⁵. This shows that distributed infrastructure can be used within an accountable institutional framework. However, such systems still depend on the currency, network and providers through which they operate. A pilot in Afghanistan also showed that access can remain limited by connectivity, digital skills and other social barriers⁸⁶. The benefits of distributed systems therefore depend both on their governance and on whether people can access them in practice.

The discussion above **concerns trust functions that require an accountable authority to confirm facts such as identity or ownership**. They do not always require an authority to verify an external fact, so technical distribution can go further, while federated models can allow separate organisations to retain control of their own data and systems⁸⁷. Federated learning, for example, keeps data with participating

^{viii} Examples include the open x402 protocol, developed by Coinbase and now stewarded by the Linux Foundation, which enables agents and applications to make payments directly through web requests and currently relies heavily on dollar-denominated stablecoins. Google's Agent Payments Protocol and Mastercard's agent-payment infrastructure provide further examples of non-EU firms developing payment systems for AI agents, although these support a wider range of payment methods.

organisations and shares only what is needed for computation^{ix}, whereas decentralised storage uses a distributed technical architecture in which data is stored across multiple independent nodes rather than with a single provider^x.

These approaches can reduce dependence on individual providers, but **technical distribution does not by itself make data either sovereign or decentralised in terms of control**. Distribution describes where technical functions or resources sit; decentralisation concerns whether dependence on a single point of control is reduced; sovereignty concerns who has effective and legal control, along with access and choice. A European cloud service can therefore support sovereignty objectives without being decentralised, while a distributed system can still depend on foreign operators or governance⁸⁸. This distinction is particularly important for data storage, examined in the box below.

Box 3. Example: Importance of sovereign data storage

Experts consulted for this project highlighted sovereign storage as particularly important, since AI technologies increase the strategic value of data⁸⁹. Under the US CLOUD Act, US authorities can in certain circumstances require US providers to disclose data they control even when it is stored outside the US⁹⁰. Given the strong position of US hyperscalers in the European cloud market⁹¹, storing data in the EU does not by itself remove all dependence on foreign providers or foreign law.

Experts consulted for this project highlighted sovereign cloud, on-premise deployment, federated data environments and privacy-preserving technologies as different approaches that can reduce exposure to external providers or third-country access⁹². These approaches are different, but they all aim to give European organisations greater control over where data is held, processed and accessed.

European initiatives are already developing some of these options. IPCEI-CIS supports a multi-provider European cloud-edge environment⁹³, while SIMPL provides open-source software intended to support interoperability between data spaces and cloud-to-edge services⁹⁴. Their contribution to sovereignty will depend on whether they give users practical alternatives and make it easier to move data and workloads between providers.

The technical approaches that can support greater decentralisation of data storage and processing are at different stages of maturity. Some are already usable in specific settings, while others still face limits related to cost, performance, security and integration. The European Health Data Space shows that demand for federated data processing and privacy-preserving technologies is already emerging secondary use of health data will rely on secure processing environments connected through a federated European infrastructure⁹⁵.

Table 1. Technical approaches relevant to decentralisation at the data layer

Decentralised storage	Privacy-preserving computation	Federated learning
Decentralised storage has reached enterprise scale, but data persistence still depends on the economic incentives that keep node operators storing it ⁹⁶ , retrieval remains slower than centralised cloud, making it suited today to archival rather than real-time use ^{97,98} , and integration with existing	Privacy-preserving computation is technically proven but computationally expensive, with zero-knowledge proof generation taking seconds per proof and demanding resources that put it beyond latency-sensitive applications and ordinary consumer devices ¹⁰⁰ , while adoption is further slowed by a shortage of specialised	Federated learning likewise remains at an early stage, constrained by communication overhead and by weak defences against adversaries injecting

^{ix} According to experts consulted for this project federated learning works best in closed federations of participants who trust one another and run the same model, such as bank networks or hospital consortia, and it remains coordinated in governance even where its operation is distributed.

^x Storage and processing do not require the same type of trusted authority as identity or asset ownership because no external fact needs to be certified. Their technical operation can therefore be distributed more extensively, although governance and coordination may still remain centralised or federated.

enterprise systems requires	expertise and the absence of standardised frameworks and certification ¹⁰¹ .	harmful updates into the shared model ^{102,103} .
-----------------------------	---	--

Source: authors elaboration; for a detailed analysis of decentralised technology enablers and their maturity refer to the paper “Decentralised data and service architectures” prepared as part of the project.

The barriers differ across these approaches. They include cost, performance, integration, skills, security and procurement readiness, focusing on accelerating these technologies towards commercially viable deployment rather than on building confidence in them¹⁰⁴. For public bodies, the assurance requirements proposed under CADA may also affect when and where these services can be procured¹⁰⁵. Policy support should therefore focus on uses where technical distribution, federation or privacy-preserving computation provides a clear benefit, rather than treating decentralisation as an objective in itself.

EU Policy response:

Existing EU measures address parts of this problem, but they do not form a single policy for decentralised data governance. The Data Act focuses mainly on reducing lock-in by making it easier for customers to switch between data-processing providers or use several providers¹⁰⁶. Its purpose is therefore to improve switching and contractual conditions rather than to change the structure of the cloud market directly¹⁰⁷.

The proposed CADA addresses a different part of the problem by seeking to expand European cloud and AI capacity and strengthen cloud sovereignty¹⁰⁸. These provisions can support a more diverse European market, but this outcome is not automatic. New capacity could still become concentrated around a small number of providers or around the software and services used to coordinate them. It also refers explicitly to both distributed and decentralised cloud and edge approaches, reflecting the distinction between the technical distribution of capacity and the broader objective of reducing concentration and dependency¹⁰⁹.

The main policy gap concerns how existing instruments are implemented together. The Data Act can make switching easier, while CADA can support new European capacity. Their contribution to sovereignty will depend on whether that capacity remains interoperable, whether users can move workloads between providers, and whether several providers can compete on viable terms. Some stakeholders^{xi} have therefore proposed making federation and common interoperability requirements for a stronger part of European cloud policy and procurement¹¹⁰.

A separate issue is legal clarity.

Some EU rules were developed around services with a clearly identifiable operator, while decentralised systems can distribute responsibility across several participants. This can make it harder to determine who is responsible for complying with obligations such as data protection rights. The European Data Protection Board has begun clarifying how the GDPR applies to blockchain-based systems¹¹¹, while MiCA mainly regulates identifiable issuers and service providers¹¹². Further guidance could help clarify how existing rules apply where responsibility is distributed, including who is accountable for personal data and how data-subject rights should be implemented. Experts consulted for this project identified this uncertainty as a barrier to deployment¹¹³.

Recommendations:

- **Further develop and invest in Europe's foundational trust and data infrastructure for the agentic AI era.** Introduce federated and decentralised elements where they can reduce dependencies and strengthen sovereignty, including in data storage, processing and governance, alongside privacy-preserving technologies.
- **Strengthen European trust infrastructure through hybrid approaches.** Further develop EUROPEUM and the trust frameworks supporting the EUDI and Business Wallets, combining distributed verification where useful, with clearly accountable governance and trusted

^{xi} For example, Digital SME, more information available at: <https://www.digitalsme.eu/the-case-for-building-europes-sovereign-cloud-a-vision-for-the-cloud-and-ai-development-act/>

issuers. Ensure that these systems remain secure and under clear long-term governance as their use expands.

- **Support deployment in areas where federated and distributed approaches already offer practical value.** The European Health Data Space provides a concrete case for federated and secure processing¹¹⁴, while several AI Factories are being designed to handle sensitive-data workloads¹¹⁵. Table 1Box 3Public-interest uses of EU-regulated digital settlement systems should also be explored.

