Centres for European Policy Network
FREIBURG | BERLIN | PARIS | ROMA

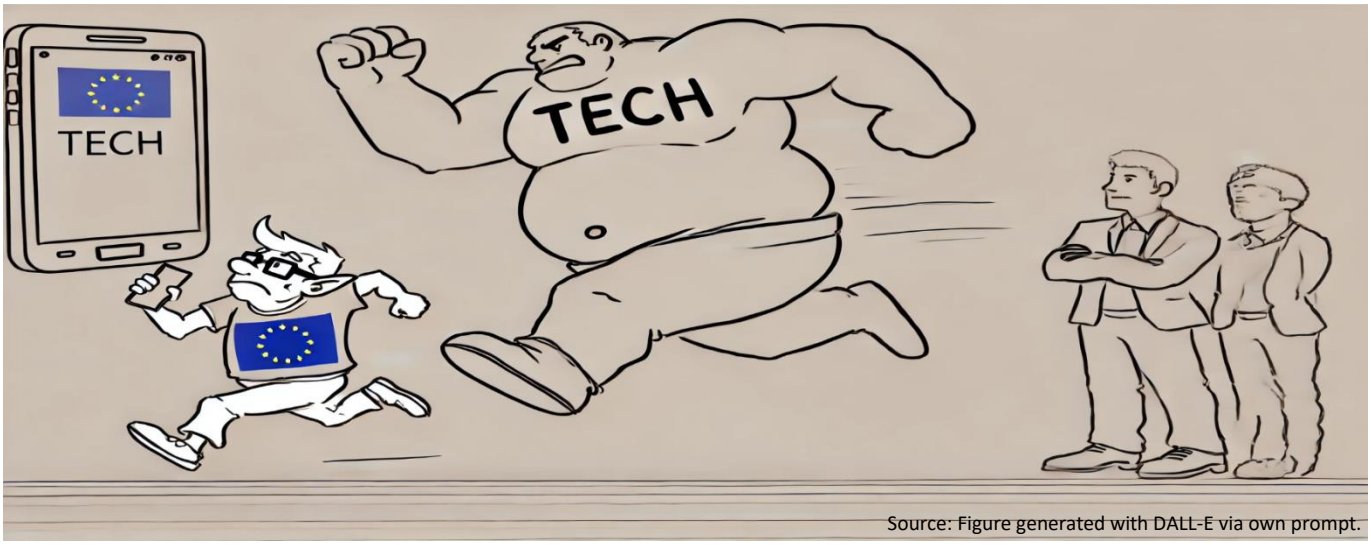
cepInput special

Mission Letters No. 2 | 2024 29 October 2024

The EU's Digital Ambitions

Candidates, Portfolios and EU Initiatives for the EU Commission 2024-2029

Philipp Eckhardt, Matthias Kullas, Anja Hoffmann and Anselm Küsters



Source: Figure generated with DALL-E via own prompt.

Between the 4th and 12th of November, the candidates for the upcoming European Commission 2024-2029 will be closely scrutinised by the members of the European Parliament. During these confirmation hearings, the Commissioners-designate will have to answers questions on EU initiatives outlined by the Commission President Ursula von the Leyen in her Political Guidelines and Mission Letters to the new Commissioners. In the run-up of the hearings, this cepInput takes a closer look at the candidates, portfolios and important EU initiatives which will shape the future EU digital policies.

- In the new legislature, the Commission's main objectives will be to further strengthen cybersecurity, catch up on Artificial Intelligence (AI) and cloud computing, stimulate investment in digital infrastructures, make the EU's data policies more consistent and improve the protection of citizens in the digital environment.
- The revision of the EU Cybersecurity Act should make sure that the EU legislator (not the Commission) decides on the inclusion of sovereignty requirements within EU cybersecurity certification schemes. The legislator must also set clear deadlines for the implementation of such schemes.
- To foster data sharing, the EU must prioritise the elimination of legal ambiguities and overlaps in data-related provisions, promote legally compliant anonymisation and use of synthetic data, resolve conflicts with core data protection principles and enable innovation-friendly handling of the General Data Protection Regulation.
- The Commission's sweeping plans to steer AI innovation and deployment from the top risk tying up Europe's technological future in bureaucratic red tape. The ambition to boost AI capabilities is laudable, but granting privileged access to select startups could distort markets, while the planned public funding is still far below that of competing actors. A more holistic strategy would reduce regulatory hurdles, foster a business-friendly environment for SMEs, and incentivise private investment. The future of European AI lies not in European champions, a few supercomputers, and centralised planning, but in unleashing its entrepreneurial energies.

1 Run-up to the Next European Commission 2024-2029

Following the elections of the European Parliament in June and the re-election of Ursula von der Leyen for her second term as President of the European Commission 2024-2029 in July, the remaining 26 members of the College of Commissioners have to be appointed in the coming weeks. Based on proposals by the EU Member States, Ursula von der Leyen presented her list of candidates[1] in September along with a revised organisational structure of the next European Commission regarding the functions and the policy portfolios the of the commissioners. Before the College of Commissioners will be collectively approved by the European Parliament and appointed by the European Council, each candidate will be closely scrutinised by the members of the European Parliament. During these public confirmation hearings, which will take place between the 4th and 12th of November[2], the Commissioners-designate will have to answers questions especially on those prospective EU initiatives and legislative projects which have been outlined by the Commission President in her Political Guidelines[3] and also on their respective tasks as assigned in the Mission Letters[4] addressed to each of them. In the run-up of the hearings, this cep**Input** takes a closer look at the Commissioners-designate as well as at their portfolios, tasks and important EU initiatives which will shape the future specifically of the EU digital policies.

