European Parliament
2024-2029

TEXTS ADOPTED

P10_TA(2026)0022

European technological sovereignty and digital infrastructure

European Parliament resolution of 22 January 2026 on European technological sovereignty and digital infrastructure (2025/2007(INI))

The European Parliament,

– having regard to the Treaty on the Functioning of the European Union (TFEU), in particular Articles 173, 179 and 190 thereof,

– having regard to the Commission communication of 29 January 2025 entitled ‘A Competitiveness Compass for the EU’ (COM(2025)0030),

– having regard to the Commission communication of 11 February 2025 entitled ‘Commission work programme 2025: Moving forward together: A Bolder, Simpler, Faster Union’ (COM(2025)0045),

– having regard to Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe’s semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act)[1],

– having regard to Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)[2],

– having regard to the detailed report by the European Union Agency for Cybersecurity (ENISA) entitled ‘Foresight Cybersecurity Threats For 2030 – Update 2024’, published in March 2024[3],

– having regard to Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with

---

1 OJ L 229, 18.9.2023, p. 1, ELI: http://data.europa.eu/eli/reg/2023/1781/oj.
2 OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj.
3 https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024.

digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)[4],

– having regard to Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)[5],

– having regard to Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)[6],

– having regard to Regulation (EU) 2025/37 of the European Parliament and of the Council of 19 December 2024 amending Regulation (EU) 2019/881 as regards managed security services[7],

– having regard to the Commission White Paper of 21 February 2024 entitled 'How to master Europe's digital infrastructure needs?' (COM(2024)0081),

– having regard to Mario Draghi's report of 9 September 2024 entitled 'The future of European competitiveness',

– having regard to Enrico Letta's report of 17 April 2024 entitled 'Much more than a market',

– having regard to the Commission communication of 2 July 2024 entitled 'State of the Digital Decade 2024' (COM(2024)0260),

– having regard to Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030[8],

– having regard to Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (the Interoperable Europe Act)[9],

– having regard to Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information[10],

– having regard to Regulation (EU) 2024/795 of the European Parliament and of the Council of 29 February 2024 establishing the Strategic Technologies for Europe Platform (STEP), and amending Directive 2003/87/EC and Regulations (EU)

---

4 OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.
5 OJ L 151, 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.
6 OJ L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj.
7 OJ L, 2025/37, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/37/oj.
8 OJ L 323, 19.12.2022, p. 4, ELI: http://data.europa.eu/eli/dec/2022/2481/oj.
9 OJ L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj.
10 OJ L 172, 26.6.2019, p. 56, ELI: http://data.europa.eu/eli/dir/2019/1024/oj.

2021/1058, (EU) 2021/1056, (EU) 2021/1057, (EU) No 1303/2013, (EU) No 223/2014, (EU) 2021/1060, (EU) 2021/523, (EU) 2021/695, (EU) 2021/697 and (EU) 2021/241[11],

– having regard to 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 and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)[12],

– having regard to Regulation (EU) 2024/1309 of the European Parliament and of the Council of 29 April 2024 on measures to reduce the cost of deploying gigabit electronic communications networks, amending Regulation (EU) 2015/2120 and repealing Directive 2014/61/EU (Gigabit Infrastructure Act)[13],

– having regard to Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)[14],

– having regard to Regulation (EU) 2021/1153 of the European Parliament and of the Council of 7 July 2021 establishing the Connecting Europe Facility (CEF) and repealing Regulations (EU) No 1316/2013 and (EU) No 283/2014[15],

– having regard to Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240[16],

– having regard to Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013[17],

– having regard to Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU[18],

– having regard to Regulation (EU) 2023/588 of the European Parliament and of the Council of 15 March 2023 establishing the Union Secure Connectivity Programme for the period 2023-2027[19],

– having regard to Council Regulation (EU) 2021/2085 of 19 November 2021 establishing the Joint Undertakings under Horizon Europe and repealing Regulations

---

11 OJ L, 2024/795, 29.2.2024, ELI: http://data.europa.eu/eli/reg/2024/795/oj.
12 OJ L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj.
13 OJ L, 2024/1309, 8.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1309/oj.
14 OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj.
15 OJ L 249, 14.7.2021, p. 38, ELI: http://data.europa.eu/eli/reg/2021/1153/oj.
16 OJ L 166, 11.5.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/694/oj.
17 OJ L 170, 12.5.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/695/oj.
18 OJ L 170, 12.5.2021, p. 69, ELI: http://data.europa.eu/eli/reg/2021/696/oj.
19 OJ L 79, 17.3.2023, p. 1, ELI: http://data.europa.eu/eli/reg/2023/588/oj.

(EC) No 219/2007, (EU) No 557/2014, (EU) No 558/2014, (EU) No 559/2014, (EU) No 560/2014, (EU) No 561/2014 and (EU) No 642/2014[20],

– having regard to Council Regulation (EU) 2021/1173 of 13 July 2021 on establishing the European High Performance Computing Joint Undertaking and repealing Regulation (EU) 2018/1488[21],

– having regard to Council Regulation (EU) 2024/1732 of 17 June 2024 amending Regulation (EU) 2021/1173 as regards a EuroHPC initiative for start-ups in order to boost European leadership in trustworthy artificial intelligence[22],

– having regard to Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code[23],

– having regard to Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework[24],

– having regard to the joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 21 February 2025 to the European Parliament and the Council entitled 'EU Action Plan on Cable Security' (JOIN(2025)0009),

– having regard to the Commission communication of 29 January 2020 entitled 'Secure 5G deployment in the EU – Implementing the EU toolbox' (COM(2020)0050),

– having regard to the European Declaration on Digital Rights and Principles for the Digital Decade, which commits 'to promote a European way for the digital transformation, putting people at the centre'[25],

– having regard to the Commission communication of 30 December 2021 entitled 'Criteria for the analysis of the compatibility with the internal market of State aid to promote the execution of important projects of common European interest' (IPCEIs) (COM(2021)8481),

– having regard to Rule 55 of its Rules of Procedure,

– having regard to the report of the Committee on Industry, Research and Energy (A10-0107/2025),

A. whereas technological sovereignty should be seen as the whole value chain from excellence in research to creating better competition and achieving greater European sovereignty;

---

20 OJ L 427, 30.11.2021, p. 17, ELI: http://data.europa.eu/eli/reg/2021/2085/oj.
21 OJ L 256, 19.7.2021, p. 3, ELI: http://data.europa.eu/eli/reg/2021/1173/oj.
22 OJ L, 2024/1732, 19.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1732/oj.
23 OJ L 321, 17.12.2018, p. 36, ELI: http://data.europa.eu/eli/dir/2018/1972/oj.
24 OJ L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj.
25 OJ C 23, 23.1.2023, p. 1.