4. Network and infrastructure layer: who controls and coordinates the underlying capacity?

At the network and infrastructure layer, the main strategic issue is resilience and dependence on a small number of non-European providers. Europe relies heavily on external firms for connectivity and computing capacity, and some of this dependence is tied to physical assets. The region accounts for around 4.8 per cent of global AI supercomputer performance, compared with 74.4 per cent for the US and 14.1 per cent for China. European-owned capacity on subsea cables between Europe and North America is also limited, while US hyperscalers account for around 90 per cent of that capacity¹¹⁶. This creates both economic dependence and potential points of vulnerability in infrastructure on which Web 4.0 services will rely.

Technically, the internet is already highly distributed. It is built on open protocols and independently operated networks, with only a limited number of shared functions, such as the naming root, requiring common coordination¹¹⁷. The main concentration problem at this layer is therefore not the internet's basic architecture, but ownership and control of the infrastructure networks run on. Subsea cables, data centres, compute capacity and other critical assets are increasingly owned or operated by a relatively small number of firms¹¹⁸. This means that a technically distributed network can still be highly concentrated in economic and operational control. For this brief, the relevant question is therefore whether greater distribution of infrastructure also reduces dependence on individual providers, rather than whether the network is distributed in technical terms.

This concentration is increasingly reinforced by vertical integration. The same large firms can now span subsea connectivity, data centres, cloud infrastructure and services running above them¹¹⁹. They can concentrate control over several parts of the infrastructure chain in the same companies. The EU has started to examine some of these dependencies. Under the 2025 EU Action Plan on Cable Security, for example, an expert group is mapping submarine cable infrastructure, including ownership, capacity and landing points¹²⁰.

More distributed infrastructure can improve resilience by spreading capacity across locations and nodes. It can also contribute to decentralisation where capacity and control are spread across independent providers rather than remaining with a single operator. Edge and peer-to-peer architectures do this by moving computing, storage or connectivity closer to where they are needed and across a wider range of nodes. DePIN¹²¹ is one example, using digital incentives to coordinate physical resources contributed by independent operators. But a technically distributed system can still remain concentrated in ownership or governance, for example where one platform or software provider coordinates the participating resources.

This also creates opportunities in areas where market positions are not yet fixed. The Commission's Expert Forum on Frontier AI similarly identified secure and verifiable AI infrastructure as an emerging layer of the global stack where no actor yet holds a dominant position and Europe could take leadership¹²².

The same issue is visible in strategic sectors where physical infrastructure is becoming more distributed. Energy is the clearest case, since digitalisation is turning the grid into a network of

independent nodes, and the same questions of resilience and dependence arise there directly (see Box 4). Defence and space point to a second, more forward-looking case. Modern defence systems increasingly depend on satellites, sensors, autonomous systems and edge devices that must continue operating when individual links or nodes fail¹²³. In both cases, technical distribution can support decentralisation only if it also reduces dependence on individual suppliers or coordinating platforms.

Many of the underlying technologies are also dual-use, including satellite connectivity, AI, edge computing, secure communications and distributed sensing¹²⁴. As European defence investment expands¹²⁵, this could create additional demand for European infrastructure and suppliers¹²⁶. EU defence and space initiatives already emphasise interoperability, modularity and systems that can work across multiple components and operators^{127,128}. The opportunity is therefore to use new investment to strengthen resilience and supplier diversity, rather than replacing one dependency with another.

Europe does not need to decentralise infrastructure simply because technical distribution is increasing. Web 4.0 is likely to increase demand for distributed and edge deployment, because many real-time and agentic applications benefit from processing closer to where data is generated and used¹²⁹. The policy question is whether this technical shift also creates greater provider choice and reduces strategic dependencies.

The key question is therefore whether more distributed infrastructure also leads to greater decentralisation of control. New capacity can still be controlled by the same firms that dominate today's cloud and digital infrastructure markets¹³⁰. Dependence can also move to the software and interfaces used to coordinate distributed resources. Interoperability, open interfaces and the ability to use multiple providers therefore matter as much as physical distribution itself.

The **energy sector illustrates this particularly clearly** because its physical assets are becoming more distributed while the digital coordination layer is still taking shape.

Box 4. Distributed energy: an open coordination layer

Web 4.0 will increase pressure on the electricity system at the same time as the grid itself becomes more distributed. The IEA expects data-centre electricity use to rise sharply over the next decade¹³¹, while renewable generation, storage and flexible demand are increasing the number of assets that need to be coordinated across the grid. Renewables already supplied 48 per cent of EU electricity production in 2024¹³². This makes digital coordination increasingly important for balancing supply and demand across many different actors. The same is reflected in the Commission's 2026 measures on digitalising the energy system¹³³.

Concentration is uneven across this emerging system. Some upstream parts of the value chain are already highly concentrated: China accounted for around 80 per cent of global inverter manufacturing capacity in 2025, compared with around 8 per cent in Europe^{134,135}. By contrast, the digital layer used to coordinate distributed energy resources in Europe is not yet dominated by a single provider. A Commission mapping identified 37 local flexibility-market initiatives, most still at pilot or preparatory stage, with different commercial and system-operator models in use¹³⁶. This is therefore a part of the market where future concentration is not yet fixed.

Distributed generation and storage can also strengthen resilience by allowing more supply and balancing to take place locally when wider networks are under pressure. Recent analysis argues that European resilience will depend on combining cross-border integration with more local generation, storage and microgrids^{137,138,139}. The 2025 blackout in Spain illustrates the importance of system resilience: investigations pointed to problems including voltage control, grid oscillations and plant disconnections^{140,141}. Spain subsequently strengthened voltage-control requirements and accelerated measures supporting storage and other resources able to provide grid-stability services^{142,143}. The lesson is not that distributing assets alone prevents outages, but that generation and storage can form part of a more resilient system when properly integrated and coordinated.

That coordination layer could itself become a new point of concentration. Large technology companies are moving beyond electricity procurement into areas such as energy trading, infrastructure ownership and grid

software^{144,145,146xii}. Companies with large installed bases of energy devices can also expand into coordination services. Tesla, for example, combines batteries, control software, customer applications and virtual power plant services¹⁴⁷. This does not mean that these firms currently dominate European distributed-energy coordination, but it shows how control across several parts of the value chain could become concentrated as the market develops. The same pattern of firms expanding from an existing strong position into adjacent layers is also identified in the project's infrastructure paper¹⁴⁸.

The policy opportunity is therefore to ensure that a more distributed energy system does not produce a new concentration of control at the coordination layer. Interoperable interfaces, the ability to connect equipment from different suppliers and non-discriminatory access to coordination services can help keep that layer open and contestable.

The energy example illustrates a wider point across this layer: technical distribution does not by itself decentralise control. **Distributed systems still depend on shared protocols, interfaces and reference points** that allow different participants to work together^{xiii}. If these are controlled by a single provider, dependence can simply move from the physical infrastructure to the coordination layer. The main takeaway is that distributed infrastructure still needs coordination, but that coordination should not become a new point of private control.

Box 5. Why distributed systems still need shared coordination

Distributed systems still need some common rules and reference points. The Domain Name System (DNS) is a good example. Many different organisations operate parts of the DNS, but they all rely on one shared root. This ensures that the same website name points to the same destination everywhere. Without this shared reference point, different parts of the internet could give different answers for the same name.

Blockchain-based naming systems take a different approach. They can register names outside the ICANN-coordinated DNS¹⁴⁹. This can give users more control, but it can also create separate naming systems that do not always work together. Users may then need specific wallets, gateways or other tools to access them.

AI agents will face a similar problem. Agents need to be able to find and verify other agents and services. If this function is controlled by one platform, that platform could decide which agents are visible or easy to use. This could create a new form of lock-in^{150,151}.

