cepStudy

European Leadership in the digital Economy

Seventeen Recommendations

EXECUTIVE SUMMARY

This is the summary of a cepStudy commissioned by SAP. The complete study can be downloaded here.

This study identifies three main priorities and seventeen detailed recommendations for a European political agenda aiming to reach European leadership in the digital economy. Setting priorities is urgently necessary. Europe is lagging behind the United States and China in artificial intelligence and cloud computing, two of the main global technical trends which will seriously affect economic growth in the years to come.

Whereas network effects and economies of scale have led to an American and Chinese dominance in B2C-markets, the EU should now take the necessary actions to avoid the same happening in B2B-markets.

Protectionism measures are not helpful in regaining European technological sovereignty. On the contrary, the three priorities all have a market-oriented approach, spurring innovation and safeguarding competition amongst suppliers in the digital economy.

As a **first priority**, the EU should actively foster a true internal market for data as the EU is not nearly using the economic potential associated with the sharing and (re-) use of the data present in its territory. Actions in this field should concern personal, public and non-personal data.

Regarding personal data, we plead for more harmonisation and the use of sandboxes and regulatory hubs to create legal certainty in applying the GDPR.

The availability of public data should be increased through standardisation of data formats, through the inclusion of data availability as a factor in public procurement and through stricter data-access rules for public data of high-value.

Reasons why businesses are hesitant in sharing and pooling non-personal data are very diverse and not all of them can be solved through policy action. The EU data space initiative can however contribute to lowering transaction costs of B2B data sharing.

National data localisation requirements concerning the storing of personal, public or non-personal data hinder the realisation of economics of scale and are generally incompatible with the very idea of an internal market for data. They should remain the exception and we call upon the Commission to consistently proceed against localisation requirements that are not justified under the GDPR and the FFD-Regulation.

As a **second priority**, the EU should ensure effective competition on digital markets in the B2B-sphere. B2B-markets are markedly different from B2C-markets and we do not see a wide-spread need for regulatory action to safeguard competition. In the field of cloud activities, vertical integration and limited access to infrastructure on the different layers of the market (IaaS, PaaS and Saas) might be able to limit competition in the future. Competition law can handle such problems and sector-specific regulation is not needed. On the same markets, limited access to essential data may also limit competition. In these cases, regulatory interventions aiming at ensuring data portability on cloud markets may be necessary. In any case, such intervention should be targeted to operators with a market dominant position only.

The **third priority** concerns a European digital industrial policy and focusses on the general competitiveness of the European digital economy as a precondition for digital sovereignty. The digital industrial policy should protect the openness of the economy, allow for economies of scale, entail investment friendly infrastructure regulation and promote digital skills.

We propose a EU Framework for secure and trusted cloud computing as a main element of such a digital industrial policy. The framework addresses concerns related to data security, data governance and service availability in the cloud. Those concerns go back to the widespread use of non-European hyperscalers by EU companies and reflect the public good character of cloud service availability to our economies and societies.

The proposed framework is proportionate, efficient and non-discriminatory. It defines certification schemes for the voluntarily classification of cloud service providers on the basis of the EU Cyber Security Act. Following that, we propose a governance structure that guarantees a safe use of cloud services by a limited number of operators of essential services such as financial services, energy or

transport throughout the EU. Most importantly, our proposal aims at avoiding any competitive distortions between private providers of such essential facilities.

17 Recommendations to promote European leadership in the digital Economy

NINE RECOMMENDATIONS FOR A SINGLE MARKET FOR DATA IN THE EU

- **Recommendation No. 1:** The Commission should keep on **monitoring closely** the evolution of the **market of data trusteeship** to timely detect the emergence of any future obstacle preventing the business from going cross border.

- **Recommendation No. 2:** The European Commission should use the upcoming review of the **GDPR** to ensure **legal certainty through a higher level of harmonisation**.

- **Recommendation No. 3:** Initiatives that aim at increasing **legal clarity in the GDPR** by establishing a dialogue between Data Protection Authorities (DPAs) and businesses or innovators are **to be supported**. They can help DPAs to identify new developments in technology and innovation while ensuring that people's rights to privacy and data protection are respected. At the same time, these initiatives, whether called **"sandboxes" or "regulatory hubs" must be market neutral** (i.e. available to all market participants).

- **Recommendation No. 4:** The Commission should develop, together with the relevant stakeholders, **open standards on platforms and data formats for public sector bodies** to make available their data. The standardisation should be carried out on a sectoral basis.