B. whereas the EU relies on non-EU countries for over 80 % of digital products, services, infrastructure and intellectual property;

C. whereas a few technological companies hold concentrated power over key digital markets and control over underlying internet infrastructure, including operating systems, computing, artificial intelligence (AI), search engines, social media capacity, digital advertising and payment services;

D. whereas our technological sovereignty will greatly depend on Europe's ability to create the market conditions needed for European companies to flourish and compete with each other, thereby increasing the quality of their products;

E. whereas the EU is at risk of failing to meet its digital decade targets and objectives, including the adoption of cloud, big data and AI;

F. whereas European firms contribute a minor share to global research and development (R&D) in software, internet technologies and electronics, while the United States and China lead in these sectors;

G. whereas the Commission's Digital Compass, Digital Decade Policy Programme, and Competitiveness Compass are essential frameworks for strengthening Europe's digital ecosystem, securing technological leadership and ensuring long-term economic resilience;

H. whereas digital infrastructure is composed of hardware elements related to connectivity, including fibre, 5G and 6G, submarine cables, satellites and spectrum, and computing, including semiconductors, data centres, HPC and quantum technologies, and of software elements including identity solutions, the Internet of Things, and cloud and AI systems, as well as the intermediary layer including advertising, search engines, payments and communication systems;

I. whereas the EU's competitiveness will increasingly depend on the digitalisation of all sectors, supported by resilient, safe and trustworthy digital infrastructure; notes, in this context, that the digital single market is a vital asset as it can enable companies to grow and scale up;

J. whereas the full potential of the digital single market remains untapped, with intra-EU trade in digital services representing just 8 % of GDP, which is significantly lower than the 25 % for trade in digital goods;

K. whereas the availability of eID schemes and digital public services and access to e-Health records are increasing, but there are still significant gaps in the provision of privacy preserving, fully user-centric, accessible and sovereign digital public services among Member States due to differences in the adoption of eID;

L. whereas eID is currently available to 93 % of the EU's population, but achieving 100 % of digital public services for citizens and businesses by 2030 remains challenging;

M. whereas interoperability and interconnectedness would enhance the competitiveness of the European economy and might benefit from policies such as open-source first and public money, public code, and the implementation of common and open standards;

N. whereas digital infrastructure is of key importance for EU industry, including the automotive industry and the possible development of connected and autonomous vehicles; whereas robust data and communications infrastructure is needed to support a secure ecosystem for connected and autonomous vehicles;

O. whereas fibre-optic networks form one of the backbones of the EU's digital infrastructure, enabling high-speed internet, 5G networks and future technological improvements;

P. whereas the EU is behind on the roll-out of 5G to meet its 2030 targets, with still limited fibre coverage of only about 64 % of European households being included;

Q. whereas investment needs in state-of-the-art connectivity in the EU are immense;

R. whereas resolving challenges related to access to land and grids is key to the successful deployment of digital infrastructure;

S. whereas the EU GOVSATCOM initiative aims to ensure the long-term availability of secure, reliable and cost-effective governmental satellite communication services for EU and national public authorities that manage critical security infrastructure and missions;

T. whereas chips play a crucial role in increasing the technological competitiveness and resilience of Europe;

U. whereas the Commission's Competitiveness Compass, the Clean Industrial Deal and the 2025 Commission Work Programme make little to no mention of semiconductor technologies despite their critical importance for the EU's industrial ambition;

V. whereas the Chips Act was an ad hoc adaptation mechanism aimed at addressing certain challenges regarding semiconductor shortages; whereas its areas of action are mostly limited to advanced semiconductors; whereas EU engagement on legacy semiconductors is insufficient; whereas the revision of the Chips Act is expected in September 2026;

W. whereas the existing European regional clusters in the semiconductor sector have a role to play and should be further strengthened;

X. whereas processors, memory technologies, graphics processing units (GPUs), and quantum chips are critical to Europe's digital infrastructure and supply chain security;

Y. whereas cloud services are fundamental to a wide range of computational activities and computing services that have become an essential enabler of competitiveness;

Z. whereas federated models could enhance the competitiveness of the EU market by facilitating the emergence of significant European alternatives, building on local market expertise and presence;

AA. whereas large-scale AI infrastructure, such as AI gigafactories, is essential for enabling open and collaborative development of the most complex AI models;

AB. whereas the AI value chain is still under development and tackling the development of AI models is only part of it; whereas European AI solutions may be developed using Europe's public and private computing infrastructure, driving innovation, and start-ups and small companies should be in particular beneficiaries of access to public computing infrastructure;

AC. whereas AI models that can be run on widely available hardware at moderate costs allow a greater number of actors to shape how AI systems are created and used, providing more immediate value in applications and enabling a more democratic use of AI;

AD. whereas at the moment, the roll-out, marketing and deployment of AI is often shaped by a small number of big tech companies; whereas some AI features are not being rolled out in the EU at the same time as in non-EU countries, creating a competitive disadvantage for European businesses and consumers;

AE. whereas data centres are an essential part of an advanced digital society, as enablers of distributed processing and effective data storage;

AF. whereas trusted capacity and availability of data storage is essential for European resilience and development; whereas most data centres in Europe are not owned by European companies;

AG. whereas building and operating large-scale data centres requires substantial investment;

AH. whereas around 9 % of global electricity consumption results from data centres, cloud services and connectivity;

AI. whereas submarine cables are critical infrastructure for global connectivity, economic stability and security, carrying over 99 % of international communications through them, and they remain vulnerable to physical damage, cyberthreats and geopolitical risks;

AJ. whereas secure and resilient digital infrastructure is crucial, particularly considering the increasing number of cyberattacks against the EU, its Member States and its industry and society;

AK. whereas the EU toolbox for 5G security is important for preventing cyberespionage and strengthening the resilience of supply chains in the EU's digital infrastructure;

AL. whereas 21 % of businesses cite compliance and legal uncertainties as a barrier to digital investment;

AM. whereas the 'one in, one out' approach ensures that all burdens introduced by Commission initiatives are considered and that administrative burdens are offset by removing burdens of equivalent value in the same policy area;

AN. whereas the energy consumption challenges in AI, cloud and quantum computing, as well as data centres, require the integration of sustainability into digital infrastructure strategies;

AO. whereas data centre power consumption is projected to nearly triple by the end of this decade, increasing from approximately 62 terawatt-hours (TWh) today to more than 150 TWh, thus escalating from 2 % to 5 % of total European power consumption;