Open approaches aim to avoid this. For example, the Linux Foundation's DNS-AID project uses the existing DNS to publish information about AI agents¹⁵². The aim is to let agents find each other across different services without depending on one company. Experts consulted for this project stressed that such open solutions need to be available early, before developers become dependent on proprietary systems¹⁵³. One expert also noted that distributed AI systems will only work well if agents can find and select one another across different networks and providers¹⁵⁴.

The main lesson is simple: distributed infrastructure still needs coordination, but that coordination should not become a new point of private control.

The implication is not that infrastructure should be decentralised wherever technically possible. Some functions benefit from technical distribution, redundancy and multiple providers, while others require shared or central coordination. In practice, this often results in hybrid architectures, combining distributed operation with shared or central coordination where needed. The objective should be to reduce strategic dependencies while keeping necessary points of coordination open and accountable.

^{xii} Large technology companies are moving beyond electricity procurement into wholesale trading, energy-infrastructure ownership and grid software, including Meta's authorisation to sell electricity at wholesale rates and Alphabet's acquisition of Intersect and development of Tapestry's AI-based grid-planning platform.

^{xiii} Some functions require a shared reference point by design. For example, internet names only resolve consistently because participants rely on a common root. Other functions may also need shared coordination until fully distributed alternatives are mature enough to work reliably at scale.

This is consistent with the JRC's concept of 'modular resilience', or accepting that some interdependencies are unavoidable while reducing them where this is feasible and strategically important¹⁵⁵.

This question is becoming particularly important for Web 4.0 because some of its basic coordination mechanisms are still being defined. In agentic systems, these include the protocols agents use to communicate, describe their capabilities and discover other agents and services. Proprietary approaches are developing alongside open and multistakeholder standards processes¹⁵⁶. If common approaches do not emerge, the market could fragment between incompatible systems; if one proprietary approach becomes dominant, control could instead concentrate around a small number of providers. The project's agentic AI papers examine this emerging standards landscape in more detail¹⁵⁷. **Europe therefore has an opportunity to influence these choices before market positions become fixed.** Open standards are important, but they will not be sufficient on their own. Open alternatives also need to be usable, maintained and adopted at scale, while procurement and investment decisions need to preserve interoperability and the possibility of using multiple providers. The EU policy response below examines how existing initiatives address these conditions and where gaps remain.

EU Policy response:

The EU is already investing in many of the building blocks needed for more resilient and less dependent infrastructure. EuroHPC AI Factories and planned AI Gigafactories are expanding European compute capacity^{158,159}, while CADA explicitly supports distributed and decentralised cloud and edge approaches^{xiv}, and introduces an EU framework for assessing cloud and AI sovereignty¹⁶⁰. The Digital Decade also targets 10,000 secure, climate-neutral edge nodes by 2030¹⁶¹. Experts consulted for this study noted that compute capacity is increasingly well supported, while greater attention is still needed for the data infrastructure on which this capacity depends¹⁶².

Other initiatives address the openness and sectoral deployment of this infrastructure. The Open Source Strategy and related digital-commons initiatives support open technologies and protocols¹⁶³, while the 2026 energy roadmap promotes greater European control over the digital technologies used in critical energy infrastructure¹⁶⁴. Growing investment in defence and space creates another opportunity to develop resilient European communications, sensing and edge infrastructure, with interoperability and reduced strategic dependencies already reflected in EU priorities¹⁶⁵.

The remaining issue is how these investments fit together and who ultimately controls them. Technically distributed capacity can still remain concentrated in commercial control, for example through software, orchestration, access or other coordination functions. EU programmes promote sovereignty, interoperability and distributed capacity in different ways, but they do not yet provide a common approach to ensuring that publicly supported infrastructure remains interoperable across sites and providers, portable where appropriate, and open to competing suppliers.

The independent EuroStack proposal points in this direction by advocating a federated and decentralised European infrastructure in which edge and centralised capacity complement one another¹⁶⁶. In practical terms, federation would allow independently operated infrastructures to work together through common interfaces, while the broader decentralisation objective is to avoid dependence on a single provider or control point. It is not EU policy, but the EuroStack proposal illustrates the broader choice facing Europe: new sovereign capacity can either develop as separate systems or as interoperable infrastructure that preserves choice between providers.

The policy challenge is therefore not to decentralise every infrastructure by design. It is to use the current investment cycle in compute, edge, energy, defence and space to reduce strategic dependencies while avoiding new points of concentration. The same principle applies to the open protocols and coordination

^{xiv} In the terminology used in this brief, this can mean both spreading capacity technically across locations and nodes, and reducing dependence on individual providers.

mechanisms now emerging for AI agents: standards and open specifications matter, but they also need practical adoption and routes to scale.

At this layer, the objective should be to **use distributed or federated approaches where they improve resilience and reduce strategic dependencies** without undermining performance, interoperability or effective coordination. Greater decentralisation here, can introduce trade-offs, including higher coordination costs, fragmentation, operational complexity and, in some cases, weaker performance or accountability. At the same time, technically distributed systems can still create new points of concentration in the software, gateways or coordination mechanisms on which they depend¹⁶⁷. Monitoring where such new dependencies emerge is therefore important, particularly in areas such as agent discovery, naming, gateways and other coordination functions, where new gatekeepers could emerge. This implies using public infrastructure investment to preserve interoperability and supplier choice and strengthening the monitoring of ownership and control in submarine cable infrastructure.

Recommendations:

- **Leverage EU AI infrastructure initiatives** such as the AI Factories and Gigafactories to test and deploy decentralised and federated approaches where they can strengthen resilience and reduce supplier dependencies. This includes the following points:
 - Ensuring that emerging mechanisms for agent discovery, traceability, and auditability do not become new central points of control, using distributed or federated approaches where technically appropriate.
 - Supporting interoperable coordination between AI agents and services across providers, including through European participation in open, multistakeholder standards setting for agent communication, capability description and discovery, including approaches that build on openly governed infrastructure such as DNS where appropriate.
- **Support the integration and coordination of distributed assets** (e.g., renewable generation, storage and vehicle batteries) using existing initiatives such as the EU roadmap for Digitalisation and AI in the Energy Sector to accelerate their deployment and integration into the grid. Open interfaces, interoperability and non-discriminatory access should allow different providers and technologies to participate without creating new points of concentration.

Conclusions

The central challenge for European sovereignty in Web 4.0 is the concentration of control over the services, data and infrastructure on which the next generation of the internet will depend. Existing digital markets already show how control can accumulate around a small number of platforms and infrastructure providers. Web 4.0 could deepen these dependencies as AI agents, virtual environments and increasingly automated services become important ways of accessing information, markets and public services. At the same time, many parts of this emerging ecosystem are still taking shape.

The EU therefore needs to **change the conditions under which Web 4.0 markets and infrastructure develop.** This does not necessarily require a new overarching policy framework, but a more deliberate use of existing policies, investment and procurement instruments to ensure that the advantages of today's hyperscalers do not automatically translate into entrenched positions in emerging areas.

Decentralisation can help create such alternatives by reducing reliance on single points of control and allowing services, data or infrastructure to be organised across multiple independent actors. This can involve federated models, where independent providers interoperate while retaining control of their own systems, or distributed architectures, where technical functions and capacity are spread across multiple nodes or locations. Neither approach automatically disperses control or market power, however. Dependence can re-emerge in the platforms, software, standards, settlement systems or other coordinating functions on which these systems rely.