- **Recommendation No. 5:** The Commission should aim to **extend the scope of the PSI Directive to include private companies providing public interest services**, thus ensuring the availability of privately held data relating to the provision of the public interest service. The Commission should also encourage Member States and their public authorities to make public procurement conditional upon the availability of data generated in this context.

- **Recommendation No. 6:** The Commission should investigate whether establishing a **general obligation to grant access to public sector data and public interest data** might be necessary, first and foremost **for high-value datasets**. It should especially look into the existing data sharing practices of public and private companies in particular sectors – e.g. transport, geospatial – to evaluate if data sharing based on voluntary agreements is sufficient or if further action – be it through soft-law measures or binding EU law – is required.

- **Recommendation No. 7:** The European Commission's European **data space initiative may contribute to reducing transaction costs of B2B data** sharing in Europe. The initiative deserves to be intensified as long as it is market-neutral by design.

- **Recommendation No. 8:** A **legal ownership right to data should not be introduced**. De facto control over data through contract law and technical restrictions form a sufficient basis for data market development.

- **Recommendation No. 9:** As data localisation requirements hinder the development of a single market for data in the EU, the EU-Commission should consistently **proceed against national data localisation requirements** that are not justified under the GDPR and the FFD-Regulation. In order to enable the identification of data localisation requirements under the GDPR, the possibility of installing a register for national data localisation requirements under the GDPR should be investigated.

FIVE RECOMMENDATIONS TO MAINTAIN EFFECTIVE COMPETITION ON CLOUD AND DIGITAL MARKETS

- **Recommendation No. 10:** The market for large scale cloud services (**hyperscaler market**) is currently characterised by intense competition amongst a relatively small number of competitors facing high fixed costs. It remains to be seen whether the current level of competition will prevail also in the future. In any case, any **public intervention** – e.g. by regulating switching-costs between cloud providers, interoperability requirements or end-user-prices – which is **motivated by competition concerns should take place only given proof of a significant and non-contestable market power** (SMP) of a cloud service provider. Upon proof of such market power, competition law seems well able to offer an appropriate answer. The use of **sector-specific regulation** addressing dominant cloud service providers is **not recommended**.

- **Recommendation No. 11:** Whether or not a PaaS-provider holds significant market power has to be investigated on a case-by-case basis. In any case, **the finding of a non-contestable market dominance of a platform provider should be a pre-condition for competition-based intervention.** If proven, such dominance can be dealt with appropriately using general competition law. **A need for sector-specific regulation is not evident.**

- **Recommendation No. 12:** Tying and bundling practices by **cloud providers vertically integrating into the PaaS-market** are unproblematic, unless those providers hold a non-contestable market power on the cloud-markets. If they do, **competition law** is well fit to cope with this abuse behaviour.
  Absent tying and bundling, the **refusal** by a vertically integrated cloud provider **to grant** PaaS-competitors **access** to its cloud infrastructure **can be dealt with using** the essential facilities doctrine. This doctrine offers a convincing trade-off between protection of intellectual property rights and competition on aftermarkets. The need for intervention is limited to cases where the following criteria are fulfilled: (1) the cloud provider holds a non-contestable dominance on the cloud market, (2) the use of the cloud is imperative, (3) competing PaaS-providers offer a novelty and (4) the cloud provider cannot offer objective reasons justifying the refusal of access. Although a sector-specific access regulation regime may be able to cope with dominant, vertically integrated cloud providers on the PaaS-market, clear advantages of such regulation as compared to **general competition law** are not apparent.

- **Recommendation No. 13:** Privileged data access may hinder competition. **On the SaaS-market, the vertical integration of IaaS-providers down to the PaaS and SaaS-markets** and the associated market concentration **may** aggravate the competition problems on the SaaS-market associated

with privileged data access. Also, privileged access to data may **cause competition problems** in very different downstream markets.

With the essential facilities doctrine, **competition law** offers a sound fundament to deal with competition issues in respect with vertical integration. However, in practice, if data turns out to be the essential facility, access-granting **may prove** to be very **difficult and unpractical.** In that case, alternative remedies or **regulatory interventions** that prevent data being or becoming an "essential facility" **may be necessary**. Such interventions **should aim at increasing data portability**, be it by lowering barriers to switching and preventing lock-in situations or by granting direct portability rights.