AP. whereas the digital skills gap remains a major concern, with only 54 % of European citizens possessing at least basic digital skills – well below the 80 % target set in the digital decade policy programme;

AQ. whereas the shortage of ICT professionals in the EU is projected to reach 12 million by 2030, falling significantly short of the EU's target of 20 million skilled workers;

AR. whereas the 2024 State of the Digital Decade report and the Draghi report both stress the urgent need to invest in digital and science, technology, engineering and mathematics (STEM) skills to preserve Europe's technological capabilities and global competitiveness;

AS. whereas 60 % of EU companies report difficulties in recruiting skilled workers in areas such as AI, cybersecurity and clean technologies, posing a significant barrier to innovation, competitiveness and the green and digital transitions;

AT. whereas current labour market developments, including global lay-offs and political instability outside the EU, create an opportunity to attract high-skilled digital talent to the EU;

AU. whereas increasing competitiveness and resilience require appropriate funding; whereas public funding can act as a catalyst and private investment and competitive market forces are key for the long-term development of digital infrastructure;

AV. whereas a robust, agile and excellence-driven research and innovation (R&I) ecosystem is essential to ensure the EU's global competitiveness and leadership in strategic technologies, such as quantum and AI;

AW. whereas standardisation is at the core of genuine European digital and technological sovereignty; whereas the importance of standards is growing due to increasing technological competition across the world, particularly with the United States and China;

AX. whereas the EU is committed to negotiating comprehensive digital trade agreements (DTAs) to promote secure, resilient and competitive digital infrastructure development with partner countries;

AY. whereas the Commission has announced landmark DTAs with South Korea and Singapore, setting an important precedent for future agreements;

AZ. whereas Parliament and the Council have agreed on the 'EU horizontal provisions on Cross-border data flows and protection of personal data and privacy in the Digital Trade Title of EU trade agreements', which was endorsed by the Commission and remains an important tool in relation to digital trade and the establishment of new DTAs;

General introduction

1. Underlines that European sovereignty is the ability to build capacity, resilience and security by reducing strategic dependencies, preventing reliance on foreign actors and single service providers, and safeguarding critical technologies and infrastructure; calls for the development of a comprehensive risk assessment framework to monitor and address dependencies across the digital value chain; underlines that such a framework should serve as a basis for ensuring EU preparedness and resilience by enhancing European industrial policy and boosting domestic R&D and manufacturing capabilities in strategic technologies;

2. Believes that technological sovereignty is the capacity to design, develop and scale up digital technologies needed for the competitiveness of our economy, the welfare of our citizens and the EU's open strategic autonomy in a globalised world; believes that this includes ensuring the EU's ability to make autonomous decisions, engaging with trusted non-EU countries and entities, diversifying and strengthening supply chains and promoting the concept of openness and interoperability to ensure that Europe remains an attractive hub for investment;

3. Recognises the increasing concentration of power in non-EU companies, which constrains Europe's ability to innovate, compete and maintain control over its digital economy, society and democracy; is concerned by excessive dependencies on non-EU actors in critical areas such as cloud infrastructure, semiconductors, AI and cybersecurity – where market concentration and foreign control threaten to undermine Europe's competitiveness, democratic resilience and security;

4. Reaffirms that the EU must remain sovereign in enforcing its laws, especially in the digital field; firmly condemns and calls for the cancellation of the travel bans imposed by the United States on civil society leaders Imran Ahmed, Clare Melford, Anna-Lena von Hodenberg and Josephine Ballon, whose work contributes to a safer digital environment for all and holds digital platforms accountable, as well as the travel ban imposed by the United States on former EU Commissioner Thierry Breton, who played a key role in establishing EU digital rules; calls on the Commission and the Member States to deliver a firm response to these unprecedented attacks; notes recent enforcement actions taken under the Digital Services Act[26] for breaches of transparency and risk-mitigation obligations, such as the EUR 120 million fine against X; recalls that enforcement of the EU's digital legislation aims to ensure compliance with EU law and the protection of fundamental rights, and not to regulate political opinions; underlines that the deployment of new functionalities, including those based on generative AI, by very large online platforms must be accompanied by appropriate safeguards and risk-mitigation measures to ensure full compliance with EU law, in particular as regards the prevention of the dissemination of illegal or manipulated content; denounces the support provided by certain political parties – such as the AfD, Reconquête, Fidesz or Konfederacja – which repeat narratives originating from outside the EU and weaken the EU's digital legislation and democratic values;

5. Believes that the EU's industrial tech ambitions should focus on the key strategic technologies of the future, such as semiconductor technologies or quantum, that

---

[26] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj).

contribute to the EU's open strategic autonomy and are essential for our green, digital and defence transitions;

6. Recognises the shift in the geopolitical landscape and the resulting opportunity for market demand for European products and services; sees this as a window of opportunity to position Europe as a global leader in trusted and secure digital solutions;

7. Underlines the need to foster a supportive regulatory environment that encourages innovation, investment and the development of cutting-edge technologies in Europe, while protecting EU end users from the consequences of extraterritoriality;

8. Recognises the need for a comprehensive European industrial policy for the digital ecosystem, integrating all relevant policy domains such as market access, standardisation, R&D, investment, trade and international cooperation; calls on the Commission to develop this comprehensive policy with the aim of reducing harmful strategic dependencies, strengthening domestic value chains and ensuring a secure, trustworthy and innovation-driven digital ecosystem that adheres to European values;

9. Recalls that the high-tech product and digital services markets depend heavily on external supply chains, posing risks to sovereignty and resilience; stresses the importance of boosting industrial capacity and technological expertise in emerging and disruptive technologies to support the EU's open strategic autonomy;

10. Emphasises that boosting Europe's technological sovereignty in the era of rapid technological development requires enhancing innovation and commercialisation in order to build the necessary capabilities; highlights that Europe must transform itself into a globally attractive and agile business environment by reducing bureaucracy, enhancing regulatory predictability and fostering entrepreneurship and risk-taking;

11. Recognises that open strategic autonomy and democratic resilience must be at the core of the Commission's agenda and that a comprehensive approach must integrate procurement, funding and long-term institutional frameworks to establish sovereign digital infrastructure in critical domains;

12. Calls on the Commission to analyse and establish a comprehensive list of critical dependencies in digital infrastructure and technologies, assessing, at minimum, storage services, identity and payment systems, communication platforms, as well as the software, protocols and standards that support them, and to propose measures to promote market access for products and services with a strong positive impact on the EU's technological sovereignty, resilience and sustainability; believes, in that regard, that the use of specific award criteria in public procurement may be promoted in areas where such critical dependencies exist; believes that such criteria can help incentivise competition and strengthen European technological sovereignty by facilitating the procurement of European digital products and services, where possible;