This challenge takes a different form at each layer of Web 4.0. At the web layer, the main risk is that incumbent platforms extend their control over users and markets into AI agents, discovery and other new interfaces. Open and federated decentralised alternatives can provide competing routes, but they need more than open-source code: they need usable services, sustained digital commons and enough demand to reach scale. **At the data layer,** the issue is control over data and trusted information. Some functions, such as identity and credentials, will continue to require accountable institutions even when their technical operation or verification is more distributed, while storage and processing can be distributed further where this provides clear benefits. **At the network and infrastructure layer,** the internet is already technically distributed, but ownership of compute, connectivity and other physical capacity is highly concentrated. New edge, energy and other distributed infrastructure will only contribute to decentralisation of control if it also preserves interoperability, supplier choice and the ability to use multiple providers.

Some of the most important choices about decentralisation concern governance rather than the sole physical infrastructure. Distributed systems still need shared ways to identify participants, exchange information and make different components work together. DNS shows that shared coordination can support a highly distributed system without one commercial provider controlling the whole network. Emerging areas such as AI-agent discovery show that similar choices are being made again. Open standards matter, but standards alone will not prevent concentration: open alternatives also need practical implementations, maintenance, interoperability testing and users before proprietary solutions become established defaults.

Europe can build on existing instruments to influence this transition. The Data Act, CADA, AI Factories and Gigafactories, the Digital Decade, the EUDI Wallet and European trust infrastructure, the Open Source Strategy and digital commons, and Europeum EDICs all address parts of the problem. Sectoral investment in energy, defence and space creates further opportunities. These initiatives can be leveraged (and complemented) to implement the recommended decentralisation actions, to preserve choice, increase EU sovereignty and prevent new dependencies. Public investment and procurement can require portability and interoperability where appropriate; infrastructure programmes can monitor ownership and concentration; open alternatives can be given routes to adoption; and emerging coordination layers can be kept open to new entrants before market structures harden.

European technological sovereignty does not require Europe to own, centralise or decentralise every component of Web 4.0. It requires the ability to make meaningful choices, switch between providers, maintain critical functions and influence the rules and standards on which European services depend. In practice, this points towards a mix of centralised, federated and distributed architectures, combined with accountable governance and cooperation with international partners.

5. Endnotes

¹ Barcevičius, E., et al. (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> ; Barcevičius, E., et al. (2025). Digital identity and identifiers in the era of Web 4.0 and virtual worlds [Thematic paper]. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://op.europa.eu/en/publication-detail/-/publication/4f7b8585-4829-11f1-8095-01aa75ed71a1/language-en>

² European Commission. (2024). The Future of European Competitiveness, Part A: A Competitiveness Strategy for Europe (Draghi report). Available at: https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en

³ PPMI. (Forthcoming). Agentic AI, trust and security: Thematic paper. WEB4HUB; PPMI. (Forthcoming). Agentic AI: state of play: Thematic paper. WEB4HUB; PPMI. (Forthcoming). Infrastructure in the age of agentic AI: Thematic paper. WEB4HUB.

⁴ Barcevičius, et al. (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>

⁵ PPMI & TNO. (Forthcoming). Decentralised data and service architectures. WEB4HUB.

⁶ Blind, K., Böhm, M., Grzegorzewska, P., Katz, A., Muto, S., Pätsch, S., & Schubert, T. (2021). The impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy (Final study report). European Commission, Directorate-General for Communications Networks, Content and Technology. Available at: <https://digital-strategy.ec.europa.eu/en/library/study-about-impact-open-source-software-and-hardware-technological-independence-competitiveness-and>

⁷ Draghi report.

⁸ Blind, K., Böhm, M., Grzegorzewska, P., Katz, A., Muto, S., Pätsch, S., & Schubert, T. (2021). The impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy (Final Study Report). Luxembourg: Publications Office of the European Union. <https://doi.org/10.2759/526721>

⁹ IMF. (2025). Understanding stablecoins (Departmental Paper). Available at: <https://www.imf.org/en/publications/departmental-papers/issues/2025/12/02/understanding-stablecoins-570602>

¹⁰ World Economic Forum. (2026). Digital economy inflection point: What to expect for digital assets in 2026. Available at: <https://www.weforum.org/stories/financial-and-monetary-systems/digital-economy-inflection-point-what-to-expect-for-digital-assets-in-2026/>

¹¹ Barcevičius, E., Gabaliņa, R., Butym, M., Wójtowicz, A., & Zepcan, A. (2026), forthcoming. Digital identity and identifiers in the era of Web 4.0 and virtual worlds: Thematic paper. Publications Office of the European Union. <https://doi.org/10.2759/6450018>.

¹² This is distinct from decentralised finance in the permissionless sense, the open, non-intermediated protocols where anyone can participate and no regulated entity is accountable.

¹³ BCG. (2025). Global Payments Report 2025. Available at: <https://web-assets.bcg.com/25/91/2269153c468ca43684442f055cb0/2025-global-payments-report-sep-2025.pdf>

¹⁴ IMF. (2025). Understanding stablecoins (Departmental Paper). Available at: <https://www.imf.org/en/publications/departmental-papers/issues/2025/12/02/understanding-stablecoins-570602>

¹⁵ Copic, E. (2025, July 31). Update on key digital asset technologies. Visa Economic Empowerment Institute. Available at: <https://corporate.visa.com/en/sites/visa-economic-empowerment-institute/update-on-key-digital-asset-technologies.html>

¹⁶ US Congress. (2025). S.1582, GENIUS Act of 2025. Available at: <https://www.congress.gov/bill/119th-congress/senate-bill/1582/text>

¹⁷ Xinhua. (2025, December 29). China to enhance digital yuan management with deposit features starting 2026. The State Council of the People's Republic of China. Available at: https://english.www.gov.cn/news/202512/29/content_WS69526d4ec6d00ca5f9a08511.html