2 Relevant Commissioners-designate, Functions and Portfolios

The revised organisational structure of the next European Commission regarding the organisational functions and the policy portfolios of the Commissioners aims to reflect that EU initiatives and legislative projects often involve different subject matters and pursue various objectives simultaneously – e.g., environmental protection, cost-effectiveness, international competitiveness, and social aspects. While Ursula von der Leyen emphasises[5] that according to the EU treaties[6] all members of the college of commissioners are equal, her organisational revision introduces a functional distinction between "Executive Vice-Presidents" and "regular" Commissioners. All members of the College of Commissioners will be assigned a policy portfolio with specific tasks for implementing the existing EU acquis and for developing new EU initiatives in the respective policy fields. To fulfil these tasks, each College member will be supported by one or more Directorates-General (DGs) assigned specifically to them. In addition, however, the six Executive Vice-Presidents will play a leading role in a thematic priority area, working together with one or more regular Commissioners by giving "guidance" to them. Consequently, to or more members of the College of Commissioners will cooperate on a specific EU initiative or legislative project, albeit with different functions ranging, e.g., from "leading" to "overseeing" or "supporting" to "contributing". With regard to the EU's digital policies, the following Commissioners-designate, organisational functions and policy portfolios are relevant:

1 European Commission (2024), List of Commissioners-designate (2024-2029).
2 European Parliament (2024), Confirmation hearings for the European Commission.
3 European Commission (2024), Political Guidelines for the next European Commission 2024-2029; see De Petris, A. et al. (2024), The Political Guidelines 2024-2029 of the European Commission "von der Leyen II" – Recommendations for Concrete EU Measures to Implement Them, cepInput 12/2024.
4 European Commission (2024), List of Commissioners-designate (2024-2029).
5 European Commission (2024), Press statement of 17 September 2024 by President von der Leyen on the next College of Commissioners.
6 Treaty on European Union (TEU), Art, 17; Treaty on the Functioning of the European Union (TFEU), Art. 244 et seq.

Henna Virkkunen — Tech Sovereignty, Security and Democracy

Country: Finland

European Parliamentary Group: European People's Party (EPP)

Portfolio: Executive Vice-President for Tech Sovereignty, Security and Democracy

Assigned DGs: Communications Networks, Content and Technology (DG CONNECT) / Digital Services (DG DIGIT)

Lead President: Works under the guidance of

Ursula von der Leyen, President of the EU Commission

Michael McGrath — Democracy, Justice, and the Rule of Law

Country: Ireland

European Parliamentary Group: European People's Party (EPP)

Portfolio: Commissioner for Democracy, Justice, and the Rule of Law

Assigned DG: Justice and Consumers (DG JUST)

Lead Vice-President: Works under the guidance of

Henna Virkkunen, Executive Vice-President for Tech Sovereignty, Security and Democracy

Olivér Várhelyi — Health and Animal Welfare

Country: Hungary

European Parliamentary Group: Independent

Portfolio: Commissioner for Health and Animal Welfare

Assigned DG: Health and Food Safety (DG SANTE)

Lead Vice-Presidents: Works under the guidance of

- Teresa Ribera Rodríguez, Executive Vice-President for Clean, Just and Competitive Transition, and
- Roxana Mînzatu, Executive Vice-President for People, Skills and Preparedness

Stéphane Séjourné

Prosperity and Industrial Strategy

Country: France

European Parliamentary Group: Renew Europe

Portfolio: Executive Vice-President for Prosperity and Industrial Strategy

Assigned DG: Internal Market, Industry, Entrepreneurship and SMEs (Grow)

Lead President: Works under the guidance of

Ursula von der Leyen, President of the EU Commission

Ekaterina Zaharieva

Prosperity and Industrial Strategy

Country: Bulgaria

European Parliamentary Group: European People's Party (EPP)

Portfolio: Commissioner for Prosperity and Industrial Strategy

Assigned DG: Innovation and Research (RTD)

Lead Vice-President: Works under the guidance of

- Stéphane Séjourné, Executive Vice-President for Prosperity and Industrial Strategy, and
- Henna Virkkunen, Executive Vice-President for Tech Sovereignty, Security and Democracy.