Digital public infrastructure

13. Strongly believes that digital infrastructure is the backbone of our economy and that there should therefore be a base layer of digital public infrastructure (DPI) that ensures sovereignty and a competition-friendly market environment; observes that the market has not developed this base layer in many important areas, which has resulted in

monopolies and reliance on foreign actors; underlines that in order to fill this gap, the EU should take the lead in creating a strong foundation for DPI by creating layers of digital technologies consisting of semiconductors, connectivity solutions, cloud infrastructure, software, data and AI; believes that European DPI should be founded on fair and competitive economic models and also use governance models where neither private companies nor governments maintain centralised control; is of the opinion that it should be built on common and open standards, embrace interoperability and interconnectedness, so as to prevent user and vendor 'lock-ins', and spur innovation by facilitating new market entrants, and that it should also ensure privacy and security by default;

14. Believes that the deployment of DPI should be focused on areas where critical dependencies exist, as identified in the Commission's comprehensive list; calls on the Commission to prepare a detailed and comprehensive plan for establishing European DPI by identifying technologies that are best suited to European action, and urges the Commission and the Member States to dedicate appropriate resources to deploying European DPI;

15. Stresses that European DPI should be stimulated by coordinated action at EU level to ensure the presence and competitiveness of European providers as well as a competitive market environment; underlines that these objectives will not be achieved through regulation alone and will require significant public investment; recognises that the forthcoming multiannual financial framework (MFF) should therefore include additional funding for this purpose, focusing on EU added value and financing the base layer of European DPI;

16. Recognises that as part of the forthcoming MFF, the EU must commit to increased spending to achieve technological sovereignty; underlines that this should include a dedicated envelope for the development and deployment of the DPI layers identified in the Commission's comprehensive list, as well as additional funds to ensure a competition-friendly market environment in other digital areas;

17. Believes that the funding under the forthcoming MFF should prioritise active capacity-building in key hardware, software and service areas, including high-performance computing, quantum computing, encryption and communication, connectivity, cloud, data, web and AI ecosystems, and digital libraries;

18. Is of the opinion that European DPI should be based on EU values and remain open to like-minded non-EU partners; calls on the Commission and the Member States to sustain their efforts and add more impetus to the process with the UN Development Programme on DPI;

19. Recognises e-government services as a key enabler of efficient, secure and accessible public service delivery, which should be designed to facilitate digital identification, government data sharing and public sector payments without distorting markets or undermining existing private sector solutions; emphasises that the EU's approach to e-government services should focus on strengthening digital government-to-citizen and government-to-business interactions, while ensuring trust, interoperability and accessibility; believes, therefore, that secure and seamless access to public services requires a trustworthy e-identification framework and welcomes the announcement of a

‘business wallet’ aimed at significantly simplifying the interconnection between businesses and public authorities;

20. Calls on the Commission to further develop public interest data platforms, enabling secure cross-border data sharing between public and private entities for use cases, in particular, in healthcare, urban planning and environmental monitoring; calls, furthermore, on the Commission to promote interoperability between public interest and industry-specific data platforms, ensuring the seamless flow of data while minimising administrative burdens; notes that this could be achieved by leveraging existing market-driven solutions that foster innovation, maintain trust and uphold privacy and security standards;

21. Recognises that under the current legal framework, European citizens have the right to control their personal data and that data generated within the EU must be processed in accordance with EU law; stresses that safeguarding privacy and personal data is essential for building trust in the digital economy, allowing European consumers to engage with confidence, regardless of where their data is processed; highlights that European companies – particularly small and medium-sized enterprises (SMEs) – must be able to make use of data in a lawful, ethical and secure manner to drive sustainable growth and competitiveness;

Digital infrastructure

22. Highlights that digital infrastructure is the backbone of Europe’s economy and society and that its importance will continue to grow; calls on the Commission to include in the requested list of critical dependencies a comprehensive assessment of the composition of European digital infrastructure in order to adequately analyse the state of play, assess risks and coordinate action;

23. Believes that in order to strengthen digital infrastructure, it is essential to implement capacity-building initiatives in critical areas at EU level; considers that these initiatives should focus on developing a base layer of public infrastructure, such as a network of AI gigafactories and a European web index model; is of the opinion that this base layer will empower companies to develop their business models and boost technological sovereignty; points to the digital solutions created by the EU, such as the EU digital identity, that can offer innovative infrastructure for the EU’s digital economy;

24. Recognises the strategic importance of critical digital infrastructure and the need to strengthen their security and resilience; understands that critical digital infrastructure includes, but is not limited to, cables (terrestrial and submarine), cellular network towers, satellite communication systems, spectrum and radio equipment, cloud servers that contain sensitive information and data centres that process sensitive information, as well as certain software elements, including security software that protects critical networks and data centres;

25. Highlights the need to ensure that this infrastructure falls under EU jurisdiction, meaning that it fully adheres to EU law; stresses the importance of privacy and security-by-design; calls on the Commission. therefore, to introduce legislation to mitigate risks posed by high-risk vendors from non-EU countries, including risks posed by foreign-controlled energy resource providers;

26. Calls on the Commission, while preparing future legislative proposals and the forthcoming MFF, to concentrate efforts on deepening the single market, in line with the recommendations made in Enrico Letta's report entitled 'Much more than a market' and in Mario Draghi's report on 'The future of European competitiveness', with the aim of unlocking the potential of the digital single market;

27. Takes note of the recommendations laid down in these two reports that the EU needs a paradigm shift from promoting connectivity in the EU to establishing a single market for electronic communications and connectivity; supports a simplified, harmonised and innovation-friendly telecommunications framework that ensures fair competition and the accessibility of infrastructure;

28. Welcomes the Commission's white paper on how to master Europe's digital infrastructure needs, which outlines three pillars: creating the '3C Network' – 'Connected Collaborative Computing', completing the digital single market, and secure and resilient digital infrastructure for Europe;

29. Views the white paper and the subsequent consultation process as part of the preparation of the legislative initiatives planned for this term, including the Digital Networks Act; calls on the Commission to take a more holistic view of digital infrastructure throughout this process and to acknowledge that digital infrastructure comprises many elements beyond mere connectivity; underlines the need to accompany any new digital policy measure with an impact assessment;

30. Urges the Commission to simplify and harmonise telecommunications rules as part of the forthcoming Digital Networks Act and the broader Digital Package;

31. Calls on the Commission to introduce an EU cloud and AI development act to strengthen European data infrastructure and the promotion of European cloud providers; underlines that this act should aim to actively build a European single market for cloud and AI;