- ¹⁸ Zhu, Y. (2025, January 7). China to finish building national data infrastructure by 2029. Yicai Global. Available at: <https://www.yicaiglobal.com/news/china-to-complete-building-national-data-infrastructure-by-2029>.
- ¹⁹ Yu, H. (2025, February 6). New data infrastructure guidelines to shape digital future. Science and Technology Daily. Available at: https://www.stdaily.com/web/English/2025-02/06/content_291149.html
- ²⁰ Kaur, D. (2025, January 10). China's digital infrastructure gets \$54.5B blockchain overhaul. Tech Wire Asia. <https://techwireasia.com/2025/01/chinas-digital-infrastructure-gets-54-5b-blockchain-overhaul/>
- ²¹ European Central Bank. (2026). The Eurosystem's comprehensive payments strategy. Available at: <https://www.ecb.europa.eu/press/pubbydate/2026/html/ecb.eurosystemcomprehensivepaymentsstrategy202603.en.html>
- ²² European Commission. (2026). European Tech Sovereignty, accompanied by an EU Open Source Strategy, COM(2026) 503 final. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52026DC0503>
- ²³ European Commission. (n.d.). European Blockchain Services Infrastructure (EBSI). European Blockchain Partnership. Available at: <https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home>
- ²⁴ European Commission. (2026). The EU Open Source Strategy. Shaping Europe's Digital Future. Available at: <https://digital-strategy.ec.europa.eu/en/policies/open-source-strategy>
- ²⁵ More information available at: <https://digital-strategy.ec.europa.eu/en/policies/event-web-4-governance>
- ²⁶ Barcevičius, et al. (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>
- ²⁷ PPMI. (Forthcoming). Agentic AI, trust and security: Thematic paper. WEB4HUB; PPMI. (Forthcoming). Agentic AI: state of play: Thematic paper. WEB4HUB; PPMI. (Forthcoming). Infrastructure in the age of agentic AI: Thematic paper. WEB4HUB.
- ²⁸ Arcep. (2026, January). Intelligence artificielle générative : quels défis pour un internet ouvert ? [Generative artificial intelligence: what challenges for an open internet?]. Autorité de régulation des communications électroniques, des postes et de la distribution de la presse. Available at: https://www.arcep.fr/uploads/tx_gspublication/rapport-IA-generative-defis-internet-ouvert-janvier2026.pdf
- ²⁹ Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). (2022). Official Journal of the European Union, L 265, 12.10.2022. Available at: <https://eur-lex.europa.eu/eli/reg/2022/1925/oj>
- ³⁰ PPMI. (Forthcoming). Agentic AI, trust and architecture: Thematic paper. WEB4HUB: 'A Space for the Metaverse – Virtual Worlds and the Transition to Web 4.0'.
- ³¹ Ibid.
- ³² Lessig, L. (1999, 9 February). Code and the commons [Keynote address]. Media Convergence conference, Fordham Law School, New York.
- ³³ Wikimedia Foundation. (2025). The public domain, digital commons, and digital public goods (DPGs): How Wikimedia projects advance a positive vision for the internet's future. Wikimedia Policy. Available at: <https://medium.com/wikimedia-policy/the-public-domain-digital-commons-and-digital-public-goods-dpgs-how-wikimedia-projects-d3b2846d72eb>
- ³⁴ Jones, J. E. (2017). Open source software is philanthropy. Stanford Social Innovation Review. Available at: <https://doi.org/10.48558/Z1MM-TF27>
- ³⁵ Wikimedia Foundation. (2025). New user trends on Wikipedia.
- ³⁶ PPMI. (forthcoming). Agentic AI, trust and security: Thematic paper. WEB4HUB.
- ³⁷ Matrix.org Foundation. (n.d.). Matrix.org: An open network for secure, decentralised communication. Available at: <https://matrix.org/>
- ³⁸ European Commission. (n.d.). About – European Commission on Mastodon. Available at: <https://ec.social-network.europa.eu/about>
- ³⁹ Scott, C. (2020, 11 November). Tim Berners-Lee startup releases its decentralisation tech to enterprises. Computer Weekly. Available at: <https://www.computerweekly.com/news/252491925/Tim-Berners-Lee-startup-releases-its-decentralisation-tech-to-enterprises>
- ⁴⁰ Solid Project. (n.d.). Solid: Your data, your choice. Retrieved 25 August 2026, from <https://solidproject.org/>
- ⁴¹ W Social AB. (2026). W: The European social network for verified humans. Available at: <https://wsocial.eu/>
- ⁴² European Commission. (n.d.). Next Generation Internet Initiative. Shaping Europe's Digital Future. Available at: <https://digital-strategy.ec.europa.eu/en/policies/next-generation-internet-initiative>
- ⁴³ Sovereign Tech Agency. (2026, 30 March). Digital Commons EDIC takes shape with more countries, director, and first projects [Press release]. Available at: <https://www.sovereign.tech/public/press/2026-03-26-Press-Release-Sovereign-Tech-Agency-EDIC-Digital-Commons-Director.pdf>

- ⁴⁴ European Commission. (2026). The EU Open Source Strategy. Shaping Europe's Digital Future. Available at: <https://digital-strategy.ec.europa.eu/en/policies/open-source-strategy>
- ⁴⁵ European Commission. (2026). Proposal for a Regulation establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act) (COM(2026) 502 final). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2026%3A502%3AFIN>
- ⁴⁶ SUSE. (2026, 16 June). EU Cloud and AI Development Act: A major step for open source. SUSE Blog. Available at: <https://www.suse.com/c/eu-cloud-ai-development-act-open-source-first/>
- ⁴⁷ Blind, K., Böhm, M., Grzegorzewska, P., Katz, A., Muto, S., Pätsch, S., & Schubert, T. (2021). The impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy: Final study report. Publications Office of the European Union. Available at: <https://doi.org/10.2759/430161>
- ⁴⁸ BCG. (2025). Global Payments Report 2025. Available at: <https://web-assets.bcg.com/25/91/2269153c468ca43684442f055cb0/2025-global-payments-report-sep-2025.pdf>
- ⁴⁹ IMF. (2025). Understanding stablecoins (Departmental Paper). Available at: <https://www.imf.org/en/publications/departmental-papers/issues/2025/12/02/understanding-stablecoins-570602>
- ⁵⁰ The Agent Economy: autonomous agents and machine-to-machine micropayments. (2026). Available at: <https://arxiv.org/pdf/2602.14219>
- ⁵¹ PPML. (Forthcoming). Agentic AI, trust and security. Thematic Paper.
- ⁵² Interview findings (July, 2026).
- ⁵³ European Commission. (2026). Guidelines on transparency of AI-generated content. Shaping Europe's Digital Future. Available at: <https://digital-strategy.ec.europa.eu/en/policies/guidelines-transparency-ai-generated-content>
- ⁵⁴ World Bank (Clark, J., Marin, G., Ardic Alper, O. P., & Galicia Rabadan, G. A.). (2025). Digital public infrastructure and development: A World Bank Group approach (Digital Transformation White Paper, Vol. 1). Washington, DC: World Bank. <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099031025172027713>
- ⁵⁵ Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). (2022). Official Journal of the European Union, L 265, 12.10.2022. Available at: <https://eur-lex.europa.eu/eli/reg/2022/1925/oj>
- ⁵⁶ Gates, N., Tridgell, J., Schwäbe, C., Hummler, A., Blind, K., Streinz, T., & Torracco, R. M. (2025). Funding Europe's open digital infrastructure: The economic, legal, and political feasibility of an EU Sovereign Tech Fund (EU-STF). OpenForum Europe. Available at: https://openforumeurope.org/wp-content/uploads/2025/10/EU-STF-Feasibility-Study_final.pdf
- ⁵⁷ Singh, A., & Tarkowski, A. (2026). Beyond open source: What the Tech Sovereignty Package gets right and misses on Digital Commons. Open Future. Available at: <https://openfuture.eu/blog/beyond-open-source/>
- ⁵⁸ OpenForum Europe. (2025). The EU Open Source Policy Summit 2025: What did we learn and where do we go from here? Available at: <https://openforumeurope.org/the-eu-open-source-policy-summit-2025-what-did-we-learn-and-where-do-we-go-from-here/>
- ⁵⁹ Ibid.
- ⁶⁰ Interview findings (July, 2026)
- ⁶¹ Barcevičius, E., et al. (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, PPML, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701> ; Barcevičius, E., et al. (2025). Digital identity and identifiers in the era of Web 4.0 and virtual worlds [Thematic paper]. European Commission, PPML, TNO, & WEB4HUB. Available at: <https://op.europa.eu/en/publication-detail/-/publication/4f7b8585-4829-11f1-8095-01aa75ed71a1/language-en>
- ⁶² US Congress. (2018). H.R. 4943, Clarifying Lawful Overseas Use of Data (CLOUD) Act, 115th Congress, codified at 18 U.S.C. § 2713. Available at: <https://www.congress.gov/bill/115th-congress/house-bill/4943/text>
- ⁶³ Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act). Available at: <https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng>.
- ⁶⁴ European DIGITAL SME Alliance. (2026). The case for building Europe's sovereign cloud: A vision for the Cloud and AI Development Act [Policy paper]. Available at: <https://www.digitalsme.eu/digital/uploads/DIGITAL-SME-Policy-Paper-The-case-for-building-Europes-sovereign-cloud.pdf>
- ⁶⁵ Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). (2023). Official Journal of the European Union, L series, 22.12.2023. Available at: <https://eur-lex.europa.eu/eli/reg/2023/2854/oj>