Magnus Brunner

Internal Affairs and Migration

Country: Austria

European Parliamentary Group: European People's Party (EPP)

Portfolio: Commissioner for Internal Affairs and Migration

Assigned DG: Migration and Home Affairs (Home)

Lead Vice-President: Works under the guidance of

Henna Virkkunen, Executive Vice-President for Tech Sovereignty, Security and Democracy

Glenn Micallef

Intergenerational Fairness, Youth, Culture and Sport

Country: Malta

European Parliamentary Group: Progressive Alliance of Socialists and Democrats (S&D)

Portfolio: Commissioner for Intergenerational Fairness, Youth, Culture and Sport

Assigned DG: Education, Culture, Youth and Sport

Lead Vice-President: Works under the guidance of Roxana Minzatu, Executive Vice-President People, Skills and Pre-paredness

3 Important Tasks: EU Initiatives and Legislative Projects

Ursula von der Leyen has outlined in her Political Guidelines for the next European Commission 2024-2029 and in Mission Letters addressed to each of the Commissioners-designated specific tasks assigned to them. With regard to the EU's digital policies the following are of special importance:

3.1 High standards of cybersecurity

Task
Ensure high standards of cybersecurity
Executive Vice-Presidents and Commissioners Involved
Executive Vice-President for Tech Sovereignty, Security and Democracy (lead), with the help of Commissioner for Internal Affairs and Migration
Background
Maintaining cyber security is, and will continue to be, an ongoing challenge. Forecasts suggest that cybercrime is an ever-growing threat to our societies, with global costs likely to soar in the coming years. It is therefore essential that ensuring cyber security stays high on the Commission's agenda for the new mandate. Yet, the past legislative period has already seen a considerable number of regulatory initiatives that will be transposed, implemented and/or finally adopted in the near future, such as the revised NIS 2 Directive (see cep**Adhoc**) which was adopted in December 2022, the Cyber Resilience Act (CRA, see cep**PolicyBrief**), which entered into force at the end of October 2024, or the Cyber Solidarity Act (CSA), which was provisionally agreed in March 2024. In the new mandate, the Commission should, before launching new burdensome regulatory initiatives, focus on enabling market and public actors affected by these much-needed but also challenging policies measures to cope with them. We merely consider it necessary to revise the so-called "Cybersecurity Act" (see cep**PolicyBrief** on ENISA and cep**PolicyBrief** on cybersecurity certification) in the coming year to address some of the frictions that have emerged in its practical application (see also Sections 3.7 and 3.9).

3.2 Action plan for the cybersecurity of hospitals and healthcare providers

Task
Prepare an EU action plan for the cybersecurity of hospitals and healthcare providers in the first 100 days of the new mandate
Executive Vice-Presidents and Commissioners Involved
Commissioner for Health and Animal Welfare (lead), with contributions by Executive Vice-President for Tech Sovereignty, Security and Democracy
Background
According to a Health Threat Landscape report by the European Union Agency for Cybersecurity (ENISA), the EU healthcare sector has faced an alarming number of cyber-attacks and incidents in

recent years, with healthcare providers and hospitals being the main targets. The majority of incidents have been ransomware attacks involving data breaches and data theft, which is particularly worrying given the sensitive data that healthcare providers and hospitals process and store. However, it is not only the security of (patient) data that makes cybersecurity highly relevant for these stakeholders, but also the fact that any disruption caused by cyber-attacks and incidents can have a serious impact on the health and lives of patients. With the adoption of the revised NIS-2-Directive (see cep**Adhoc**), which Member States had to transpose by mid-October 2024 – many failed to do so – a large number of healthcare actors are already required to take appropriate and proportionate technical, operational and organisational measures to manage risks related to the security of network and information systems, and to report on cybersecurity incidents. The Medical Devices Regulation (MDR) and the General Data Protection Regulation (GDPR) also already set high standards. However, the sector is often still insufficiently prepared and faces significant vulnerabilities. An action plan specific to the healthcare sector is therefore a crucial element in addressing these shortcomings. Such an action plan should include guidance and best practices on the implementation of the NIS-2-Directive, measures to overcome the use of legacy IT systems, addressing the cybersecurity knowledge and skills gap among users of digital health infrastructures, products, devices and services, and establishing clear and straightforward procedures for dealing with cyber incidents (cyber hygiene).

3.3 Use of digital technologies and AI for law enforcement

Task

Develop a strategy on the use of digital technologies, including AI, to make EU civil and criminal justice systems more efficient, resilient and secure.

Executive Vice-Presidents and Commissioners Involved

Commissioner for Democracy, Justice, and the Rule of Law, under the guidance of Executive Vice-President for Tech Sovereignty, Security and Democracy

Background

Ursula von der Leyen has entrusted Commissioner-designate Michael McGrath in her Mission Letter with developing a strategy on the use of digital technologies, including AI, to make EU civil and criminal justice systems more efficient, resilient and secure.
As Mario Draghi has pointed out in his report, digitalisation and the deployment of AI are essential to the ability of public administrations to deliver European public goods also in the field of justice. In addition, AI and other legal tech solutions have the potential to improve judicial services and shorten proceedings by enabling faster decisions and can thus contribute to reducing the costs both for the justice system and for the parties involved in the court or administrative proceedings. However, the use of AI in the field of justice imposes considerable risks for the fundamental rights and freedoms of affected persons, especially if AI systems are deployed for criminal law enforcement purposes. Therefore, the EU AI Act prohibits the use of biometric real-time remote identification systems in publicly accessible areas for criminal law enforcement purposes with narrow exceptions (Art. 5 (1) lit. a) of the EU AI Act). To the extent that it does not prohibit them, the AI Act categorises AI systems in the area of criminal law enforcement or biometrics as high-risk AI systems which are

