BRIEFING

EPRS Ideas Paper
Towards a more resilient EU

European Parliament

Digital sovereignty for Europe

SUMMARY

There is growing concern that the citizens, businesses and Member States of the European Union (EU) are gradually losing control over their data, over their capacity for innovation, and over their ability to shape and enforce legislation in the digital environment. Against this background, support has been growing for a new policy approach designed to enhance Europe's strategic autonomy in the digital field. This would require the Union to update and adapt a number of its current legal, regulatory and financial instruments, and to promote more actively European values and principles in areas such as data protection, cybersecurity and ethically designed artificial intelligence (AI). This paper explains the context of the emerging quest for 'digital sovereignty', which the coronavirus pandemic now seems to have accelerated, and provides an overview of the measures currently being discussed and/or proposed to enhance European autonomy in the digital field.

Context

The notion of 'technological' or 'digital sovereignty' has recently emerged as a means of promoting the notion of European leadership and strategic autonomy in the digital field. Strong concerns have been raised over the economic and social influence of non-EU technology companies, which threatens EU citizens' control over their personal data, and constrains both the growth of EU high-technology companies and the ability of national and EU rule-makers to enforce their laws.[1] In this context, 'digital sovereignty' refers to **Europe's ability to act independently in the digital world**[2] and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies).

In this context, Ursula von der Leyen, President of the European Commission, has identified digital policy as one of the key political priorities of her 2019-2024 term in office and pledged that Europe must achieve 'technological sovereignty' in critical areas. A recent Commission report highlighted that competition from global tech-driven players which do not always obey European rules and fundamental values, and which put data appropriation and valuation at the heart of their strategy, constitutes a major policy challenge for Europe. The European Parliament has expressed deep concern about the security threats connected with growing Chinese technological presence in the EU and has called for possible action at EU level to reduce such dependence. The European Council has stressed that the EU needs to go further in developing a competitive, secure, inclusive and ethical digital economy with world-class connectivity, and has called for special emphasis to be placed on data security and on artificial intelligence (AI) issues.

In parallel, the coronavirus pandemic which hit the EU in spring 2020 showed the essential role played by the high-tech sector in ensuring the continuity of social life, businesses and administrations and has accelerated the reflection on the need for sovereign digital technologies. In its roadmap for recovery, the European Council called for action to ensure the strategic autonomy of the EU in a post-pandemic context and stressed that investing in digital capacities, infrastructure and technologies will be a key element of the recovery effort.

Author: Tambiama Madiega

PE 651.992 - July 2020

EN

Digital sovereignty: State of play

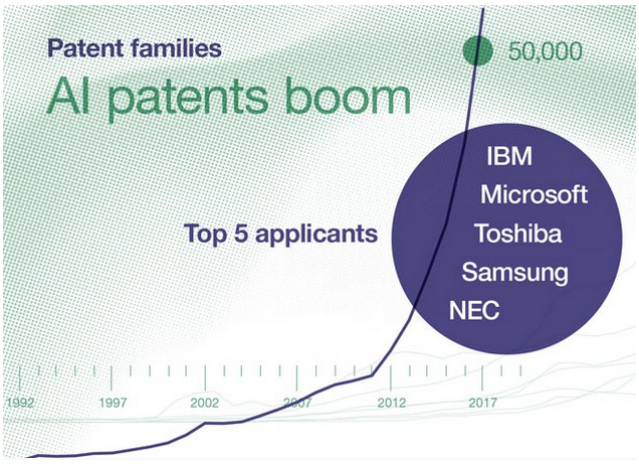
The influence of non-EU tech companies has become a concern for EU policy-makers, especially with regard to their impact on the EU's data economy and innovation potential, on EU privacy and data protection and on the establishment of a secure and safe digital environment.

EU data economy and innovation

Concerns

In the last decade, a range of innovations such as 5G, artificial intelligence (AI), cloud computing and the internet of things (IoT) have become major strategic assets for the EU economy. With a worldwide market for new digital technologies expected to reach €2.2 trillion by 2025, a large part of Europe's growth potential resides in digital markets.[3]

Figure 1 – Boom in AI patents



Source: WIPO Technology Trends Report 2019.

