Digitisation and sovereignty of the state

Services for citizens are bundled in one-stop shops. Artificial intelligence and automation are increasingly resulting in a "no-stop government" in which neither citizens apply for services nor do administrative staff actively intervene in processes. Algorithms make the initial decisions, for example about the allocation of services. IT is becoming a critical infrastructure.

This challenges the state and our understanding of the state. When the actions of the administration, the foundations on which they are based, and the means by which they are carried out change, the ways in which the state acts, the relationship of the state to its citizens, and international dependencies change. Ultimately, the crucial question is whether the state can control these ongoing changes and/or sufficiently frame them to maintain its sovereignty.

In brief

- Digitisation also changes politics and the state. State sovereignty is massively challenged, especially with regard to administrative action, digital infrastructure, and democratic processes.
- Digital sovereignty refers to the exclusive self-determination of legal entities such as states and natural persons under the conditions of digitisation.
- In order to (re)establish digital sovereignty, it is necessary to act consistently on various levels (national and international), both in technical, organisational and regulatory terms, and not least in public discourse.

How sovereign is the sovereign's representation in the 21st century?

Foto: © Parlamentsdirektion / Th. Topf

What is it about?

Digitisation is a very important process of change in the 21st century. There are hardly any areas of human activity today that could do without electronic devices and data-based applications. Politics and state administration are no exception to this development. Administrative action has long since ceased to be just an activity in offices: the term e-government was already established around two decades ago. The state now provides many services via the Internet. Information technology has also long played a central role in the so-called back office. Administration is increasingly relying on automation-supported communication and interaction, for example via chatbots, and is exploring the potential of artificial intelligence.

Sovereignty refers to the exclusive self-determination of legal entities, especially states, but also of persons. Of course it can never be absolute because it is always limited by the existence of other states or individuals and their actions. The term "digital sovereignty" now refers to sovereignty under the conditions of digitisation. In an ideal scenario, a state is "digitally sovereign" if it acts autonomously in its area of responsibility in the digital space and exercises the monopoly of state power against the resistance of other states and non-state actors in particular.

In that sense, can there be any digital sovereignty at all for Austria (or any other nation state)? The following four areas are affected: (1) action in their own area, especially in administration; (2) the provision of necessary digital infrastructures on their territory or for their citizens; (3) the creation of conditions for functioning democratic processes; and (4) the creation of legal and infrastructural frameworks that enable their citizens to digitally act with sovereignty, i.e. be self-determined.

INSTITUTE OF TECHNOLOGY ASSESSMENT

Challenges

A closer examination of the four areas mentioned clearly shows that, in the age of digitisation, the state is under strong pressure and that much is still unclear: With ongoing partial automation of the administration, the question of responsibility for automated decisions arises. Furthermore, there is hardly any discussion on ethical principles for and impact assessments of algorithms in the administrative sector.

The administration is increasingly making use of global digital platforms (e.g. Google, Amazon) which have functional sovereignty that has traditionally been exercised by the state. This raises the question as to where non-state sovereign territories have already established themselves and what options exist for regaining state sovereignty.
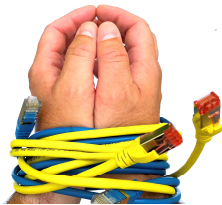
The state, too, is placed in digital dependency.

The worldwide networking of digital infrastructures, the lack of transparency regarding the functioning of IT components, and the potential danger of cyber-attacks, even from outside the country, are creating massive security risks. Possible measures include avoiding dependencies on certain providers (e.g. through open source software), the acquisition of independent technological competence, and the development of own offerings for critical infrastructures and services in order to push back global digital monopolies.

In the political sphere, for example, the question arises of how to achieve a balance of interests between equally justified state and individual digital sovereignty. Or how legislation at EU or global level could possibly create a new model of digital state sovereignty that creates a fair balance under the conditions of global digitisation. Sensitive and essential questions also arise for the stability of democracy. The future handling of the increasing and easier-to-achieve manipulation of public opinion in the digital media is an important issue since social bots, deep fakes, etc. have become a serious threat to the digital sovereignty of the political system.

What to do?

In order to maintain or restore digital state sovereignty, consistent action is needed on various levels (national and international), both from a technical as well as organisational and regulatory point of view, and not least in public discourse.

- In view of the importance of digitisation for the future of our societies and democracy, politics and civil society have to become aware of this issue and conduct a comprehensive debate with a view to thoughtful, democratically-oriented digital sovereignty.
- A comprehensive and ambitious digitisation strategy at national and European level would have to make the best possible use of existing scope for action and open up new one, avoid lock-ins or critical security gaps, and promote society's confidence in the sustainable safeguarding of digital sovereignty.
- The factual basis and options for action required for this discussion necessitate a more in-depth analysis. As a first step, administrative decision-makers' and experts' open questions (see section "Challenges") have to be examined in more detail whilst analysing respective procedures.

Further reading

Nentwich/Jäger/Embacher-Köhle/Krieger-Lamina (2019) Kann es eine digitale Souveränität Österreichs geben? Herausforderungen für den Staat in Zeiten der digitalen Transformation. ITA-manu:script 19-01.
epub.oeaw.ac.at/ita/ita-manuscript/ita_19_01.pdf

Contact

Michael Nentwich

Email: tamail@oeaw.ac.at

Phone: +43(1)51581-6582