subject to the strictest category of requirements under the AI Act. However, the Mission Letter could also refer to Legal tech applications with potential to improve the civil justice systems. These could range from proposals to support the digitalisation of the justice systems without AI elements, such as the digital filing of lawsuits in order to enhance access to justice, or the software-supported structuring of party submissions, to AI-empowered applications, such as applications to improve the handling of mass proceedings, to anonymise court decisions or to automatically categorize incoming pleadings (see also here). Such AI applications can increase the publication rate of court decisions or offer great added value in the processing of large-scale court proceedings. As far as such AI applications only entail limited risks, they will thus be categorised below the high-risk level and have to fulfil the respective provisions of the AI Act. It remains to be seen which policies or legal initiatives the Commissioner-designate will exactly propose. In any case, the Commission must assure that legal tech tools only provide support and that legal decisions are always made by a human being under full respect of the fundamental rights and the principle of the rule of law. Inter alia, the transparency of decision-making in the justice system must be maintained, and biased and false decisions avoided.

3.4 Boosting of AI innovations (AI Factories strategy)

Task

Boost AI innovation within the European Commission's first 100 days, primarily through providing start-ups access to supercomputers as part of the AI Factories strategy

Executive Vice-Presidents and Commissioners Involved

Executive Vice-President for Tech Sovereignty, Security and Democracy, under the guidance of President of the EU Commission

Background

The Commission's goal of boosting AI innovation within its first 100 days, primarily by giving start-ups access to supercomputers as part of the AI Factories strategy, is quite ambitious and certainly necessary from a geopolitical perspective. In particular, the Commission's main strategy seems to be to expand the European High-Performance Computing (EuroHPC) network to create "AI factories" for start-ups (Council Regulation (EU) 2024/1732 of 17 June 2024). But is this enough to close the AI innovation gap with the US? The EuroHPC supercomputers are primarily designed for scientific research, not for developing AI models. Adapting this infrastructure for AI purposes will take time and may result in a sub-optimal allocation of resources while still failing to meet the specific needs of AI start-ups. Furthermore, the proposed budget of €7 billion for EuroHPC (2021-2027) is already substantial, and there are calls for a significant increase. While such large public investments are probably necessary to compete in a winner-takes-all market with Big Tech firms from the US and China, they raise questions about fiscal responsibility and potential market distortions. From an ordoliberal perspective, it is also questionable whether the Commission, by providing privileged access to certain start-ups, risks engaging in de facto industrial policy, potentially distorting market competition and stifling organic innovation. More market-oriented alternatives for fostering a competitive AI ecosystem in Europe could include a greater focus on reducing bureaucratic barriers for AI start-ups, creating a more business-friendly environment for them that attracts private

investment, and creating incentives for AI researchers to stay in Europe, thus addressing the prevalent "brain drain" issue. As a recent Commission review itself notes, Europe still needs more venture capital to scale up breakthrough innovations. Overall, the Commission's goal of boosting AI innovation in the first 100 days is laudable, but the proposed approach of providing access to supercomputers through AI factories may not be the most effective or market-driven solution.

3.5 Develop an 'Apply AI' strategy for the use of AI in industry and the public sector

Task

Accelerating the adoption and implementation of AI technologies across industry and the public sector

Executive Vice-Presidents and Commissioners Involved

Executive Vice-President for Tech Sovereignty, Security and Democracy, under the guidance of President of the EU Commission

Background

While details are still scarce, the Apply AI strategy has the potential to be an important initiative for translating the EU's AI regulatory framework into practical implementation across Europe's different sectors. It is also in line with our call for practical help for European SMEs to apply large language models (LLMs) in their business models, without risking new dependencies on American Big Tech firms (cep**Input** No7/2024). To be successful, the strategy should leverage existing initiatives, support mainly SMEs and start-ups, and focus on transforming the public sector. For example, the AI Office and the GenAI4EU initiative could play a crucial role in implementing the Apply AI strategy. Particular attention should be paid to the public sector and internal EU processes, where AI can improve citizen-government interactions, enhance analytical capabilities, and increase efficiency (cep**Input** special, 7 May 2024). Key challenges include updating complex procurement processes, managing data effectively, and developing AI skills across the European workforce. The strategy also needs to foster cross-border collaboration, increase funding for industry-relevant AI deployments, and establish a robust monitoring framework. By comprehensively addressing these aspects, the envisioned Apply AI strategy could indeed help boost the EU's competitiveness and efficiency in both industry and public services.

3.6 Establish an EU AI Research Council

Task

Establish an EU AI Research Council for coordinating and advancing AI research across Europe

Executive Vice-Presidents and Commissioners Involved

Commissioner for Startups, Research and Innovation, under the guidance of Executive Vice-President for Tech Sovereignty, Security and Democracy

Background

The establishment of an EU AI Research Council is a strategic initiative that, by centralising and coordinating research efforts across the EU, could increase resource efficiency, foster synergies, and focus public and industry attention on key areas in line with European interests and values. Whether it will be sufficient to bridge the gap between academia and industry, promote ethical AI development in Europe, and improve talent retention remains to be seen and depends on concrete implementation. As recent data show, Europe is still far from reaching the target of 3% of EU GDP invested in R&D, as private investment is hampered by regulatory, legal, and administrative barriers that need to be addressed to attract more investors and innovators. If the EU AI Research Council is given a prominent role in funding promising state-of-the-art research projects in Europe and facilitating international collaboration, it could make a significant contribution to the EU's global competitiveness in AI. However, its success will depend on effective governance, adequate funding, and the ability to handle diverse national and institutional interests within the EU, as Member States have their own strategic interests in attracting AI companies and talent, and there are many competing AI-related public institutions in the pipeline.