32. Acknowledges that deploying cutting-edge digital infrastructure across the EU requires substantial investment and recognises that both public and private funding are essential for achieving this goal; expresses concern over the persistent shortage of venture capital and investment financing in Europe, which undermines technological sovereignty; calls on the Commission to significantly scale up public-private investment instruments, including venture capital, strategic platforms and dedicated funding tools for start-ups and scale-ups in critical technology sectors; highlights the importance of leveraging public procurement to support the deployment and scaling of open and interoperable digital solutions and of ensuring that private capital, competition and innovation become the main drivers of Europe's digital transformation over the medium and long term;

High-speed connectivity

33. Is of the opinion that the upcoming Digital Networks Act must support the objective of providing all EU consumers with high-quality connectivity by 2030, especially in remote and rural areas, as well as removing administrative barriers for the roll-out of 5G, 6G and secure, high-speed broadband;

34. Recognises the increasing convergence of telecommunications infrastructure with cloud and edge technologies, and sees the potential of open radio access networks to deliver advanced technological solutions, reduce costs and enhance the interoperability of connectivity; believes that the future of connectivity lies in the complementarity of diverse technologies such as 5G/6G, Wi-Fi and satellite, where seamless integration benefits both businesses and consumers;

35. Recognises that with cloud and edge services at the core of their transformation, connectivity networks are evolving rapidly into platforms for innovation and will increasingly depend on cloud computing, AI, virtualisation and other technologies;

36. Calls for ambitious targets in the development and innovation of wireless communication networks, acknowledging the need for a broad-based approach that includes cloud computing, AI, edge computing and quantum computing; emphasises that the innovation ecosystem for electronic communications, especially for vertically integrated telecoms, should remain market-driven, and insists that future regulatory measures be based on thorough, knowledge-based impact assessments of existing regulations;

37. Recognises that competition between operators of all sizes remains a key driver of investment in connectivity networks; calls on the Member States to ensure that copper networks are switched off progressively in favour of fibre-optic or 5G technologies, in particular where regular maintenance or updates of the network are needed, thus ensuring that the shift is carried out in an attainable manner and allowing providers to plan logistically and financially in advance;

38. Stresses that all consumers in the EU should have access to adequate quality, reliable and affordable connectivity, thus contributing to increased demand for connectivity services; calls on the Commission and the Member States to expand and upgrade digital networks, especially in rural areas, and to support public-private investments in broadband and 5G/6G deployment, while maintaining cybersecurity standards and secure-by-design principles;

39. Is convinced that, as digital connectivity infrastructure such as fibre, 5G and 6G will be crucial for future industrial competitiveness, the forthcoming MFF should include funds for the large-scale deployment of network infrastructure, bridging the existing deployment gap to achieve the 2030 Digital Decade targets, creating pan-European 5G coverage for citizens' use and ensuring the successful deployment of Industry 4.0 tools;

Fibre

40. Stresses the importance of accelerating the deployment of fibre-optic networks and modern wireless communications systems that can deliver fast, secure and reliable digital services;

41. Recognises that the need to prioritise direct fibre connections for homes, businesses and public institutions is crucial to ensure ultra-fast and reliable connectivity, in addition to network roll-outs with public works, such as roads, water and electricity, to streamline fibre roll-out;

42. Welcomes the introduction of the Gigabit Infrastructure Act, which responds to the growing needs for faster, reliable and data-intensive connectivity; recognises the importance of the shared use of ducts and poles for deploying very high capacity networks to optimise resources and reduce costs; urges the Member States to streamline permitting processes and harmonise regulations to lower financial and administrative barriers to the expansion of fibre infrastructure;

5G and 6G

43. Believes that private investments are essential for deployment of electronic communication networks, 5G and 6G that are advanced enough in terms of transmission, speed, storage capacity, edge computing power and interoperability;

44. Stresses that the enforcement and implementation of the Gigabit Infrastructure Act is further necessary for the creation of a one-stop shop for permits and a centralised digital permitting process to reduce delays in infrastructure deployment and to ensure uniform rules for infrastructure access, pricing and environmental impact assessments; calls, in this regard, for strong efforts in this area;

45. Takes the view that the EU needs strong cybersecurity protection in all critical infrastructure sectors, with stricter measures to de-risk high-risk vendors in 5G and 6G networks, ensuring dense deployment of small cells and macro towers, particularly in urban and rural areas with inconsistent coverage, and ensuring the sustainability and energy efficiency of the infrastructure so as to support Europe's global competitiveness in the digital economy;

Spectrum

46. Calls on the Commission and the Member States to work towards enhanced coordination of spectrum allocations, in particular through earlier identification and the harmonisation of the release of new frequencies, starting with 6 GHz frequencies; calls for a radio spectrum policy that promotes investment in Europe, including through the harmonisation of spectrum assignment policies across the Member States to accelerate 5G deployment based on best practices, the promotion of longer license durations and access to new spectrum such as the upper 6 GHz band in order to meet future demand and enable 6G; believes that a shared effort from public and private entities is necessary in order to increase the competitiveness of Europe and not lag behind the fastest growing networks in the world, i.e. in China and South Korea;

Satellites and satellite communication systems

47. Underlines the importance of satellite-based communications in developing EU digital infrastructure, increasing its resilience, strengthening the capabilities of EU actors, and reducing dependence on non-EU providers, particularly in the area of defence; highlights the need to provide alternative connectivity solutions for consumers in remote and rural areas;

48. Highlights the strategic role of the EU space programme, as one of the pillars of EU sovereignty, in providing state-of-the-art and secure positioning, navigation and timing services for Galileo and EGNOS and cost-effective satellite communication services for GOVSATCOM; notes that this allows the EU and its Member States to have greater

sovereignty in their satellite capabilities, including geopositioning, earth observation, space surveillance and connectivity; welcomes, in particular, the EU GOVSATCOM and IRIS^2 programmes, which aim to ensure the short- and long-term availability of secure, reliable and cost-effective governmental satellite communication services for EU and national public authorities that manage critical security infrastructure and missions;

49. Deplores the strong dependence on non-EU data for the tracking and surveillance of space objects; stresses the need for Europe to urgently reinforce its own capabilities and infrastructure in space situational awareness (SSA) to ensure open strategic autonomy and security; calls on the Commission and the Member States to significantly increase investment in EU-owned surveillance and tracking assets, and to develop effective mechanisms for information-sharing among the Member States, enabling Europe to independently monitor and protect its critical space infrastructure;