- ⁶⁶ European Commission. (2026, June 3). Proposal for a Regulation establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act) (COM(2026) 502 final). Available at: <https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada>
- ⁶⁷ Barcevičius, E., Gabaliņa, R., Butym, M., Wójtowicz, A., & Zepcan, A. (2026), forthcoming. Digital identity and identifiers in the era of Web 4.0 and virtual worlds: Thematic paper. Publications Office of the European Union. <https://doi.org/10.2759/6450018>.
- ⁶⁸ Barcevičius, E., Gabaliņa, R., Butym, M., Wójtowicz, A., & Zepcan, A. (2026), forthcoming. Digital identity and identifiers in the era of Web 4.0 and virtual worlds: Thematic paper. Publications Office of the European Union. <https://doi.org/10.2759/6450018>
- ⁶⁹ PPMI. (forthcoming). Post quantum transition & Web 4.0. WEB4HUB.
- ⁷⁰ PPMI & TNO. (Forthcoming). Decentralised data and service architectures. WEB4HUB.
- ⁷¹ Barcevičius, E., Gabaliņa, R., Butym, M., Wójtowicz, A., & Zepcan, A. (2026), forthcoming. Digital identity and identifiers in the era of Web 4.0 and virtual worlds: Thematic paper. Publications Office of the European Union.
- ⁷² PPMI & TNO. (Forthcoming). Decentralised data and service architectures. WEB4HUB.
- ⁷³ Zwitter, A. J., Gstrein, O. J., & Yap, E. (2020). Digital identity and the blockchain: Universal identity management and the concept of the “self-sovereign” individual. *Frontiers in Blockchain*, 3, 26.
- ⁷⁴ PPMI & TNO. (Forthcoming). Decentralised data and service architectures. WEB4HUB.
- ⁷⁵ Giannopoulou, A. (2023). Digital identity infrastructures: A critical approach of self-sovereign identity. *Digital Society*, 2(2), 18.
- ⁷⁶ Barcevičius, E., Gabaliņa, R., Butym, M., Wójtowicz, A., & Zepcan, A. (2026), forthcoming. Digital identity and identifiers in the era of Web 4.0 and virtual worlds: Thematic paper. Publications Office of the European Union.
- ⁷⁷ European Commission. (2024, 22 May). Blockchain: Creation of EUROPEUM-EDIC [News article]. Shaping Europe's Digital Future. Available at: <https://digital-strategy.ec.europa.eu/en/news/blockchain-creation-europeum-edic>
- ⁷⁸ European Commission. (n.d.). EU Digital Identity Wallet home. Available at: <https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487738/EU+Digital+Identity+Wallet+Home>
- ⁷⁹ European Commission. (n.d.). Common European data spaces. Available at: <https://digital-strategy.ec.europa.eu/en/node/12304/printable/pdf>
- ⁸⁰ Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (MiCA). Available at: <https://eur-lex.europa.eu/eli/reg/2023/1114/oj>
- ⁸¹ European Central Bank. (2025). Project Pontes. ECB. Available at: <https://www.ecb.europa.eu/paym/target/pontes/html/index.en.html>
- ⁸² European Central Bank. (2026). Appia: Paving the way for a future-ready, integrated financial ecosystem leveraging tokenisation and DLT. Available at: <https://www.ecb.europa.eu/press/payments-news/ecb.pubconpm202603.en.html>
- ⁸³ US Congress. (2025). S.1582 – GENIUS Act of 2025. Available at: <https://www.congress.gov/bill/119th-congress/senate-bill/1582/text>
- ⁸⁴ IMF. (2025). Understanding stablecoins (Departmental Paper). Available at: <https://www.imf.org/en/publications/departmental-papers/issues/2025/12/02/understanding-stablecoins-570602>
- ⁸⁵ UNHCR. (2022). UNHCR launches pilot cash-based intervention using blockchain technology for humanitarian payments to people displaced and impacted by the war in Ukraine. Available at: <https://www.unhcr.org/ua/en/52555-unhcr-launches-pilot-cash-based-intervention-using-blockchain-technology-for-humanitarian-payments-to-people-displaced-and-impacted-by-the-war-in-ukraine-unhcr-has-launched-a-first-of-its-kind-integ.html>
- ⁸⁶ Mercy Corps Ventures. (2025). Pilot insights: Stablecoin payments cut costs and increase safety in Afghanistan. Available at: <https://www.mercycorpsventures.com/blog> (verify clean URL before circulation).
- ⁸⁷ World Bank (Clark, J., Marin, G., Ardic Alper, O. P., & Galicia Rabadan, G. A.). (2025). Digital public infrastructure and development: A World Bank Group approach (Digital Transformation White Paper, Vol. 1). Washington, DC: World Bank. <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099031025172027713>
- ⁸⁸ PPMI & TNO. (Forthcoming). Decentralised data and service architectures. WEB4HUB.
- ⁸⁹ WEB4HUB expert roundtable. (2026, 2 July). Opportunities for Europe in the Web 4.0 and Agentic AI Era.
- ⁹⁰ Eurojust. (2022). The CLOUD Act (SIRIUS Project report). Available at: <https://www.eurojust.europa.eu/publication/cloud-act>

- ⁹¹ Synergy Research Group. (2025). European cloud providers' local market share now holds steady at 15%. Available at: <https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15>
- ⁹² Interview findings.
- ⁹³ European Commission. (2023). Approved IPCEI Next Generation Cloud Infrastructure and Services. Available at: https://competition-policy.ec.europa.eu/state-aid/ipcei/approved-ipceis/cloud_en. See also 8ra Initiative. (n.d.). IPCEI-CIS. Available at: <https://www.8ra.com/ipcei-cis/>
- ⁹⁴ European Commission. (n.d.). SIMPL: cloud-to-edge federations and data spaces made simple. Shaping Europe's Digital Future. Available at: <https://digital-strategy.ec.europa.eu/en/policies/simpl>
- ⁹⁵ Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847. (2025). Official Journal of the European Union, L series, 5.3.2025. Available at: <https://eur-lex.europa.eu/eli/reg/2025/327/oj>
- ⁹⁶ Uriarte, R. B., Zhou, H., Kritikos, K., Shi, Z., Zhao, Z., & De Nicola, R. (2021). Distributed service-level agreement management with smart contracts and blockchain. *Concurrency and Computation: Practice and Experience*, 33(14), e5800. Available at: <https://onlinelibrary.wiley.com/doi/pdf/10.1002/cpe.5800>
- ⁹⁷ Guidi, B., et al. (2022). Evaluating the decentralisation of Filecoin. *Proceedings of the 3rd International Workshop on Distributed Infrastructure for the Common Good (DICG '22)*. Association for Computing Machinery. <https://doi.org/10.1145/3565383.3566108>
- ⁹⁸ Yang, S., & Li, M. (2023). Web 3.0 data infrastructure: Challenges and opportunities. *IEEE Network*, 37(1), 4–5. Available at: <https://ieeexplore.ieee.org/iel7/65/10110010/10110018.pdf>
- ⁹⁹ Zhang, H., & Lu, Y. (2025). Web 3.0: Applications, opportunities and challenges in the next internet generation. *Systems Research and Behavioral Science*. Available at: <https://onlinelibrary.wiley.com/doi/abs/10.1002/sres.3151>
- ¹⁰⁰ European Digital Identity Cooperation Group. (2025). G – Zero knowledge proof (Discussion paper, Version 1.4). In *Architecture and reference framework: Discussion topics*. Available at: <https://eudi.dev/2.4.0/discussion-topics/g-zero-knowledge-proof/>
- ¹⁰¹ Information Commissioner's Office. (2024). Tackling barriers to privacy-enhancing technologies adoption – a PETs project report. Available at: <https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/tackling-barriers-to-privacy-enhancing-technologies-adoption/>
- ¹⁰² European Data Protection Supervisor. (2025). TechDispatch #1/2025 – Federated learning. EDPS Publications. Available at: https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2025-06-10-techdispatch-12025-federated-learning_en
- ¹⁰³ Shirvani, G., Ghasemshirazi, S., & Beigzadeh, B. (2024). Federated learning: Attacks, defenses, opportunities and challenges. In *2024 11th International Symposium on Telecommunications (IST)* (pp. 470–479). IEEE.
- ¹⁰⁴ OECD. (2023). Emerging privacy enhancing technologies: Current regulatory and policy approaches (OECD Digital Economy Papers, No. 351). OECD Publishing. Available at: <https://doi.org/10.1787/bf121be4-en>
- ¹⁰⁵ European Commission. (2026). Proposal for a Regulation establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act) (COM(2026) 502 final). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52026PC0502>
- ¹⁰⁶ Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). (2023). Official Journal of the European Union, L series, 22.12.2023. Available at: <https://eur-lex.europa.eu/eli/reg/2023/2854/oj>
- ¹⁰⁷ European Commission. (2022). Impact assessment report accompanying the proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) (SWD(2022) 34 final). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022SC0034>
- ¹⁰⁸ European Commission. (2026, June 3). Proposal for a Regulation establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act) (COM(2026) 502 final). Available at: <https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada>
- ¹⁰⁹ European Commission. (2026, June 3). Proposal for a Regulation establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act) (COM(2026) 502 final). Available at: <https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada>
- ¹¹⁰ European DIGITAL SME Alliance. (2026). The case for building Europe's sovereign cloud: A vision for the Cloud and AI Development Act. Available at: <https://www.digitalsme.eu/the-case-for-building-europes-sovereign-cloud-a-vision-for-the-cloud-and-ai-development-act/>
- ¹¹¹ European Data Protection Board. (2025). Guidelines 02/2025 on processing of personal data through blockchain technologies (Version 1.0, public consultation draft). https://www.edpb.europa.eu/public-consultations/guidelines-022025-on-processing-of-personal-data-through-blockchain_en

