Law | Policy Concepts

PC.30 Digital Sovereignty

Authors: Aline Blankertz

Last update: 2021-10-04 08:16:39 | By: Aline Blankertz

Created at: 2021-05-15 09:30:36

"Digital sovereignty" is a term that has strongly gained importance at the German and European levels in recent years. The call for (more) digital sovereignty is omnipresent in strategy and position papers and is shared by a wide range of actors, including state, business and civil society.

"Digitally sovereign" can be individuals, organizations, nation-states, and the public administration, which performs state functions as an organization. A variety of implications for data and information protection can arise from digital sovereignty.

There are various approaches to determining the concept of digital sovereignty:

> *- Digital association **Bitkom** defines it in distinction to the two opposite poles of digital dependency and digital autarky (Bitkom, **Digitale Souveränität: Anforderungen an Technologie- und Kompetenzfelder mit Schlüsselfunktion**, 2019).*

> *- **Kompetenzzentrum Öffentliche IT** speaks of "strategic digital autonomy," which it in turn divides into different domains, namely knowledge, research, development, production, operations, usage, and transparency sovereignty (Mohabbat Kar/Thapa, **Digitale Souveränität als strategische Autonomie**, 2020).*

> *- **IT-Planungsrat** operationalizes the term as the extent to which an entity can switch, shape, and influence providers*
>
> *(IT-Planungsrat, **Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung**, 2021).*

Another question relevant to digital sovereignty is in which areas it should be desirable. The focus is on technologies with key functionality which, in turn, can be defined via national political and economic interests. These interests encompass technologies for national security as well as potentially other critical infrastructures.

However, there is also criticism of using digital sovereignty as a policy objective, which is necessarily

relative (*Tiedeke*, **Die (notwendige) Relativität digitaler Souveränität**, in: MMR 2021, 624). The conceptual proximity to nation-statehood can be understood to mean that similar borders are to be transferred to the digital realm. In the process, a conflation with power and industrial policy goals takes place, criticizes *Thiel*, among others, and proposes "a much more efficient and socially inclusive control of public as well as private power" as a more clearly determined political goal (*Thiel*, **Das Problem mit der digitalen Souveränität**, FAZ vom 25.1.2021).

Digital sovereignty is not to be confused with data sovereignty [see **Tile PC.29**].

Concrete areas of application of digital sovereignty

Cloud infrastructure

> *It is widely discussed that European companies and public organizations are dependent on large US companies for their use of cloud infrastructure. In addition, there is concern that data sovereignty, as an aspect of digital sovereignty, is endangered because US authorities can access clouds hosted under US law. The large-scale EU project GAIA-X is intended to address this by developing standards and interfaces to ensure interoperability between cloud providers. This, in turn, should increase the opportunities for cloud users to switch and lower the barriers to entry for European providers.*

Operating system interfaces

> *In the fight against the Covid 19 pandemic, providers of mobile operating system influence when and how interfaces are opened. Apple and Alphabet (Google's parent company) chose to open Bluetooth interfaces only to decentralized models of contact tracing by government agencies. While this was intended to protect the privacy of users, private actors were criticized for deliberately limiting the state's room for maneuver. As a result, the state's digital sovereignty was considered at risk.*

Mobile communications infrastructure

> *5G infrastructure is often deemed critical infrastructure because it is necessary for mobile data exchange. This led to a controversial discussion in the US and the EU, among others, about whether Chinese providers such as Huawei should be excluded from providing 5G infrastructure. The intention was to prevent the Chinese government from gaining access to and control over data streams in other countries. The US government decided to exclude Chinese providers, which in turn has motivated US trading partners to enforce similar measures.*