While, the EU has strong assets, including a world-leading AI research community and a strong industry, some indicators show that the EU also exhibits some weaknesses that are detrimental in the global race to develop such new technologies. In the area of AI, for instance, the EU is lagging behind the United States (US) and China in private investment[4] and the level of adoption of AI technologies by companies and by the general public is comparatively low compared to the US.[5] The US also attracts more AI talent and researchers and is the world leader in patent applications, while China leads the race on data collection and data access (i.e. the raw material for most AI technologies) and has made significant progress in developing new hardware equipment such as supercomputers.[6] Furthermore, the US and China are leading in regards patents on quantum-computing technologies, while Europe's level of investment in blockchain technologies and IoT is comparatively low.[7]

Against this background, EU policy-makers have identified a potential dependence on foreign technology as presenting a risk to Europe's influence.[8] The coronavirus crisis further highlights this risk, as telecommunications and big data analysis techniques are increasingly used for tracking and controlling the spread of the disease, and AI and high performance computing are expected to come into play for developing strategies for testing and finding vaccines. The crisis also reveals Europe's urgent need to foster digitalisation in a variety of sectors, ranging from health to retail and from manufacturing to education.

Main EU actions so far

The EU has put several instruments in place to **narrow the investment gap**. Horizon 2020, the EU research and innovation programme with nearly €80 billion of public funding to disperse over seven years (2014 to 2020) makes such funding available for research on key digital technologies such as nano-electronics, photonics, robotics, 5G, high-performance computing, big data, cloud computing, and AI. Other instruments, such as the 5G-PPP, a new Artificial Intelligence and Blockchain Investment Fund, and a large-scale research initiative to foster the development of a competitive quantum industry in Europe, support companies working in the AI and blockchain sectors.

In parallel, EU policy-makers are designing measures to **adapt EU industrial and technological capacity** to the competitive environment. The European data strategy adopted in February 2020 lays down a path towards the creation of European data spaces to ensure that more data becomes available for use in the economy and society, while keeping companies and individuals in control of their data. Furthermore, the EU has adopted an approach for developing AI technologies that adhere to high ethical standards with the aim of becoming a global leader in responsible and trustworthy AI and providing European developers and manufacturers with a competitive advantage (i.e. with consumers and users ultimately favouring EU-compliant products) to catch up with the US or China in the race to develop AI.[9] Furthermore, additional reflection is currently under way to address the opportunities and challenges of AI for the EU in the context of global competition.

Privacy and data protection

Concerns

Technology companies are collecting massive amounts of personal data and the economic model used by Google, Apple, Facebook, Amazon and Microsoft – sometimes referred to as the 'GAFAM' – is largely based on the collection and exploitation of online users' data to generate advertising revenue.[10] The Cambridge Analytica scandal illustrated how online platforms are also able to extract personal data for political profiling purposes. These trends, often referred to as surveillance capitalism, ultimately result in European citizens gradually losing control over their personal information and privacy.

Concern has grown in the EU as to how European citizens can **recover control of their digital data** (or 'trace') in an online environment that is now largely dominated by non-EU tech companies. A recent example is the controversy concerning the development of contact-tracing solutions for controlling the spread of coronavirus. The technological choices made by Apple and Google have frustrated the ability of some Member States to design their own contact-tracing solutions (such as 'Stop Covid' in France) and fuelled the quest for digital sovereignty.[11] In a post-coronavirus pandemic world, where technology will no doubt play a more crucial role, the challenge remains for EU policy-makers to find the right balance between control and privacy rights while, as stated by Commission Vice-President Margrethe Vestager, EU citizens want to trust technology when they use it and not begin a new era of surveillance.

Main EU actions so far

The EU has adopted a very stringent framework for privacy and data protection, with the General Data Protection Regulation (GDPR) at its centre, and has introduced a protective 'right to be forgotten' and a data portability right to enhance individuals' control of their own data. Furthermore, the Commission has set out a strategy on promoting international data protection standards. The EU is seen as a **standard-setter in privacy and data protection**, with various countries having incorporated GDPR provisions into their national legislation and some multinationals having opted to adopt GDPR as their global standard of operation.[12]

However, the coronavirus crisis comes as a real test for the EU framework, while EU Member States are looking at adopting location-tracking measures to contain the spread of the virus. The EU institutions have been instrumental in fostering the development and use of technical solutions that abide by the stringent EU privacy standard, such as the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) system. The EU has also used a soft law approach to ask telecom firms to hand over anonymised mobile metadata (to help analyse patterns of coronavirus contagion), and adopt guidelines and a toolbox for developing coronavirus-related apps that provide sufficient data protection and limit intrusiveness. The EU will also scrutinise contact-tracing technology proposed by Google and Apple, to ensure it meets the bloc's new standards.