- ¹¹² Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (MiCA). (2023). Official Journal of the European Union, L 150, 9.6.2023. Available at: <https://eur-lex.europa.eu/eli/reg/2023/1114/oj>
- ¹¹³ WEB4HUB expert roundtable. (2026, 2 July). Opportunities for Europe in the Web 4.0 and Agentic AI Era.
- ¹¹⁴ Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847. (2025). Official Journal of the European Union, L series, 5.3.2025. Available at: <https://eur-lex.europa.eu/eli/reg/2025/327/oj>
- ¹¹⁵ EuroHPC JU. (2025). Six additional AI Factories selected. See, for example, the Netherlands AI Factory, which emphasises AI applications involving highly sensitive data such as health information and IP-protected datasets. Available at: <https://www.hpcwire.com/off-the-wire/eurohpc-selects-6-additional-ai-factories-to-expand-europes-ai-capabilities/>
- ¹¹⁶ Shamir, A., & Negele, M. (2025). RAND Europe's response to the EU Cloud and AI Development Act call for evidence (CT-A4156-1). RAND Corporation. Available at: <https://www.rand.org/pubs/testimonies/CTA4156-1.html>
- ¹¹⁷ PPMI & TNO. (Forthcoming). Decentralised data and service architectures: Thematic paper. WEB4HUB: 'A Space for the Metaverse – Virtual Worlds and the Transition to Web 4.0'.
- ¹¹⁸ Joint Committee on the National Security Strategy. (2025). Subsea telecommunications cables: Resilience and crisis preparedness (First Report of Session 2024–26). UK Parliament. Available at: <https://publications.parliament.uk/pa/jt5901/jtselect/jtnatsec/723/report.html>
- ¹¹⁹ PPMI. (Forthcoming). Agentic AI and internet infrastructure: Thematic paper. WEB4HUB: 'A Space for the Metaverse – Virtual Worlds and the Transition to Web 4.0'.
- ¹²⁰ European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2025). EU action plan on cable security (JOIN(2025) 9 final). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52025JC0009>
- ¹²¹ Ballandies, M. C., Wang, H., Law, A. C. C., Yang, J. C., Gösken, C., & Andrew, M. (2023). A taxonomy for blockchain-based decentralized physical infrastructure networks (depin). In 2023 IEEE 9th World Forum on Internet of Things (WF-IoT) (pp. 1-6). IEEE. Available at: <https://arxiv.org/pdf/2309.16707>
- ¹²² European Commission. (2026). Enhancing competitiveness, sovereignty and security of the European Union in frontier AI: Key insights from the first meeting of the European Expert Forum on Frontier AI. Publications Office of the European Union. Available at: <https://doi.org/10.2759/8947951>
- ¹²³ Thangavel, K., Sabatini, R., Gardi, A., Ranasinghe, K., Hilton, S., Servidia, P., & Spiller, D. (2024). Artificial intelligence for trusted autonomous satellite operations. *Progress in Aerospace Sciences*, 144, 100960. <https://doi.org/10.1016/j.paerosci.2023.100960>
- ¹²⁴ European Commission (2021). Action Plan on Synergies between Civil, Defence and Space Industries – dual-use/cross-fertilisation. Available at: https://www.google.at/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjvZywisGWAXvFBdsEHdYaBs0QFnoECBcQAQ&url=%2Fgoto%3Furl%3DCAESwQEB6zswFUA8D6EKPf_5EMIDDmvu5pRnrOFMsRxjpzhIP29YrjsPsJlg-6QzLKYNxQjNYE2QeXlpT7tFVL0gk1_PwMsX2bDwQHlKJRy9QzejJlcSY9oy411XZrIn-QqWGIHZzkIW74RAfk1PxUaSGluwFFTaiUHoqrLBRHQJWSDv824KoyWHk2QXLdoO4G3TLbnlisP_ZIY2eRCazK_PX93PCA2WUoQWBv0FyWP8_R_niHhFfHORsUqAcSNirFS1SI02&usq=AOvVaw2C9BkQ5XDC3yIdmHL28_6&opi=89978449
- ¹²⁵ European Defence Agency. (2026, July 16). EU defence spending: €418 billion in 2025, projected to €454 billion in 2026. European Defence Agency. Available at: <https://eda.europa.eu/news-and-events/news/2026/07/16/eu-defence-spending--418-billion-in-2025--projected-to-454-billion-in-2026>
- ¹²⁶ European Commission, Joint Research Centre. (n.d.). Dual-use technologies in Europe: Strategic dependencies and recommendations. Raw Materials Information System (RMIS). Available at: <https://rmis.jrc.ec.europa.eu/dualuse>
- ¹²⁷ European Commission, Directorate-General for Defence Industry and Space. (2026, April 15). Result of the EDF 2025 calls for proposals. European Commission. Available at: https://defence-industry-space.ec.europa.eu/funding-opportunities/calls-proposals/result-edf-2025-calls-proposals_en
- ¹²⁸ European Defence Agency. (2026, April 22). EDA and ESA to focus on Earth observation technology for defence. Available at: <https://eda.europa.eu/news-and-events/news/2026/04/22/eda-and-esa-focus-on-long-term-earth-observation-technology-for-defence-in-joint-research-push>
- ¹²⁹ PPMI. (Forthcoming). Agentic AI and internet infrastructure: Thematic paper. WEB4HUB: 'A Space for the Metaverse – Virtual Worlds and the Transition to Web 4.0'.
- ¹³⁰ PPMI. (Forthcoming). Agentic AI and internet infrastructure: Thematic paper. WEB4HUB: 'A Space for the Metaverse – Virtual Worlds and the Transition to Web 4.0'.

