Strengthening Europe's digital sovereignty and protecting data effectively

Deutsche Telekom's Data Privacy Advisory Board in favor of equitable duty of protection and competition in the digital economy

Summary: Protecting European fundamental rights – supporting a responsible data economy

Our current, and certainly our future society and economy are and will be influenced by the momentum of digitalization. Our digitalized world is based on globally scalable platform solutions and cloud services. Europe, too, continues to be dominated by the major internet and cloud providers. These hyperscalers act as "supranational entities," often according to their own rules. They dominate the global market and systematically expand their position. To date, European providers have played only a minor role in the global market. In an increasingly globalized world, Europe presents itself as a champion of ethical European values. The EU has developed a wide range of regulatory approaches to this end, such as the General Data Protection Regulation (GDPR).

However, the lack of effective digital sovereignty means that Europe cannot guarantee compliance with these European values for its citizens. In the digitalization competition, Europe plays the role of arbitrator instead of active player.

Anyone who depends excessively on others ultimately ceases to make the rules and instead has to follow them. The German Federal Government's Data Ethics Commission has already pointed to this logic with some concern. Efforts to secure digital sovereignty are not only about seizing market opportunities.
More than this, digital sovereignty is about securing the fundamental rights and freedoms of people in social interactions and, as such, benefits society. Although Europe is a champion of industry – also when it comes to digital solutions (Industry 4.0) – there is a risk that Europe will drop behind to the status of a "digital colony," particularly given the serious deficits in Europe in terms of enforcing data privacy.

We therefore call on the governments of Europe and the EU to support European companies in building a sovereign data economy. This requires a single European digital market that establishes the following principles:

1. Consistent, comprehensible regulation in the area of data privacy.
2. The enforcement of data privacy law by way of timely and effective implementation of existing rules, in particular by better coordinating the approach of the national European data protection authorities.
3. The establishment of equitable, responsible competition.
4. Strengthening of public sector demand for digital services from European providers based on a sovereign European infrastructure (Gaia-X/EU Cloud).

One of Europe's key functions is to assert its own industry and innovative power. It needs to act quickly if it is to seize the opportunity for digital sovereignty. Europe must play to its strengths.

In the process, we Europeans must not subjugate our cultural understanding of the protection of fundamental rights and freedoms and the ensuring of fair competition to the effective market power of non-European players.

Europe's culture as a strength

We need European solutions. Europe's strengths are an inventive spirit, innovation, industrial capabilities. Europe creates trusted business models for society. The European approach takes the fundamental values of the European Union – which include data privacy and security – seriously. Europe needs a European industrial policy to promote European values. Industrial promotion must not be allowed to founder on national sensitivities. Rather, it must take a continental perspective, including, for example, in mergers, in antitrust law, and in regulation. Europe needs a single digital market. In this respect, four action areas are vital:

1. **Consistent, comprehensible regulation in the area of data privacy**
   Europe is becoming entangled in unclear regulation. Despite the existing and much criticized potential for overlap with the GDPR, after almost four years of negotiations at EU level, there may be an end in sight for the drafts of the E-Privacy Regulation. However, the digital world has already moved on in this time. In terms of content, no satisfactory solution is emerging. Instead of consistent and equitable treatment for data privacy, telecommunications providers are disadvantaged by regulations that differ from those for services with the same function provided largely by non-European providers. For example, the option of using personal location information is heavily restricted for telecommunications providers but remains flexible for other providers.
   The Data Privacy Advisory Board deems a level playing field here to be critical. The regulation should take a more risk-based approach, especially with regard to electronic communications and the associated services. For instance, processing of location information could be permitted with the use of protective mechanisms such as pseudonymization and anonymization in order to promote socially useful functions, such as traffic management or autonomous driving. The discrimination against European players and this divergent regulation for comparable data is unjustified.

   The success of digital services and business models depends in large part on the trust of consumers. The awareness for data privacy is growing fast and can be a differentiator for digital services. As such, the Data Privacy Advisory Board takes a critical view of initiatives that intend to effectively ban end-to-end encryption Europe-wide. Obligations to build in back doors for security authorities and weak encryption jeopardize this trust and would ultimately result in Europe falling further behind in the digital arena.