Cybersecurity, data control and online platforms' behaviour

Concerns

In the field of **cybersecurity**, reliance on Chinese 5G infrastructure has been identified as a critical weakness for the EU and the risk that the absence of a unified European cyberspace opens the door to foreign influence has been stressed.[13] EU Member States have issued a report warning against over-dependence on one equipment supplier, which increases exposure to potential supply interruption and creates a security risk. Furthermore, cyber-criminals are taking advantage of the coronavirus pandemic, with a dramatic increase in the number of cyber-attacks.

Another growing concern for EU Member States is their **lack of control over data** produced on their territory. The global public cloud market is currently largely dominated by US and Asian companies,[14] and European governments and industry players in Europe have become concerned about using non-European data services, given the expansive extra-territorial ability granted to US law enforcement agencies to obtain foreigners' personal data under the 2018 US CLOUD Act. European governments have started to move away from cloud solutions offered by non-EU companies and to instead deploy European-designed cloud solutions.

Experts warn that the GAFAM's control over data can make it hard for others to compete in new and innovative markets. Because the high-tech economy is increasingly based on intangible assets (i.e. data and intellectual property rights), non-EU companies could quickly develop critical infrastructure (such as data centres) and enter new industry sectors, as Google is doing by moving from search engine optimisation to robotics, as well as Amazon in moving from online markets to cloud computing to healthcare.[15] The EU's data dependency is arguably becoming even more of a concern due to the coronavirus pandemic, as reliance on data analysis tools - possibly developed outside the EU - may prove necessary for screening the population and assessing infection risks, optimising clinical trials for treatments and finding potential vaccines.[16]

Furthermore, large **online platforms** (mostly non-EU based) are increasingly seen as dominating entire sectors of the EU economy and depriving EU Member States of their sovereignty in areas such as copyright, data protection, taxation or transportation. This concern has extended to other areas such as e-commerce and online disinformation where the EU framework falls short of addressing the influence of foreign high tech companies.

Main EU actions so far

A range of new EU instruments were adopted during the 2014-2019 legislative term to address cyber-attacks. The 2016 Network and Information Security Directive (NIS) improves Member States' cybersecurity capabilities and cooperation and imposes measures on companies to prevent and report security incidents and cyber-attacks in key sectors (i.e. energy, transport, banking, financial market infrastructures, the health sector, drinking water supply and distribution and digital infrastructure). The European Cybersecurity Act approved in 2018 creates a (non-mandatory) EU-wide cybersecurity certification scheme for ICT products to ensure consumers and businesses are protected from cybersecurity threats. As a result, the EU has begun to establish itself as a **standard-setter in the field of cybersecurity** as non-EU countries as well as private companies doing business - or with subsidiaries - in the EU have updated their cybersecurity practices and policies to ensure compliance with these new and expanding legal requirements.[17]

Furthermore, in the aftermath of the Huawei debate, the Commission adopted a recommendation for a **common EU approach to the security of 5G networks** in March 2019 and published an EU toolbox on 5G cybersecurity in January 2020. The extent to which EU Member States succeed in developing a common approach to the 5G security question is seen as an important test for the strategic autonomy of the EU in the digital environment.

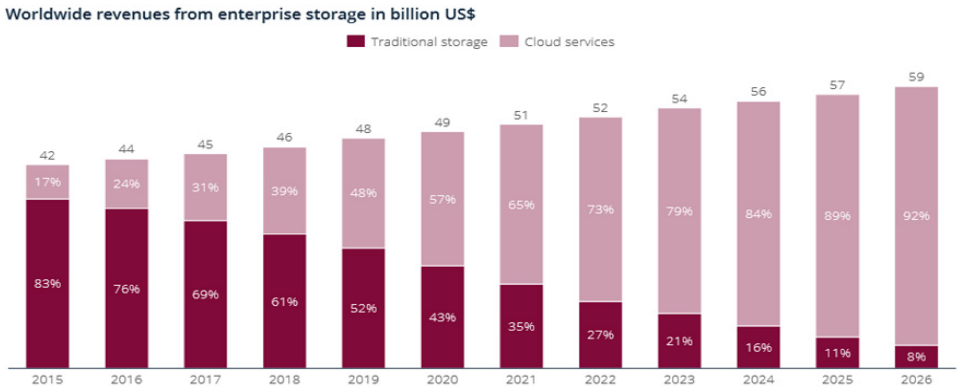
EU digital sovereignty: Towards further EU initiatives

Reliable digital infrastructure and services are critical in today's society, as the coronavirus crisis has highlighted. A range of initiatives have been proposed or are already under discussion at EU level to accelerate the digitalisation process and enhance Europe's strategic autonomy in the digital field around three building blocks of (i) building a data framework; (ii) promoting a trustworthy environment, and (iii) adapting competition and regulatory rules.