3.7 EU Cloud and AI Development Act

Task

Develop a proposal for an EU Cloud and AI Development Act to increase computational capacity as presented in the Draghi report. Furthermore, create an EU-wide framework for providing "computational capital" to innovative SMEs.

Executive Vice-Presidents and Commissioners Involved

Executive Vice-President for Tech Sovereignty, Security and Democracy, under the guidance of President of the EU Commission

Background

The task of developing an EU Cloud and AI Development Act seems to be mainly based on the ideas presented in Mario Draghi's recently published report. According to the report, such an act should pursue three main objectives. Firstly, the Act shall seek to improve European capabilities and infrastructure in the fields of high-performance computing (HPC), AI and quantum. This would include a so-called "Euro-HPC upgrade programme", consisting of, among other things, regularly increasing the computing capacity dedicated to training and algorithmic development of AI models in existing EU HPC centres, funding an extension of Euro-HPC to additional cloud and storage capabilities, and creating an EU-wide framework allowing public institutions to provide "computing capital" to innovative SMEs in the EU in exchange for a financial return. Secondly, it will harmonise requirements for cloud architectures and cloud procurement processes (more on this specific point in section 3.8). And thirdly, it will play a role in coordinating priority initiatives to increase private participation and funding. While it is too early to fully assess these early and still vague proposals, it is essential for the EU to make renewed efforts to avoid losing further or even all ground in the cloud and AI sectors, which are crucial for the EU's future competitiveness. While it will not be easy to regain such ground in cloud computing, as the US hyperscalers are far ahead, network and lock-in effects as

well as economies of scale play a crucial role, it must be in Europe's interest not to become totally dependent on non-European providers.

3.8 EU cloud policy for public administrations and public procurement

Task

Develop a single EU-wide cloud policy for public administrations and public procurement

Executive Vice-Presidents and Commissioners Involved

Executive Vice-President for Tech Sovereignty, Security and Democracy, under the guidance of President of the EU Commission

Background

As part of the EU Cloud and AI Development Act, the Commission also wants Commissioner-designate Virkkunen to develop an EU-wide cloud policy for public administrations and public procurement. Again, the idea seems to build on the groundwork laid by the Draghi report. In particular, Draghi recommended harmonising public procurement of cloud services across Member States and standardising public tenders for cloud services. Such harmonisation of public procurement rules for cloud services could go hand in hand with a revision of the current Public Procurement Directive and the desire to allow "preference" for European products, services and suppliers in public procurement in strategic sectors and to modernise and simplify public procurement rules. Beyond this, such EU-wide cloud policy may, as stipulated by Draghi, include the development of homogeneous and mandatory data residency requirements and possibly other "sovereignty criteria" for public administrations' use of cloud services. These requirements and criteria could, inter alia, specify that when public administrations store and process certain sets of highly sensible data, the data should be kept within specific geographic locations, most likely within the EU. Only recently, the introduction of such sovereignty requirements has already been the subject of intense debate in the context of the establishment of an EU Cybersecurity Certification Scheme for Cloud Services (EUCS) (see also section 3.9). However, we believe that adapting public procurement rules to promote European cloud products, services and suppliers, including by introducing sovereignty requirements, is a double-edged sword. While such revised rules may be an option in particularly sensitive areas where vital interests of governments, public authorities and bodies are at stake, it should not be a general blueprint. A blanket preference for EU products, services and suppliers in procurement would inevitably lead to higher costs, less competition, restricted access to innovation and, ultimately, a less "competitive" European public sector. It may also provoke unwanted retaliatory measures by non-EU governments. In a forthcoming cep**Input** we will look at this important topic in much more detail.

3.9 Improve the adoption process of cybersecurity certification schemes

Task

Contribute to strengthening cybersecurity by improving the adoption process of European cybersecurity certification schemes

Executive Vice-Presidents and Commissioners Involved

Executive Vice-President for Tech Sovereignty, Security and Democracy, under the guidance of President of the EU Commission

Background

The EU Cybersecurity Act (see cep**PolicyBrief**) entered into force in April 2019. In addition to defining the tasks and organisational structure of the European Union Agency for Cybersecurity (ENISA), the Act also establishes a framework for certifying the cybersecurity of ICT products, services and processes at EU level. Since the regulation came into force, the EU Commission has only managed to implement one scheme, the European Cybersecurity Certification Scheme on Common Criteria (EUCC), in January 2024. Another very important scheme, the draft European Certification Scheme for Cloud Services (EUCS), has, however, been significantly delayed. The first draft was published by ENISA back in December 2020, but the scheme has still not been adopted. This is mainly due to an ongoing, highly politicised discussion on whether the EUCS should include so-called sovereignty requirements, including rules for cloud providers to store and process data only within the EU and prescribing the primacy of EU law and the need for cloud providers to be based in the EU. Regardless of whether such sovereignty requirements are reasonable, this delay highlights a significant shortcoming in the adoption process of European cybersecurity certification schemes.