50. Stresses the importance of private sector involvement in launcher technologies to further accelerate the deployment of IRIS^2; stresses the importance of fostering a robust and competitive European space launch sector through greater private sector involvement and support for upstream and downstream industries; calls on the Commission to promote a European space industrial policy that strengthens sovereignty in space technologies and services by reducing strategic dependencies and improving the operational governance of European space programmes;

51. Calls, to this end, for concrete measures to facilitate the provision of satellite services throughout Europe, including by defining common procedures and conditions; calls, in parallel, for fair competition, with clear and enforceable rules for all satellite constellations accessing the EU market;

52. Notes that there are currently several issues with latency in satellite networks and recognises that the integration of satellite networks with 5G and, in the future, 6G technologies is pivotal in extending the reach and reliability of terrestrial networks;

High-performance computing (HPC) systems

53. Recognises the progress made in recent years in enhancing HPC; calls on the Commission to continuously integrate and enhance the computing power at EU HPC centres, in particular, enhancing the training of AI models and preparing for future advancements in supercomputing;

54. Calls on the Commission to develop a coordinated strategy to bridge the gap between Europe’s cutting-edge HPC technology and its practical, scalable deployment across industries, including by creating a public network for supercomputing; notes that this strategy should foster collaboration between public institutions and private sector partners, including SMEs, to ensure that Europe’s HPC capabilities become a key driver of economic competitiveness and technological sovereignty;

55. Highlights that HPC centres must ensure accessibility for developers and deployers of AI foundation models, generative AI and applied AI; notes that EuroHPC Centres should be available for these use cases and particularly for SMEs, start-ups and scale-ups; emphasises that this must be seamlessly complemented by initiatives to enable the development and deployment of AI in the EU;

56. Welcomes the creation of new AI factories; underlines that AI factories will upgrade EuroHPC supercomputers to deliver computing capacity for AI and support start-ups and scale-ups in the training and large-scale development of general-purpose and trustworthy AI models;

Hardware for computing: semiconductors, chips and quantum chips

57. Believes that urgent action is needed to boost EU domestic semiconductor manufacturing, improving supply chain resilience by forming strategic global partnerships, encouraging start-ups and innovation, fostering cross-border collaboration in advanced semiconductor development and providing financial incentives, regulatory support and market access;

58. Emphasises the need for legal certainty to support semiconductor development, ensuring secure supply chains for critical raw materials and avoiding disruptions caused by investment uncertainties;

59. Urges to give utmost political importance to ensuring a sufficient supply of AI chips in the EU and to make it a focal point of EU digital industry policies; notes the increase in demand for AI chips driven by expanding applications in cloud computing, edge devices, autonomous systems and generative AI;

60. Calls on the Commission to react to the new geopolitical realities and the use of digital supply chains as pressure tools; urges the Commission to find a negotiated solution to the US ban on the export of AI chips to 16 EU Member States;

61. Calls on the Commission to put advanced AI chips, including their design and production, at the core of the revision of the Chips Act; calls on the Commission to present the revision this year, featuring a long-term strategy rooted in current geopolitical realities that builds European strategic indispensability through technological leadership, adequate production capabilities and a strong R&D ecosystem, which will be essential to secure European sovereignty in increasingly troubled times; believes that it is crucial to strengthen the interactions among research, training, suppliers and robust public infrastructure to accelerate the path from research, development, testing and finally full-load production;

62. Believes that the EU should enhance its efforts on quantum chip development if it intends to accelerate the time-to-market for EU industrial innovation in quantum technology;

63. Calls on the Commission to support the manufacturing within the EU of widely used chips e.g., for electronic devices and cars; calls for support for the development of chips that reduce the energy consumption of the digital sector;

64. Underlines the need to support the performance of the circular economy and recalls that information and communications technology products and other electronics are part of the priority product groups in the working plan to be adopted by April 2025 under Regulation (EU) 2024/1781[27];

---

[27] Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 establishing a framework for the setting of ecodesign requirements for sustainable

65. Believes that additional funding under the forthcoming MFF must be allocated to the development of semiconductor production capacities and other next-generation semiconductor technologies and processes (e.g. photonic chips, wide-bandgap chips, as well as design, manufacturing, testing, assembly and advanced packaging) within the EU;

Cloud services

66. Recognises that there is a market need for sovereign solutions that offer enhanced levels of control over data for certain categories of sensitive data and acknowledges the risks associated with reliance on single dominant providers; calls for a strategy for reducing reliance on foreign cloud providers, while fostering European alternatives;

67. Notes that the discussions on the EU Cybersecurity Certification Scheme for Cloud Services have not brought any results; points out that there are sovereignty considerations, in particular related to the extraterritoriality of binding legal regimes, that cannot be solved through technical discussions; calls on the Commission to propose a definition of sovereign cloud and its scope of application in the planned cloud and AI development act;

68. Notes the need to secure data storage and computational power, and distributed computing infrastructure; calls on the Commission to ensure that cloud users have the ability to choose solutions that meet their needs by urgently removing barriers to switching and diversifying providers through multi-cloud strategies, and by fostering a competitive European cloud market, thereby reducing reliance on single providers and enhancing digital sovereignty;

69. Calls on the Commission to leverage initiatives such as 8ra and IPCEI CIS to advance decentralised cloud and edge infrastructure, which are enablers of sovereignty and contribute to reducing reliance on foreign providers and ensuring resilience while enhancing operational flexibility within Europe;

AI systems

70. Welcomes the InvestAI initiative, including the AI gigafactories; emphasises the need for Europe to position itself as a global leader in AI model training, scientific research and quantum computing advancements; is committed to further supporting AI development by launching initiatives such as AI factories to provide computing power for start-ups, scale-ups and researchers;

71. Calls on the Commission to further support the design and development of European AI and to adopt policies and measures that will enable European industrial sectors to benefit from their data and AI deployment;

72. Emphasises that the delayed deployment of AI-driven innovations hinders technological progress, market competitiveness and digital transformation within the EU;

---

products, amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and repealing Directive 2009/125/EC, (OJ L, 2024/1781, 28.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

73. Expects that the public-private financing model will unlock unprecedented private investment in AI that will open up access to supercomputers for start-ups and industry to supercomputers;

Quantum

74. Recognises the urgent need to define a clear roadmap for quantum technology development, including quantum computing and quantum encryption, ensuring that public and private investments lead to tangible commercial applications;

75. Calls on the Commission to conduct an assessment of existing national quantum sandbox frameworks and how existing legislation applies to them in order to prevent market fragmentation; welcomes the announcement of the Quantum Strategy and Quantum Act in the Commission's Competitiveness Compass;