Data framework

Control over non-personal data – the raw material of the digital economy – is critical. The EU can profit from its large industry data resources. To that end, building a secure pan-European data framework and fostering investments in frontier technologies is paramount.

Figure 2 – Worldwide revenues from business data storage



Source: Digital Economy Compass, 2019.

Cloud storage is expected to overtake device storage (i.e. local storage in computers and devices) and become the primary data storage solution worldwide in 2020. There are calls to **build a European cloud and data infrastructure** to strengthen Europe's data sovereignty and address the fact that today, the cloud and data storage market is almost exclusively dominated by non-European suppliers – with potentially detrimental implications for security and EU citizens' rights. The European cloud initiative Gaia-X project was announced jointly by Germany and France and proposes to establish, as of 2020, a federated data infrastructure at European level. This would be an important tool in ensuring a secure environment for the data of citizens, businesses and governments. In line with the European data strategy, further actions could be tabled at EU level to foster the implementation of an EU-wide cloud infrastructure (e.g. establishment of common cloud standards, a reference architecture and the interoperability requirements).

Europe has great potential to lead the race in collecting and processing data, which is the engine of the new data economy. It is proposed to achieve this by building an **EU data framework to facilitate data collection, data processing and data sharing** to secure access for innovators to data, especially in the business-to-business (B2B) or government-to-citizens (G2C) domains. In line with the European data strategy, granting open access to government data in certain strategic sectors, such as transportation or in healthcare,[18] allowing companies to have access to privacy-preserving data marketplaces and incentivising the sharing of data[19] would be critical to building an EU data space. Furthermore, reflecting on solutions to fostering public data collection at infra-national level would be useful. An interesting example is provided by the experiment conducted by the city hall of Barcelona, which included 'data sovereignty' clauses in public procurement contracts requesting its partners give back the data they gather to deliver services to the city in machine-readable format. Should such clauses prove useful, best practices could be identified at EU level.

Furthermore, **investment in frontier technologies**, including artificial intelligence, IoT, blockchain, high-performance computing and quantum technologies should be encouraged and supported to deliver the breakthrough in productivity that Europe needs. In that respect, the conclusion of the 2021-2027 multiannual financial framework (MFF) currently under consideration is critical, with its proposed €100 billion budget for the next Horizon Europe research programme. In addition, the Digital Europe programme, the first ever EU programme dedicated solely to the digital transformation, with a planned overall budget of €9.2 billion, will be instrumental in reaching the objective of attracting over €20 billion per year of total investment in the EU in AI systems, as proposed under the coordinated plan on artificial intelligence. Furthermore, setting up Public Private Partnerships (PPP) in AI, data and robotics to develop an AI innovation ecosystem in Europe based on EU values could be fostered in line with the white paper on AI. In addition, the scientific community strongly advocates the creation of a large-scale EU research cooperation framework in the field of new technologies aiming for the EU to keep pace with Chinese and North American research capabilities.[20]

Trustworthy environment

Seeking to ensure **transparency** and **trust** has become the hallmark of the EU approach to digital matters. The challenge for the Union is to further foster new standards and practices that ensure that products and services are trustworthy and controllable - even where they are of foreign origin[21] - in line with EU values and principles. This approach will require development of a set of new instruments in the fields of cybersecurity, AI and data protection.

There is a need to act in the **cybersecurity field** at least in three domains:

- First, the EU framework for cybersecurity certification scheme that provides a harmonised set of rules to ensure consumers and businesses are protected in the EU is up for review by 2023. Establishing a compulsory **EU-wide certification scheme** (and not a merely voluntary one as is the case today) would be a step forward in ensuring a truly safe environment, especially for 5G networks[22] and could foster the establishment of the EU as a standard-setter in the field of cybersecurity, while several countries have enhanced their cybersecurity legislation in recent years with specific references to the NIS Directive and relevant EU regulations. In this context, the **definition of common security standards** would be a major step forward in fostering Europe's technological know-how and industrial leadership in 5G networks and towards smart connectivity systems, in line with the current 5G Public Private Partnership. Furthermore, the EU could work towards setting **global norms in the IoT field**, for which standards are still largely absent (there is, in fact, no standard for implementing cybersecurity in smart devices).
- Second, insufficient **coordination in matters of cybersecurity** has been identified as one of the main issues EU policy-makers must tackle. While the creation of a new Joint Cybersecurity Unit to ensure reinforced cooperation between the Member States has already been announced, a report from the EU Court of Auditors stresses that more EU action is needed to address inconsistent transposition or gaps in EU law (e.g. limited and diverse legal frameworks for duties of care; the EU's company law directives have no specific requirements on the disclosure of cyber risks). An important step would also be to finalise the adoption of the Commission proposal to establish European Cybersecurity Competence Centres.
- Third, the cybersecurity threat has prompted a reflection on **procurement conditions** in the EU. A 2019 EP resolution calls for security to become an obligatory aspect in all public procurement procedures for relevant infrastructure at both EU and national levels. Member States should develop specific security requirements that could apply in the context of public procurement related to 5G networks, including mandatory requirements as regards cybersecurity certification. More generally, the revamping of the EU's public procurement

rules and grant provisions to take better account of the critical aspects of digital technologies in sensitive sectors could be assessed. That would mean giving sufficient weight to security considerations when evaluating tendering proposals and placing greater emphasis on the diversification of ICT providers, as well as on the transparency of supply chains for network equipment.[23] Revising the Directive on Security of Network and Information Systems (NIS Directive) to harmonise the protection of the EU's critical digital sector and finalising the adoption of an International Procurement Instrument to ensure reciprocal market access in public procurement would also be useful in this respect. Furthermore, the EU Court of Auditors' proposal to set up a joint procurement framework for cybersecurity infrastructure in the EU should be explored.

To preserve and expand its worldwide standard-setting role, the EU should also explore how to **adapt its data protection and privacy law framework**. The Commission reported on the implementation of the GDPR in June 2020 and highlighted the need to monitor the impact of emerging technologies on the protection of personal data. There are calls to issue specific guidelines for the application of the EU data protection principles in the health and financial services sectors for instance. In addition, the Commission could also reflect on an adaptation of the GDPR to create a more innovation-friendly environment for AI.[24] Furthermore, the revision of the e-Privacy Directive that was blocked in the Council is paramount to ensuring that all communications over public networks maintain respect for a high level of data protection and of privacy, regardless of the technology used.

Finally, EU tech policy should continue to be anchored in **transparency and trust**, the hallmark of the EU approach in digital matters. Building on the trustworthy AI approach, there is a strong case for adopting hard EU law to harmonise rules on the transparency of decision-making systems in the EU, formulate AI ethics rules specific to the healthcare ecosystem and adopt a harmonised framework for guiding the growing use of facial recognition technology (FRT). Experts also call for reform of the liability regime in the EU and, in particular, for amendment of the Product Liability Directive and revision of the e-commerce Directive (in the forthcoming digital services act). Strengthen the regime for online platform accountability for e-commerce, online advertisements and disinformation, is critical to create the trustworthy online environment the EU seeks.

Competition and regulation

Reflection has begun on how update and adapt EU competition policy and the regulatory framework to the digital era. A shift towards more defensive and prudential mechanisms, including new rules to address foreign state ownership and large tech companies' distortive practices, are now under discussion.

Protecting the potential of **European tech start-ups and small and medium-sized enterprises (SMEs)** is very important. New EU instruments could be adopted to achieve convergence in investment screening mechanisms and for assessing takeovers of high-technology EU companies. Also, the creation of an EU Task Force on Strategic Industries and Technologies tasked with identifying strategically important industries for which limits on foreign investment and exceptions to State aid and competition policy would be implemented, could ensure coordination between Member States and the EU in this matter.[25] The idea of redesigning the company tax system, so that it is fit and fair for the digital age has also gained traction among EU policy-makers aiming to help reclaim Europe's digital sovereignty. However, the proposal for establishing EU digital taxation rules tabled in March 2018 was blocked by the Council, and the international agreement negotiated in the Organisation for Economic Co-operation and Development (OECD) forum may be delayed due to the coronavirus crisis. In the short-term, it could also be useful to focus policy-makers' attention on improving company and start-up-related taxation rules where consensus could be easier to build.[26]