- ¹³¹ International Energy Agency. (2025). World energy outlook 2025. IEA. Available at: <https://www.iea.org/reports/world-energy-outlook-2025>
- ¹³² Eurostat. (2026). Energy in Europe: 2026 edition (Interactive publication). Publications Office of the European Union. Available at: <https://doi.org/10.2785/0794090>
- ¹³³ European Commission. (2026, 3 June). Commission presents measures to digitalise Europe's energy system while ensuring sustainable digitalisation. Available at: https://energy.ec.europa.eu/news/commission-presents-measures-digitalise-europes-energy-system-while-ensuring-sustainable-2026-06-03_en
- ¹³⁴ International Energy Agency. (2025). Inverter supply chains and cybersecurity [Commentary]. Available at: <https://www.iea.org/commentaries/inverter-supply-chains-and-cybersecurity>
- ¹³⁵ Wood Mackenzie. (2025). Global PV inverter shipments grew by 10% in 2024 to 589 GWac. Available at: <https://www.woodmac.com/press-releases/global-pv-inverter-shipments-grew-by-10-in-2024-to-589-gwac/>
- ¹³⁶ European Commission. (2026). Specification and design criteria for local flexibility markets (MJ0126015ENN). Publications Office of the European Union. Available at: <https://www.gopacs.eu/wp-content/uploads/2026/04/specification-and-design-criteria-for-local-flexibility-MJ0126015ENN.pdf>
- ¹³⁷ Stubenberg, C. (2026). Not all dependencies are equal: Europe's energy transition in the wake of geopolitical crisis (Policy Analysis 1/2026). Austrian Institute for International Affairs (oiip). Available at: <https://www.oiip.ac.at/en/publications/not-all-dependencies-are-equal-europes-energy-transition-in-the-wake-of-geopolitical-crisis/>
- ¹³⁸ International Energy Forum. (2021). What are microgrids and how can they help in the energy transition? Available at: <https://www.ief.org/news/what-are-microgrids-and-how-can-they-help-in-the-energy-transition>
- ¹³⁹ European Initiative for Energy Security. (2025, 6 August). EIES Insights: EIES call for securing the European grid. Available at: <https://www.secureenergyeurope.org/eies-insights-securing-the-european-grid>
- ¹⁴⁰ Freshfields Bruckhaus Deringer. (2025, November 18). After the blackout: The impact of RD 997/2025 on Spain's energy future. Available at: <https://www.freshfields.com/en/our-thinking/briefings/2025/11/after-the-blackout-the-impact-of-rd-9972025-on-spains-energy-future>
- ¹⁴¹ ESS News. (2025, November 10). Spain moves to reinforce its power system with new mandates for BESS operators and more. Available at: <https://www.ess-news.com/2025/11/10/spain-moves-to-reinforce-its-power-system-with-new-mandates-for-bess-operators-and-more/>
- ¹⁴² Bloomberg Originals. (2026, May 27). How the electrical grid is being rebuilt for AI | Bloomberg Primer [Video]. YouTube. Available at: <https://www.youtube.com/watch?v=8KOYyfZbPzo>
- ¹⁴³ Zeitlin, M. (2025, April 30). Spain's blackout has put in motion a debate over inertia. Heatmap News. Available at: <https://heatmap.news/energy/spain-blackout-inertia>
- ¹⁴⁴ Forbes and University of Houston Energy analyses of hyperscaler entry into energy markets, 2025–2026. Available at: https://www.uh.edu/energy/news/stories/2025/ow_big_tech_firms_are_disrupting_energy_hmarkets.php and <https://www.forbes.com/sites/annademeo/2026/03/23/ai-is-turning-big-tech-into-the-new-power-players/>
- ¹⁴⁵ Roy, B. (2025). New Power Players: How Big Tech Firms Are Disrupting Energy Markets. University of Houston. Available at: https://www.uh.edu/energy/news/stories/2025/ow_big_tech_firms_are_disrupting_energy_hmarkets.php
- ¹⁴⁶ Demeo, A. (2026). AI Is Turning Big Tech Into The New Power Players. Forbes. Available at: <https://www.forbes.com/sites/annademeo/2026/03/23/ai-is-turning-big-tech-into-the-new-power-players/>
- ¹⁴⁷ Tesla. (n.d.). Virtual power plant. Available at: <https://www.tesla.com/virtual-power-plant>
- ¹⁴⁸ PPMI. (Forthcoming). Infrastructure in the age of agentic AI: Thematic paper. WEB4HUB.
- ¹⁴⁹ PPMI. (2026). Blockchain naming systems: Thematic paper. WEB4HUB: 'A Space for the Metaverse – Virtual Worlds and the Transition to Web 4.0'.
- ¹⁵⁰ WEB4HUB expert roundtable. (2026, 2 July). Opportunities for Europe in the Web 4.0 and Agentic AI Era.
- ¹⁵¹ PPMI. (Forthcoming). Agentic AI, trust and security. Thematic Paper.
- ¹⁵² The Linux Foundation. (2026). Linux Foundation announces DNS-AID project to advance decentralized AI agent discovery [Press release]. Available at: <https://www.linuxfoundation.org/press/linux-foundation-announces-dns-aid-project-to-advance-decentralized-ai-agent-discovery>.
- ¹⁵³ WEB4HUB expert roundtable. (2026, 2 July). Opportunities for Europe in the Web 4.0 and Agentic AI Era.
- ¹⁵⁴ Interview findings (July, 2026).
- ¹⁵⁵ Fratini, S., Pohle, J., Di Marco, D., Thabit Gonzalez, S., & Sgueo, G. (2026). *Digital sovereignty as a geopolitical strategy – Navigating dependencies, power, and democratic resilience in a changing global order* (JRC146878). European Commission, Joint Research Centre.
- ¹⁵⁶ WEB4HUB expert roundtable. (2026, 2 July). Opportunities for Europe in the Web 4.0 and Agentic AI Era.

¹⁵⁷ PPML. (Forthcoming). Agentic AI, trust and security: Thematic paper. WEB4HUB; PPML. (Forthcoming). Agentic AI: state of play: Thematic paper. WEB4HUB; PPML. (Forthcoming). Infrastructure in the age of agentic AI: Thematic paper. WEB4HUB.

¹⁵⁸ European High Performance Computing Joint Undertaking. (2025, 10 October). The EuroHPC JU selects six additional AI Factories to expand Europe's AI capabilities [Press release]. Available at: https://www.eurohpc-ju.europa.eu/eurohpc-ju-selects-six-additional-ai-factories-expand-europes-ai-capabilities-2025-10-10_en

¹⁵⁹ European Commission. (n.d.). AI Gigafactories. Available at: https://commission.europa.eu/topics/competitiveness/competitiveness-coordination-tool-projects/ai-gigafactories_en

¹⁶⁰ European Commission. (2026, 3 June). Proposal for a Regulation establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act) (COM(2026) 502 final). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2026%3A502%3AFIN>

¹⁶¹ Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030. Available at: <https://eur-lex.europa.eu/eli/dec/2022/2481/oj>

¹⁶² Interview findings (July, 2026).

¹⁶³ European Commission. (2026). A European open source strategy (COM(2026) 503 final). Available at: https://commission.europa.eu/news-and-media/news/strengthening-europes-tech-sovereignty-2026-06-03_en

¹⁶⁴ European Commission. (2026). Strategic roadmap for digitalisation and artificial intelligence in the energy sector (COM(2026) 501). Available at: https://energy.ec.europa.eu/topics/eus-energy-system/digitalisation-energy-system_en

¹⁶⁵ European Commission. (2025). Joint white paper for European defence readiness 2030 (JOIN(2025) 120 final). EUR-Lex. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025JC0120>

¹⁶⁶ Bria, F., Timmers, P., & Gernone, F. (2025). EuroStack: A European alternative for digital sovereignty. Bertelsmann Stiftung. Available at: <https://doi.org/10.11586/2025006>