76. Urges the Commission to ensure that the Quantum Act, accompanied by an impact assessment, positions Europe as the leading region for quantum excellence and innovation by investing in R&D and innovation, mobilising funding to scale up the European quantum ecosystem, capabilities and production, and ensuring Europe's leading quantum research is commercialised in Europe; underlines that it should deliver tangible technological applications by fostering policies that accelerate technological maturity and facilitate the transition from research to commercial success;

77. Calls for targeted investments, industry collaboration and regulatory frameworks that support the development, scaling and market adoption of quantum technologies across key sectors;

78. Calls for a coordinated EU strategy for post-quantum cryptography to protect data from future cyberthreats;

Data centres

79. Calls on the Commission to support ecosystems for sharing industry-specific data within industrial sectors, fostering collaboration and driving innovation, while maintaining data sovereignty and ensuring compliance with EU regulations, as outlined in the Data Act; urges the Commission for strong enforcement to ensure that dominant market players do not impose unfair terms on SMEs and mid-sized enterprises when accessing and sharing data;

80. Believes that there is a need to ensure interconnected infrastructure that would allow data centres to work together efficiently under common standards with high-speed connectivity, while flexibility, security and scalability would be maintained; believes this interconnected system would help in ensuring distributed redundancy so that data and services remain available even in the event of a data centre failure;

81. Calls on the Commission to prioritise interoperability across platforms, enabling the seamless integration of data across businesses and sectors, in alignment with the requirements of the Data Act, which mandate data portability and interoperability obligations for cloud and edge services; stresses the need for the robust enforcement of these provisions to prevent vendor lock-in and ensure that European industrial ecosystems can leverage data-driven innovation without technical or contractual barriers;

82. Recalls the Commission's plan to make data centres climate-neutral and highly energy efficient by 2030; sees the need to improve the integration of data centres with the energy system, focusing on heat reuse and providing flexibility services to the electricity grid needs; recognises the need to incentivise research for cooling and energy-efficient processors, while special attention should be given to supporting EU data centres; urges the Commission to ensure clear and consistent implementation of existing legal requirements for data centre operators across EU legislation and the Member States;

83. Calls on the Commission and the Member States to increase and target public investment and to incentivise private investment in digital infrastructure to enable the growth and modernisation of data centres;

Submarine cables

84. Calls on the Commission to take coordinated action to protect submarine cables and reinforce cable security and repair capabilities; stresses the need for continued investment in the construction of new submarine cables to ensure redundancy; welcomes the EU's role in co-financing such projects to enhance digital infrastructure and connectivity across the Member States; calls on the Commission to explore potential synergies between the maintenance of undersea digital and energy infrastructure;

85. Emphasises the importance of improving EU and Member State repair capabilities and response mechanisms to handle submarine cable disruptions, which are essential for maintaining secure and uninterrupted communications; underlines the importance of international cooperation in repairing sabotaged cables and facilitating the necessary investments, and calls for the establishment of an EU-based rapid-response repair fleet to ensure swift recovery and operational continuity in the event of disruptions; calls on the Commission to carry out an assessment of regulatory measures to ensure fair access and security, regardless of whether the infrastructure is privately or publicly owned;

86. Welcomes the adoption of the action plan on cable security, which will be organised around four pillars: prevention, detection, response and repair, and deterrence; highlights the importance of its full and timely implementation; urges, in the current geopolitical context, increased investment in technologies to strengthen the security and resilience of subsea and offshore infrastructure;

87. Calls on the Commission to promote R&I to enable advanced technological innovations in cable security, including early warning systems and AI-driven threat assessments;

88. Urges the Commission to review available instruments designed to better leverage private investments in support of Cable Projects of European Interest (CPEIs); calls on the Commission to include submarine cable projects in the list of IPCEIs; recognises the need to streamline and simplify the application and administrative process governing IPCEIs;

Cybersecurity

89. Recalls the legislative work carried out over the previous legislative term aimed at significantly improving cybersecurity in the EU; welcomes, in particular, the adoption

of the Cyber Resilience Act, the Cyber Solidarity Act and the NIS2 Directive; stresses the need for the harmonised and timely implementation and enforcement of these measures;

90. Calls on the Commission to present an evaluation report on the Cybersecurity Act and to propose a legislative act to review it in order to strengthen the EU's cybersecurity framework, with a particular focus on the interplay between sovereignty and security; calls, furthermore, on the Commission to enhance the protection of strategic and critical infrastructure and prevent foreign interference from entities subject to extraterritorial legislation, as well as accelerating the adoption process for EU cybersecurity certification schemes; calls for ENISA's mandate to be strengthened to coordinate crisis response, oversee cybersecurity certification for critical infrastructure and ensure uniform implementation of cybersecurity standards across the single market;

91. Emphasises the importance of the upcoming European internal security strategy in strengthening cybersecurity and critical infrastructure protection;

92. Notes with concern that, according to the second report on Member States' progress in implementing the EU toolbox on 5G cybersecurity, 14 Member States have yet to implement any restrictions on high-risk suppliers, posing significant security vulnerabilities; calls for the full implementation of the EU toolbox for 5G security in order to reduce reliance on high-risk vendors; calls on the Commission to make the toolbox binding, specifically with regard to high-risk vendors in critical infrastructure;

Simplification

93. Notes that to achieve true technological sovereignty, the EU must have viable commercial alternatives; stresses that the EU must urgently pursue a comprehensive agenda of simplification and bureaucracy reduction to foster an innovation-friendly environment capable of supporting competitive European alternatives to dominant global digital players; underlines that excessive administrative burdens, fragmented regulatory frameworks, an incomplete digital single market and overly complex compliance procedures disproportionately impact European start-ups, scale-ups and SMEs, limiting their capacity to compete at global level; recognises that the EU should therefore prioritise regulatory streamlining and the deepening of the digital single market, ensuring that legislation is proportionate, innovation-driven and does not stifle the development of European technological solutions;

94. Emphasises the need for new legislative proposals to be aligned with better regulation principles, ensuring that any new digital policy measure that affects competitiveness is accompanied by an impact assessment, including a competitiveness, SME and small mid-cap check that evaluates whether a given legislative instrument is necessary, proportionate and does not create unnecessary burdens for businesses, especially SMEs, and thus its effects on competitiveness, investment prospects and consumer welfare;

95. Highlights that the simplification of EU legislation must not endanger any of the fundamental rights of citizens and businesses and thus jeopardise regulatory certainty; believes that any simplification proposal should not be rushed or proposed without proper consideration, consultation and an impact assessment;