Adapting EU competition and regulation policy instruments is necessary in the face of the swift technological evolution taking place.[27] A number of studies and reports call for a complement to

existing ex-post enforcement, through ex-ante rules that better tackle large digital platforms' behaviour, such as increasingly acting as 'digital gatekeepers'. This implies adapting a forward-looking approach to digital markets' regulation and to make online platform eco-systems and online activities more open, fair and predictable. In particular, rules imposing algorithm transparency and neutrality, and data-sharing and interoperability could be considered. Finally, in a long-term perspective, fostering policies to build digital tools and solutions (e.g. operating systems and mobile platforms) that avoid technology lock-ins and foster open, yet still secure, digital ecosystems in the EU could be explored.[28]

An OECD report stresses that Amazon, Apple, Facebook, Google, and Microsoft have made around **400 acquisitions globally in the last 10 years**. In 2017, Alphabet (Google), Amazon, Apple, Facebook and Microsoft alone spent a total of **US$31.6 billion on acquiring start-ups**. The report highlights that very few were examined in detail by national competition authorities or by the European Commission, whereas such acquisitions may give rise to the loss of a nascent competitor or be considered as **'killer acquisitions'** that result in reducing or eliminating competition and valuable products and services. A topical example is the entry of large tech companies into the personalised health and wellness market, as illustrated by Google's proposed acquisition of Fitbit. According to a recent EU Joint Research Centre (JRC) report, there is a strong argument for **scrutinising acquisitions of emerging tech companies** in the context of the Covid-19 crisis.

In the long run, building a genuinely sovereign EU digital environment will also require addressing the current lack of coordination between regulators in this field. This in turn will require **rethinking the governance mechanisms** currently operating within the EU, both horizontally (between sector-specific regulators with parallel and sometimes overlapping competences) and vertically (between Member-State and EU levels of competence). To this end, there would be some benefit to strengthening the interaction between the independent regulatory networks in order to promote collaboration and joint decision-making on digital topics.[29] Such mechanisms would be critical for instance to ensuring a coherent EU sovereign approach in many areas, such as applications management (e.g. apps or IoT devices in the data privacy field), or platform regulation (e.g. in the fields of e-commerce and disinformation). Assessing the experience garnered in the field of data protection (with the national data protection authorities and the European Data Protection Board playing their respective roles) and in telecoms market regulation (with the national regulators and the Bodies of European Regulators for Electronic Communications) would be useful to draw conclusions on a more efficient governing structure.

Conclusion

EU policy-makers have started to design policies to enhance the bloc's digital strategic autonomy. In recent years, several financial instruments have been put in place to narrow the investment gap and additional measures to adapt the EU industrial and technological capacities to the competing environment are being reflected upon in the context of the European data strategy and the AI ethical framework. The EU is increasingly seen as a standard-setter in privacy and data protection and has already undertaken an important legislative effort in the field of cybersecurity and 5G network security. Furthermore, ensuring transparency and trust has become the hallmark of the EU approach to digital matters. Against this background, proposals have been made to push further initiatives at EU level to accelerate the digitalisation process and, in particular to build a data framework, set up a trustworthy digital environment and adapt competition and regulation rules. Fostering investment in ethical AI and frontier technologies, setting up public-private partnerships, and creating a large-scale EU research cooperation framework in the field of new technologies are set to increase the EU's capacity for innovation. Building a secure pan-European data framework and adopting new standards and practices to provide trustworthy and controllable digital products and services would ensure a safer digital environment, in line with EU values and principles. Furthermore, in the competition and regulatory framework, a shift towards more defensive and prudential mechanisms, including new rules to address foreign state ownership and large tech companies' distortive practices, would seem desirable to achieve more technological autonomy.