The upcoming revision of the EU Cybersecurity Act, which is scheduled for 2025 – the EU Commission has already launched a consultation – provides a good opportunity to tackle this issue. In particular, we see three aspects that need to be addressed. First, politically contentious issues such as sovereignty requirements should no longer be decided in an implementing act approved by the Commission at Level 2, but directly by the EU legislator, i.e. the European Parliament and the Council, at Level 1. Second, there should be a greater degree of transparency for stakeholders, but also for the wider public, on the process of establishing new draft schemes, including the publication of each new iteration of a draft scheme. This should allow interested parties to comment on and challenge any new or adapted requirements, including those that are considered non-technical. And third, the legislator should set clear deadlines for the implementation of any new scheme. Already at the end of 2019, the Commission mandated ENISA to develop the Cybersecurity Certification Scheme for Cloud Services (EUCS), and after almost five years, the scheme has still not been adopted. This is inefficient, does not provide legal certainty and does not allow market participants to plan ahead. In a forthcoming cep**Input**, the cep will take a closer look at the highly controversial draft EUCS and provide further ideas and suggestions for a future policy approach.

3.10 Develop a long-term EU Quantum Chips Plan

Task

Develop a long-term EU Quantum Chips Plan, as suggested by Mario Draghi in his report on EU competitiveness.

Executive Vice-Presidents and Commissioners Involved

Executive Vice-President for Tech Sovereignty, Security and Democracy, under the guidance of President of the EU Commission

Background

The EU's long-term plan for quantum chips should take a market-driven approach, balancing strategic public investment with a focus on creating an environment conducive to private sector innovation and competition. This is in line with recent calls to create the "quantum equivalent to Silicon Valley" – or the world's first "quantum valley" in Europe. While the €65 million investment through the Chips Joint Undertaking (Chips JU) announced this year is a positive step, a more comprehensive strategy is needed. This approach should include regulatory sandboxes to allow flexible testing of new technologies and targeted tax incentives for R&D and capital investment. At the same time, the EU must invest in research and talent development, e.g. through university-industry partnerships. Infrastructure development should focus on upgrading digital infrastructure to support the deployment of quantum technologies, including quantum-safe cryptography, supply chain resilience for critical quantum chip components to reduce dependencies on external suppliers, and targeted support for quantum start-ups. By creating this enabling environment and by strengthening quantum cooperation with the US through a revamped Trade and Technology Council (TTC), the EU could kick-start a sustainable and competitive quantum chip ecosystem.

3.11 Work on a Digital Networks Act

Task

Work on a new Digital Networks Act (DNA) to help to boost secure high-speed fixed and wireless broadband and to incentivise and encourage investments in digital infrastructure

Executive Vice-Presidents and Commissioners Involved

Executive Vice-President for Tech Sovereignty, Security and Democracy, under the guidance of President of the EU Commission

Background

In February 2024, the EU Commission published a White Paper on a future "Digital Networks Act (DNA)"(see cep**PolicyBrief**) and initiated an in-depth debate on the future of the connectivity sector and connectivity infrastructures. The White Paper also reflected on the review of the both the European Electronic Communications Code (EECC) and the Recommendation on relevant markets within the electronic communications sector, which are due to be revised and updated in 2025. While the White Paper addressed many issues, including the contentious question of whether there is a need to encourage further consolidation in the telecoms sector, whether non-telecoms digital

companies should be forced to contribute more to the financing of digital network infrastructure ("fair share debate"), or whether cloud providers should be included in the EU's telecoms framework (EECC), we will only highlight and analyse some specific proposals.

Firstly, the Commission should refrain from extending the list of objectives of the EECC. Adding (a) sustainability, (b) industrial competitiveness and (c) economic security to the existing list, which already includes the promotion of network roll-out, effective competition and the interests of end-users, risks interfering in market processes for purely industrial policy reasons and could encourage the emergence of further trade-offs and unnecessarily delay decision-making processes.

Secondly, the Commission's attempt to achieve greater harmonisation of European spectrum policy and the transfer of competence to the EU level in this area may lead to more efficient spectrum use, greater planning certainty and a greater willingness to invest, especially among cross-border network operators. However, a shift to the EU level is not a panacea, as the starting positions of Member States are quite different, and the telecom markets are still characterised by a large number of national specificities.

Thirdly, the Commission's intention to phase out sector-specific ex-ante regulation of access to telecommunications networks, which is dependent on market power, and to switch to a system of ex-post control by means of competition law is generally to be supported and should be examined in more detail in the near future. The time to take the plunge and switch to ex-post control is when there are no longer any monopolistic bottlenecks in the telecommunications markets. We call for greater regionalisation of access regulation, as this would allow more targeted regulation of any remaining monopolistic bottlenecks, but we are cautious about any ex-ante regulation independent of market power.