However, when doing so, **intellectual property rights** must be given due consideration. In any case, the finding of a **dominant market position** in the absence of potential competition on a well-defined upstream data market must be a **precondition for any intervention**. In cases where markets are defined very narrowly (e.g. brand-wise), the finding of market dominance may be rather straight-forward and regulation may be appropriate. In all other cases, competition law can better guarantee an appropriate market definition and analysis of market dominance.

- **Recommendation No. 14:** The most appropriate tools to **grant legal certainty** in questions of anticompetitive behaviour **concerning data pooling** are:
  - the **guidelines** of the Commission because, by identifying significant circumstances for the application of Article 101 TFEU to data pools agreements, they can be relied upon by undertakings while self-assessing their market behaviours;
  - the **guidance letters**, because the level of change brought about by Big Data in competition law analysis is so massive that genuinely novel questions are likely to arise. This would enable the related applications for guidance letters to be finally upheld by the Commission.

THREE RECOMMENDATIONS FOR A EUROPEAN DIGITAL INDUSTRIAL POLICY

- **Recommendation No. 15:** Attaining a **competitive European digital economy is a conditio sine que non for digital sovereignty.** The bulk of the work and investment to reach this aim has to be delivered by private investors and the private economy. Nevertheless, the EU, national legislators and policy makers should set the appropriate regulatory framework for this to happen. This framework should (1) safeguard the openness of the economy and (2) competition, (3) allow for economies of scale, (4) entail investment friendly infrastructure regulation and (5) promote digital skills.

- **Recommendation No. 16:** The EU, through the Commission, should negotiate an **agreement with the US** which clarifies the rules regarding cross-border access to electronic evidence in the context of criminal proceedings. Not only should this agreement protect EU citizens and companies by ensuring the necessary safeguards, but it should also aim at increasing legal certainty in data access requests by US judicial authorities to EU service providers, thus preventing conflicts of law.

- **Recommendation No. 17:** We propose an EU Framework for secure and trusted cloud computing that addresses concerns related to data security, data governance and service availability in the

cloud. The growing use of cloud services brings about a lot of economic advantages, but at the same time confronts us with political and operational risks which may endanger the continuous availability of services which are essential to our economies. The public good character of cloud service availability justifies public intervention.

We propose the creation of an EU Framework for Secure and Trusted Cloud Computing as a model of public intervention regarding the use of cloud services which is proportionate, efficient and non-discriminatory. It consists of three steps.

- **In Step 1**, the EU should define common requirements for secure and trusted cloud computing that will address user concerns related to data security, data governance and service availability. As requested by the European Commission, the ENISA should draft baseline cloud computing security certification schemes regarding general use. In addition, ENISA should draft complementary cloud computing security certification schemes for public administrations and sectors providing essential services (according to the NIS-Directive).
- In **Step 2**, the existing modalities for the issuing of certificates in the Cybersecurity Act can be applied to the certification of cloud service suppliers without any change. There is no need for making certification compulsory.
- In **Step 3**, the use of cloud services by economic actors in certain sectors can be made conditional upon the use of a cloud provider of a certain assurance level of the cloud security certification schemes. Any such regulatory requirements must be risk-based, proportionate and may not distort competition, neither between cloud service providers nor between regulated entities.
- In order to reach a uniform application of these regulatory requirements, we recommend in **Step 3a** a consistent identification of essential service operators to whom regulatory requirements will apply. For this reason, we propose a more formal role for the NIS-Directive's "cooperation group" to identify operators from the energy, transport and financial market sector (but not for banks).
- After confirming in **Step 3b** that cloud security requirements for essential service operators will follow the EU cloud security certification scheme, it is necessary in
- **Step 3c** to safeguard a uniform application of the certification scheme. In the financial industry, the well-developed supervisory structure may be sufficient to reach this aim. For the energy and transport sector, we suggest the establishment of new decision-making bodies of sectoral supervisors and cybersecurity authorities which shall be responsible for safeguarding a uniform application. Given the national nature of markets for health, water and digital infrastructure, we suggest national authorities should be responsible for the application of the cloud certification schemes.

Although a uniform application of the EU cloud security certification scheme in the public sector is unlikely, the national use by the public sector of the certification scheme would increase the relevance of the EU cloud security certification scheme and the providers adhering to it.

Contact:

Dr. Bert Van Roosebeke
Head of Department
cep | Centrum für Europäische Politik
vanroosebeke@cep.eu
+49 761 / 386 93 230