Possible initiatives

	Project	Actor responsible	What should be done?	
1	European cloud and data infrastructure	Commission Parliament Council	Foster the creation of an EU-wide cloud infrastructure in line with the data strategy.	
2	EU data regulatory framework	Commission Parliament Council	Adopt a new set of measures to foster EU innovators' access to and use of personal and non-personal data (e.g. open access to government data). Assess the opportunity to include 'data sovereignty' clauses in public procurement contracts.	
3	Multiannual financial framework and digital Europe	Commission, Parliament, Council	Adopt the new multiannual financial framework, including Horizon Europe and the Digital Europe programme to support investments in frontier technologies (i.e. AI, IoT, blockchain, high performance computing and quantum technologies) and for advanced digital skills.	
4	Public-private partnerships in AI, data and robotics	Commission, Council	Set up public private partnerships (PPP) in AI, data and robotics to develop a AI innovation based on EU values	
5	Large-scale EU research cooperation framework	Commission, Parliament, Council	Support the creation of a large-scale EU research cooperation framework in new technologies.	
6	GDPR review	Commission Parliament Council	Amend the GDPR to introduce guidance for data protection in specific sectors, such as health or financial services. Assess the opportunity to amend the GDPR to create an innovation-friendly environment for AI.	
7	e-Privacy Directive	Commission, Parliament, Council	Complete the revision of the e-privacy Directive, paramount to ensuring that all communications over public networks maintain respect for a high level of data protection and of privacy.	
8	Set a compulsory EU-wide cybersecurity certification	Commission, Parliament, Council	Amend the EU framework for cybersecurity certification to make certification compulsory in order to ensure a truly safe environment.	
9	Foster coordination in cybersecurity at EU level	Commission, Parliament, Council	Set up a Joint Cybersecurity Unit to reinforce cooperation between the Member states and organise mutual assistance. Finalise the adoption of the proposal to establish European Cybersecurity Competence Centres to support the development and deployment of cybersecurity technologies.	
10	Revise the NIS Directive	Commission	Revise the NIS Directive to strengthen the protection of the EU's critical digital sector.	
11	Standardisation for 5G and beyond	Commission	Foster definition of common EU standards for 5G networks and smart connectivity systems	
12	Standardisation in IoT	Commission	Define common EU standards for IoT devices.	

13	Transparency of decision-making systems	Commission, Parliament, Council	Adopt legislation harmonising rules on transparency of decision-making systems in the EU.	
14	EU framework on the use of facial recognition technology	Commission, Council, Parliament	Adopt specific legislation to set ethical rules and put safeguards and accountability measures in place on the development and use of facial recognition technology.	
15	EU product safety and liability regime	Commission, Parliament, Council	Amend the EU product safety and liability regime to address safety and liability issues brought about by emerging technology such as IoT and AI. Amend the Product Liability Directive.	
16	e-Commerce Directive (Digital services act)	Commission, Parliament, Council	Amend the current liability rules applicable to online platforms and strengthen the EU legal regime for the accountability of platforms.	
17	Coordinated implementation of the EU's public procurement rules	Commission, Parliament, Council	Ensure coordinated implementation of the EU's public procurement rules to take better account of the critical aspects of digital technologies in sensitive sectors (in particular 5G). Finalise the adoption of an International Procurement Instrument to ensure reciprocal market access in public procurement.	
18	New instrument to assess takeover of high-tech EU companies	Commission, Parliament, Council	Adopt new EU instruments to assess takeover of EU high tech companies, especially 'killer acquisitions'.	
19	Create an EU Task Force on Strategic Industries and Technologies	Commission, Parliament, Council	Assess the opportunity of creating an EU Task Force on Strategic Industries and Technologies tasked with identifying strategically important industries for which limits on foreign investment and exceptions to State aid policies and competition policy may apply.	
20	EU digital taxation framework	Commission, Parliament, Council	Explore the possibility to finalise the adoption of a harmonised digital tax	
21	EU digital taxation framework	Commission, Parliament, Council	Explore the possibility to adopt specific start-up related taxation legislation to foster the development and growth of high-tech start-ups in the EU.	
22	Control digital gatekeepers	Commission, Parliament, Council	Explore the opportunity to impose ex-ante rules (e.g. on algorithm transparency and neutrality and data sharing) to better control digital platform behaviour, including increasingly acting as 'digital gatekeepers'.	
23	Foster open digital ecosystems	Commission, Parliament, Council	Assess whether the EU framework should promote digital tools and solutions (e.g. operating systems) that avoid technology lock-ins and foster open digital ecosystems in the EU.	
24	Governance mechanisms and coordination between digital regulators	Commission, Parliament, Council	Rethink the governance mechanisms and interaction between regulators to promote collaboration and joint decision-making on digital topics.	

REFERENCES

EPCS, Rethinking Strategic Autonomy in the Digital Age, EPSC Strategic Notes, 2019.

L. Ilves and A.-M. Osula, The Technological Sovereignty Dilemma – and How New Technology Can Offer a Way Out, *European Cybersecurity Journal*, 2020.

F. Gueham, Digital sovereignty - Steps towards a new system of internet governance, Fondapol, 2017.

European Commission, USA-China-EU plans for AI: where do we stand?, 2018.

ENISA, Study on CSIRT landscape and IR capabilities in Europe 2025, 2019.