And fourthly, we reject the Commission's intention to force a complete switch-off of copper networks and migration to fibre networks by 2030, as this has the hallmarks of a planned economy. It interferes with the entrepreneurial freedom of the market players concerned simply to achieve certain questionable political objectives.

3.12 Deploy digital public infrastructure, making use of the EU wallet

Task

Deploy digital public infrastructure to ensure businesses can speed up and simplify operations and reduce administrative costs. For this, make the most of the EU wallet

Executive Vice-Presidents and Commissioners Involved

Executive Vice-President for Tech Sovereignty, Security and Democracy, under the guidance of President of the EU Commission

Background

In May 2024, the Regulation on the establishment of a European Digital Identity Framework came into force (see cep**PolicyBrief**). A cornerstone of the Regulation is the establishment of harmonised conditions for the creation of a framework for so-called European Digital Identity Wallets (EDIW). Under the Regulation, each Member State will be required to make at least one such wallet available to its citizens and businesses within two years of the entry into force of implementing acts, to be adopted by the Commission by November 2024, laying down the technical specifications and

procedures for such wallets. Thus, by the end of 2026, any Member State must make such wallet available. The aim is to make it easier for users of such wallets to identify themselves electronically across borders in a secure and data-protection-friendly manner. In addition, relying parties should be given access to personal identification data and attestations of attributes of the users. In fact, EDIW have the potential to strengthen the internal market also in the public sector by facilitating and accelerating the interaction between, on the one hand, citizens and businesses, and, on the other public bodies and authorities. To unlock this potential, it is now time for the Commission to adopt the necessary implementing acts, on which it has already published drafts and consultations in August 2024 (see here, here, here, here and here). Next, both the Commission and ENISA should make rapid progress on the certification of EDIW and the development of a candidate European cybersecurity certification scheme, as foreseen in the Regulation. The fact that the Commission and ENISA have already started the process is good news (see here). After all, it is the Member States efforts, at a federal, regional and local level, that will decide upon the success of any EDIW to be developed. Ultimately, EDIW will only fly for businesses and citizens alike when federal, regional and local governments manage to provide by 2026 a plethora of digital government services that can be accessed by using any EDIW.

3.13 Present Data Union Strategy

Task

Present an EU Data Union Strategy:
- Draw on existing data rules,
- Ensure a simplified, clear and coherent legal framework for data sharing by businesses and administrations,
- Respect high privacy and security standards

Executive Vice-Presidents and Commissioners Involved

Executive Vice-President for Tech Sovereignty, Security and Democracy, under the guidance of President of the EU Commission

Background

The EU's 2020 strategy for Data has resulted in numerous legal Acts which aim to widely encourage data sharing, such as the Data Governance Act, the Data Act and the yet to be adopted European Health Data Space. Beyond this, sector-specific laws and the competition-related Digital Markets Act contain provisions on data access and portability. The AI Act regulates AI systems, which are trained with data. Finally, the EU has also adopted various rules to enhance cybersecurity including the revised NIS-2-Directive and the Cyber Resilience Act. Whenever personal data is involved, the sharing and other processing of such data must also be in line with the General Data Protection Regulation (GDPR), which remains unchanged by the other acts. Those complex acts often overlap in a non-transparent way or contain inconsistencies or very similar obligations. This complicates both their application and the delineation of the competent authorities' powers. It is key that Virkkunen – in line with Draghi's call (p. 307/311/317/323) for a consolidation and streamlining of the existing EU acquis – now takes responsibility to make the complex digital legislative landscape more business-friendly and increase legal certainty in order to enhance competitiveness of EU companies

and facilitate innovation. In doing so, Virkkunen must cooperate with Dombrovskis, who (p. 7) is responsible for the consolidation of the EU legal framework in general. To turn the complex EU digital laws into a simplified, understandable, predictable and coherent legal framework, the new EU Data Union Strategy should, in our view, comprise the following four sets of measures:

(1) Consolidate and simplify all data-related EU legal acts. Identify and address overlaps. Eliminate legal ambiguities, inconsistencies and contradictions and possible duplicate burdens.

(2) Better align the Data Act and the AI Act with the GDPR, in cooperation with Commissioner-designate Michael McGrath who (p. 7) is tasked with enforcing the GDPR and ensuring that it "remains in line with the digital transformation and enforcement of commercial needs". Data protection concerns are among the most frequently cited obstacles to data sharing between business partners (see cep**Study**). Take "appropriate actions" to provide legal certainty, as announced in the Commission's Second Report on the application of the GDPR (p. 29). In particular, propose measures to

(a) resolve the conflict between the GDPR's principle of data minimisation and the practical need to lawfully use large data sets, which is key for the emergence of data-driven business models and the adequate training of high-quality AI;
(b) clarify when data is considered anonymised and therefore not subject to the GDPR; this could be done by supporting the development of uniform and practicable standards, compliance with which is presumed to ensure a sufficient degree of anonymisation, and clarifying liability issues in case of a potential subsequent re-identification;
(c) support companies in using synthetic data and other data protection-friendly technologies;
(d) support an innovation-friendly application and interpretation of the GDPR, without disproportionately restricting the fundamental right to data protection,
(e) propose punctual legislative amendments of or clarifications in the GDPR, where legal uncertainties cannot be eliminated by guidelines and a swift clarification by the ECJ is also not to be expected.