2. The enforcement of data privacy law by way of timely and effective implementation of existing rules

A large number of companies currently effectively do not comply with, or insufficiently comply with the provisions of the GDPR. Structural deficiencies in terms of transparency and the rights of affected parties mostly cannot be remedied by users themselves (companies and end users). A deficit in enforcement and the consequent lack of sanctions against such providers are unacceptable. Although some data protection authorities have sanctioned the data privacy violations of a few companies with fines, the data protection authorities responsible for these companies in Luxembourg and Ireland remain largely inactive to date.

The misuse of personal data in some cases and the resulting distortions of competition must not be tolerated.
Given the cross-border relevance of data-driven business models, cooperation must be stepped up on the part of all European data protection authorities. The consistency mechanism set out in the GDPR to ensure the consistent application of data protection law in all member states must also be activated in the event of inaction on the part of the responsible national data protection authority. The European supervisory authorities must act with courage and cohesion to take a strong stand and enforce compliance with the rules.

3. The establishment of equitable, responsible competition

Internet and cloud providers have also been providers of telecommunications services for some considerable time. However, de facto, and in terms of regulation, they are not classified as telecommunications providers and this gives them a substantial competitive advantage. To the extent that they offer messaging, voice and video, or internet services for communications, it must be ensured once the European Electronic Communications Code is in force that they are subject to the same legal regulations as apply to offers with the same functions from telecommunications companies, for example, with regard to interoperability, data privacy, and telecommunications secrecy. The same applies for schemes of companies, such as connecting intelligent voice mailboxes with each other and thereby setting up regional data networks in the 900 MHz range. According to the company’s own information, Amazon plans initially to implement this in the United States by way of software updates for devices already sold without first obtaining consent from customers.

The competitive disadvantage arising for European telecommunications providers from one-sided or insufficient regulation robs them of substantial market shares, innovative power, and investment opportunities. The blank check for U.S. and Asian internet companies also cuts into the investment potential of European telecommunications providers, increasing the risk of Europe falling further behind in digitalization. For us, this is not about protectionism. On the contrary, Europe needs an equal and fair framework for innovative business ideas for all competitors.

Europe must not be allowed to turn into a “digital colony,” in which U.S. and Chinese companies use personalized business models to mine and then use personal data on a dubious legal basis. The legal and economic frameworks must be designed such that European enterprises do not fall behind in a digitally controlled market that is dominated by data.

Europe must decide whether to give in to supranational internet giants or to reclaim its own European identity. It can only do this if the same rules and laws apply to everyone. If companies like Facebook provide telecommunications services like WhatsApp or Facebook Messenger, then they must also be treated as telecommunications providers – with all the protective functions for consumers.

4. Strengthening of public sector demand for digital services from European providers based on a sovereign European infrastructure

The European economy also needs support from the public sector to (re)gain digital sovereignty for Europe. In principle, it is on the right track with the Gaia-X initiative, which aims to achieve closer networking of the European cloud infrastructure.

But this can only succeed if public bodies and government organizations as buyers do not base their contracting decision on cost considerations alone. To this end, in future, they have to place their data in a sovereign European cloud infrastructure instead of continuing to rely on the cloud services of major providers from the United States and China.

Furthermore, it requires a European industrial policy that strengthens a responsible, digital European economy. The basis and currency for a digital economy is trust in the information and communications technology. The more autonomous, the more intelligent or “smarter” systems become, the more we need to trust in the information and telecommunications technology. The basis for trust is the alignment of the technical systems with our ethical values. We should systematically promote the development of such systems.

Our aim:

Europe needs equality of treatment for the digital economy, not just in terms of regulation in the area of data privacy, but above all in terms of effective enforcement. It is important to note that this is not about treating individual European companies preferentially, but rather about equal opportunities with equal and comparable business models. The European players of the market economy cannot now or in future correct the described imbalance by themselves. Especially given that the major digital players are often not called directly to account. Incidentally, not even when it comes to contributing to the costs of building the infrastructure on which they generate their profits. The European industry requires support from the governments and public bodies of Europe to build a sovereign data economy.

Europe must cast off the role of arbitrator and take up the mantel of competition – now.

The Members of the Data Privacy Advisory Board of Deutsche Telekom AG