R. Csernatoni, An Ambitious Agenda or Big Words? Developing a European Approach to AI, Egmont Security Policy Brief, 2019.

M. Leonard and J. Shapiro, Empowering EU Member States with strategic sovereignty, European Council on Foreign Relations, 2019.

F. Bria, Putting tech and innovation at the service of people and the green transition, UCL Institute for Innovation and Public Purpose blog, 2020.

ENDNOTES

1 See Fondapol, Digital sovereignty - Steps towards a new system of internet governance, Farid Gueham, January 2017. See also J. Nocetti, Contest and conquest: Russia and global internet governance, International Affairs, 2015.

2 See EPCS, Rethinking Strategic Autonomy in the Digital Age, July 2019. The concept was however criticised as based on faulty assumptions. See T. Barker, Europe Can't Win the Tech War It Just Started, Foreign Policy, 2020.

3 See ESPAS, Global Trends to 2030: Challenges and Choices for Europe, April 2019, p28.

4 See European Commission, Communication Artificial Intelligence for Europe, April 2018.

5 See European Commission, USA-China-EU plans for AI: where do we stand? January 2018.

6 See D. Castro, M. McLaughlin and E. Chivot, Centre for data innovation Who Is Winning the AI Race: China, the EU or the United States? August 2019.

7 See, D. Kalff and A. Renda, Hidden Treasures, Centre for European Policy Studies 2019.

8 See European Commission, Europe in May 2019: Preparing for a more united, stronger and more democratic Union in an increasingly uncertain world, May 2019. See also EPCS, Rethinking Strategic Autonomy in the Digital Age, EPSC Strategic Notes, July 2019.

9 See R. Csernatoni, An Ambitious Agenda or Big Words? Developing a European Approach to AI, Egmont Security policy brief, November 2019.

10 See French Economic, Social and Environmental Council, Towards a European digital sovereignty policy, March 2019 at 18. Alphabet (Google) and Facebook, generate 88 % and 97 % of their income respectively from exploiting data collected for marketing purposes.

11 See La Tribune, Terminal neutrality as a tool for our digital sovereignty?, 2020.

12 See The Internet & Jurisdiction Global Status Report 2019, p.95.

13 See B. Rosa, Data laws or data wars, 2020.

14 The leaders on the cloud market are Amazon (47.8 %), Microsoft (15.5 %), Alibaba (7.7 %), Google (4 %) and IBM (1.8 %) (Gartner, July 2019). See also D. Kalff and A. Renda, Hidden Treasures, Centre for European Policy Studies, 2019, p. 173. An estimated 92 % of data produced in the Western world is currently stored in the USA and only 4 % in Europe.

15 See F. Bria, Putting tech and innovation at the service of people and the green transition, 2020.

16 See G. Petropoulos, Artificial intelligence in the fight against COVID-19, 2020.

17 See ENISA, Study on CSIRT landscape and IR capabilities in Europe 2025, February 2019.

18 See McKinsey Global Institute, Innovation in Europe, Discussion paper October 2019.

19 See CERRE white paper, September 2019, pp20 and 21.

20 See European Laboratory for Learning and Intelligent Systems (ELIS) and also Confederation of Laboratories for Artificial Intelligence in Europe (CLAIRE).

21 See L. Ilves A.-M. Osula, The Technological Sovereignty Dilemma – and How New Technology Can Offer a Way Out, 2020.

[22] See A. Bendiek and E. Pander Maat, The EU's Regulatory Approach to Cybersecurity, SWP working paper, October 2019.

[23] See EPSC, Rethinking Strategic Autonomy in the Digital Age, EPSC Strategic Notes, July 2019. See also Business Europe, The EU and China - addressing the systematic challenges, January 2020.

[24] See M. Gérot and W. Maxwell, Will the GDPR frustrate Europe's plans for AI?, 2020.

[25] See M. Leonard and J. Shapiro, Empowering EU Member States with strategic sovereignty, June 2019.

[26] See Atomico, The State of European Tech, 2019 at p. 215.

[27] Fora analysis of the technological evolution and change of policy paradigms at stake See A. Renda, Single Market 2.0: the European Union as a Platform, College of Europe, Research paper in law 2/2020.

[28] See European Digital SME Alliance, Position paper COVID-19 economic recovery: a recovery strategy building on digital, 2020. See also, The words of the day after, "digital sovereignty", Capgemini, 2020.

[29] See B. Wagner and C. Ferro, Governance of Digitalization in Europe, Bertelsmann Stiftung, 2020.

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)