(3) Give a better overview over the law and more guidance to further support companies in complying with the digital acquis. Bring together all EU legal acts with data-related provisions in a "European Data Law Rulebook", including a summary and explanation of their purpose, their content and their interplay with each other and with the GDPR. Explain similarities and unavoidable overlaps between the legal acts and help companies and authorities to utilise synergies to fulfil similar risk management measures, information duties, incident reporting or portability obligations. Supplement the proposed rulebook with existing and new EU-wide guidelines and interpretation aids.

(4) Arrange training programmes to help companies and authorities better understand the single EU digital laws and their interplay. As requested by Draghi (p. 322), "promote innovation" and inform companies about the economic benefits and potential risks and of sharing and using data sets.

It is still unclear which concrete measures the Commission will propose: In any case, such measures must strike the right balance between innovation, individual rights and commercial interests.

3.14 Investigate influence of social media

Task

Contribute to the EU-wide enquiry on the impacts of social media.

Executive Vice-Presidents and Commissioners Involved

Commissioner for Intergenerational Fairness, Youth, Culture and Sport with the Executive Vice-President for Tech Sovereignty, Security and Democracy

Background

Around four billion people worldwide use social media. On average, they spend two hours and twenty-three minutes a day on social media platforms. It is feared that there may be negative consequences for the mental health of users and for school, academic and professional performance. Calls for stricter regulation, aimed at counteracting intensive use and its potentially negative consequences, are therefore becoming louder.
There are numerous studies investigating the effects of social media on the mental health of users, the results of which are inconsistent. The majority of studies conclude that only in a small number of cases does the use of social media have a negative impact on users' mental health. However, intensive use of social media often leads to poorer school, academic and professional performance. Furthermore, it is It is worrying that around a third of social media users would like to spend less time on social media but find it difficult to achieve this. One reason for this is that social media platforms are designed to ensure that users return to a platform as often as possible and then stay on it for as long as possible. To solve these problems, we recommend strengthening users' media literacy, for example by displaying warning messages when installing, opening or intensively using social media. In addition, certain design elements should be restricted. Thus, push notifications, endless scrolling & streaming and read receipts should be deactivated by default and automatic requests to activate these design elements should be prohibited. Finally, a ban on addictive algorithms should be assessed (see cep**Input**).

3.15 Help to combat unethical online techniques under a digital fairness act

Task

Combat unethical techniques online, such as dark patterns

Executive Vice-Presidents and Commissioners Involved

Commissioner for Democracy, Justice, and the Rule of Law (lead), with a contribution from the Commissioner for Intergenerational Fairness, Youth, Culture and Sport and a contribution from the Executive Vice-President for Tech Sovereignty, Security and Democracy

Background

Dark patterns are unfair commercial practices deployed through the structure, design or functionalities of digital interfaces or system architecture that can influence consumers to take decisions they would not have taken otherwise. Dark patterns include, among other things, presenting

choices in a non-neutral manner, using emotional manipulation, phrasing questions using double negatives or misleading consent options in cookie banners.

The aim of dark patterns is to keep users on the website or app for as long as possible in order to

- collect as much user data as possible,
- make users spend as much money as possible, or
- maximise user participation in content creation, network development and data sharing.

Dark patterns are frequently used on the internet. A Commission's study showed that 97% of the most popular websites and apps used by EU consumers deployed at least one dark pattern. Therefore, the political discussion is focusing on the need for stricter regulations to limit such manipulative techniques, particularly to protect minors and vulnerable groups. On October 3, the EU Commission published a fitness check of EU consumer law on digital fairness. The report also includes a comprehensive analysis of dark patterns.

Centres for European Policy Network
FREIBURG | BERLIN | PARIS | ROMA

Authors:

Philipp Eckhardt
Head of the Department on Information Technologies
eckhardt@cep.eu

Dr. Matthias Kullas
Head of Division Single Market & Competition Policy
kullas@cep.eu

Dr. Anja Hoffmann, LL.M. Eur.
Policy Analyst
Single Market and Competition Policy | Digital Economy
hoffmann@cep.eu

Dr. Anselm Küsters, LL.M. Eur.
Head of Division Digitalisation and New Technologies
kuesters@cep.eu

Centrum für Europäische Politik FREIBURG | BERLIN
Kaiser-Joseph-Straße 266 | D-79098 Freiburg
Schiffbauerdamm 40 Räume 4205/06 | D-10117 Berlin
Tel. + 49 761 38693-0

Centre de Politique Européenne PARIS
17, rue Saint Fiacre | F-75002 Paris
Tel. + 33 1 45 54 91 55

Centro Politiche Europee ROMA
Via G. Vico, 1 | I-00196 Roma
Tel. +390684388433

The **Centrum für Europäische Politik** FREIBURG | BERLIN, the **Centre de Politique Européenne** PARIS, and the **Centro Politiche Europee** ROMA form the **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA.

Free of vested interests and party-politically neutral, the Centres for European Policy Network provides analysis and evaluation of European Union policy, aimed at supporting European integration and upholding the principles of a free-market economic system.