96. Welcomes the Commission's commitment to fully implement the principle of burden reduction for companies in EU legislation; calls on the Commission, therefore, to enhance its efforts by aiming to remove more cost and administrative burdens for businesses compared to the benefits that would be derived from any new regulatory requirements introduced at EU level in the same policy area, so that barriers to market entry are removed to help European companies to scale and grow;

97. Calls on the Commission to ensure consistent simplification, implementation and enforcement of EU digital legislation through the Digital Package, streamlining definitions and reporting procedures, assessing ways to alleviate reporting obligations and reducing the gap between industry and government;

98. Believes that supporting companies and innovators to stay in Europe by developing the EU as an attractive and agile business environment is key to enhancing technological sovereignty; emphasises, in that regard, that excessive regulation and administrative burdens should be avoided and that EU rules should be clear, consistent, predictable, proportionate and technologically neutral, thus maintaining a globally competitive regulatory environment; believes that new public procurement methods and the development of regulatory sandboxes and test beds should also contribute to an innovation-friendly framework;

99. Welcomes the Commission's proposal of a 28th legal regime, recognising that a single, harmonised set of EU-wide rules will be a game changer for digital investment and innovation; believes that reducing regulatory fragmentation across 27 national legal regimes will boost private investment, lower compliance costs and accelerate the deployment of next-generation digital infrastructure, products and services; encourages the Commission to ensure that this framework specifically addresses regulatory barriers in the digital sector, such as permitting and cross-border data flows, in order to create a true digital single market;

100. Urges the Commission to create a single point of contact to simplify the application process for private-sector access to EU funding mechanisms, ensuring that private companies, SMEs and start-ups can more easily participate in digital investment programmes;

Energy

101. Emphasises that data centres will put additional pressure on electricity grids, making it imperative to reinforce them through anticipatory investments; stresses that data centres can also help stabilise the grid by participating in demand-side flexibility; calls for measures to incentivise such contributions based on the implementation of the revision of the European electricity market reform;

102. Calls on the Commission and the Member States to propose and implement instruments that ensure orderly planning of the escalating energy demand from data centres, facilitating their strategic placement near available energy sources and thus minimising reliance on the broader grid infrastructure;

103. Recognises that fibre is more energy efficient than traditional copper networks; acknowledges the importance of reducing energy consumption in data transmission and ensuring long-term stability and efficiency;

104. Calls on the Commission to ensure a reliable and sufficient clean energy and net-zero technology supply to support the digital infrastructure of the future;

Skills

105. Recognises the urgent need for more skilled professionals in digital fields to meet the EU's strategic objectives; calls on the Member States to develop national strategies and incentives to retain European talent and attract the world's best digital professionals, thereby strengthening the EU's innovation capacity and technological leadership;

106. Stresses the importance of closing the digital and STEM skills gap to enhance technological resilience, innovation capacity and open strategic autonomy; calls on the Member States to strengthen investments in digital education, upskilling and reskilling, particularly in areas essential for the green and digital transitions; supports prioritising investments that address digital skills shortages, particularly in AI, cybersecurity, data analysis and clean technologies, in order to support innovation and technological sovereignty;

107. Calls for coordinated strategies at national level to improve access to high-quality STEM education, promote lifelong learning and attract talent to ICT and related fields; encourages partnerships between public institutions, industry and educational providers to ensure alignment between curricula and evolving market needs;

108. Calls for intensified efforts to improve digital literacy and skills across all demographics, focusing on early STEM education, vocational education and training, and lifelong learning in digital technologies; recommends aligning national education and training strategies with the EU Digital Decade goal of 80 % of the population possessing basic digital skills by 2030, with a focus on gender-inclusive policies to increase women's participation in ICT and STEM fields; calls on the EU institutions to take concrete steps to uphold the commitments referred to in the European Declaration on Digital Rights and Principles for the Digital Decade, both within the EU framework as in the Union's cooperation with third countries;

109. Supports the establishment of a common EU certification framework for digital and technical skills to improve the recognition and portability of qualifications among the Member States;

110. Encourages the European Investment Bank and national development institutions to support digital talent retention by co-investing in European deep-tech start-ups, ensuring that EU-funded innovation remains within the region and contributes to Europe's technological sovereignty;

Research and innovation

111. Recognises the importance of bridging the gap between research and commercialisation and calls on the Commission to enhance the valorisation of innovation within the EU;

112. Believes that Europe's ability to transform research into market-ready solutions is critical for building necessary capabilities and reducing reliance on non-EU technologies;

113. Emphasises that funding needs to be strategically allocated to accelerate the development and market introduction of solutions that strengthen Europe's technological resilience and drive innovation; underlines the importance of a more agile, excellence-based funding structure, particularly in improving the translation of research into industrial applications; calls for increased investment in R&I to strengthen Europe's knowledge and technological capabilities and insists that EU research, development and innovation (RDI) funding be based on open competition and excellence;

114. Highlights the need for policies that support industrial innovation, including targeted investment in key strategic technologies where Europe can lead globally, such as quantum computing, in order to build an innovation ecosystem;

115. Believes that private investment in RDI is of utmost importance and calls for the EU to create incentives that effectively leverage private funding for the development of critical technologies, including through public-private partnerships;

116. Stresses the urgent need for stronger incentives to mobilise private sector capital for technology-driven innovation; encourages the Member States to introduce targeted fiscal incentives, regulatory simplification and risk-sharing instruments designed to attract private equity to the technology and digital sectors; highlights the need to streamline cross-border capital flows within the single market to facilitate access to finance for innovative European start-ups;

Standards

117. Strongly believes that promoting interoperability and EU standards is paramount to fostering competitiveness in the technology sector, as it ensures that products can be connected and work with each other, thus fostering innovation and open markets; recalls that both interoperability and common technological standards pave the way for the functioning of the single market;

118. Underlines that the Commission must increase its engagement in existing global standardisation structures and focus on the international uptake of European standards through a bottom-up approach, avoiding centralisation;

Partnerships

119. Welcomes the EU's commitment to negotiating DTAs that facilitate secure and competitive digital infrastructure development with partner countries; encourages the Commission to increase efforts in negotiating DTAs with additional partner countries;

120. Calls on the Commission to accelerate technical cooperation in multilateral forums such as the G7, the Organisation for Economic Co-operation and Development and the World Trade Organization (WTO) so as to develop global standards for digital governance, AI regulation, cross-border data flows and emerging technologies;

121. Urges the Commission to advance negotiations on a permanent solution to the WTO moratorium on e-commerce to prevent the introduction of digital tariffs, ensuring international digital trade remains open, predictable and conducive to innovation;

°

° °

122. Instructs its President to forward this resolution to the Council and the Commission.