

## Staatliche Souveränität im digitalen Zeitalter

Die Entwicklung zu einem Staat mit hoher Digitalisierung von Aufgaben und Infrastruktur ist seit Jahren ungebremst: Softwareproduzenten drängen mit immer neuen Angeboten auf den Markt, und Behörden suchen neuartige Lösungen zur Verwaltungsvereinfachung und Effizienzverbesserung. Mittlerweile werden staatliche Aufgaben und Dienstleistungen vielfach vollautomatisiert erbracht. Die erwarteten positiven Effekte reichen von Einsparungen bis hin zu neuen Daten als bessere Entscheidungsgrundlagen (Data Driven Government) und zur Minimierung von bürokratischem Aufwand (vom One-Stop- zum No-Stop-Government). Die Regierung bekennt sich zur weiteren Digitalisierung:<sup>1</sup> Alle BürgerInnen sollen eine digitale Identität bekommen, mehr Behördenwege digitalisiert werden oder entfallen; durch Daten-Zusammenführung soll auch der Gesetzesvollzug profitieren, etwa im Bereich der Besteuerung.<sup>2</sup>

Doch wie verändert das alles unser Verständnis von „Staat“? Dies wird unter anderem unter dem Stichwort der digitalen Souveränität diskutiert (z. B. Müller Quade et al. 2018; BITKOM 2015). Durch Digitalisierung werden Bereiche des Staates auch unbeabsichtigt verändert (z. B. wer Zugang zu welchen Kommunikationskanälen hat<sup>3</sup>) und es eröffnen sich Räume, in denen Machtverhältnisse nicht klar geregelt sind. Kann das die Souveränität des Staates gefährden? Souveränität hieße hier Selbstbestimmtheit, die Fähigkeit eigenständig und unabhängig Entscheidungen (z. B. über Softwarelösungen und Datenhaltung) zu treffen. Dazu ist nicht unbedingt Autarkie erforderlich, aber Pfadabhängigkeit bei Informationstechnologie-Infrastrukturen, und nicht zuletzt Abhängigkeit von Monopolisten würde diese Souveränität gefährden. Es müssen ausreichend Kompetenzen vorhanden sein, verschiedene Lösungen zu verstehen, miteinander zu vergleichen, selbstständig zu betreiben und weiterzuentwickeln. Die Auslagerung hoheitlicher Aufgaben an privatwirtschaftliche, oft grenzüberschreitend agierende (und Daten auch anderswo speichernde) EDV-Anbieter scheint problematisch, etwa in [Cloudspeichern](#) oder bei der Verwendung von Routern. Darüber hinaus entstehen durch die Digitalisierung der Verwaltung neue Sicherheitsprobleme und veränderte Herausforderungen für das Informationssicherheitsmanagement. Durch das Übertragen von Aufgaben an technische Systeme (z. B. Entscheidungssysteme auf Basis von KI) werden viele von ihnen zu sog. Kritischen Infrastrukturen, deren Ausfall von wesentlicher Bedeutung für die Aufrechterhaltung staatlicher Funktionen wäre (Strauß/Krieger-Lamina 2017; siehe auch Projekt ISIDOR<sup>4</sup>). Es wäre

---

<sup>1</sup> Siehe dazu die Initiative „Digital Austria“ der Bundesregierung:  
[bmdw.gv.at/Themen/Digitalisierung/Strategien/Digital-Austria.html](http://bmdw.gv.at/Themen/Digitalisierung/Strategien/Digital-Austria.html).

<sup>2</sup> [futurezone.at/netzpolitik/von-breitband-bis-egovernment-das-plant-die-regierung/302.588.659](http://futurezone.at/netzpolitik/von-breitband-bis-egovernment-das-plant-die-regierung/302.588.659).

<sup>3</sup> Vgl. etwa [derstandard.at/2000078770407/IT-Blamage-Chat-des-Bundeskanzleramts-war-fuer-jeden-zugaenglich](http://derstandard.at/2000078770407/IT-Blamage-Chat-des-Bundeskanzleramts-war-fuer-jeden-zugaenglich).

<sup>4</sup> [oeaw.ac.at/ita/projekte/isidor-was-geht-ohne-internet](http://oeaw.ac.at/ita/projekte/isidor-was-geht-ohne-internet).

für den Staat zweckmäßig, sich auf den möglichen Ausfall dieser wichtigen Funktionen vorzubereiten und Überlegungen anzustellen, wie die Souveränität im Sinne von Kontrolle über hoheitliche Infrastrukturen aufrechterhalten werden könnte (siehe auch Nentwich et al. 2019; Jäger et al. 2022).

Digitale Souveränität ist längst auf der EU-Ebene angekommen (Floridi 2020): Der EU-Rat<sup>5</sup> erörtert diese Herausforderung im Rahmen der Digitalen Agenda, die EU-Kommission verweist darauf unter dem Stichwort „digitale Resilienz“ in ihrer jüngsten Kommunikation zur Digitalen Dekade.<sup>6</sup> Die Bedeutung des Themas wurde in Österreich von mehreren Einrichtungen erkannt, so vom Rat für Forschung und Technologieentwicklung (RFTE 2021). Der Internet Summit Austria 2022, organisiert von den Internet Service Providers Austria (ISPA), widmete sich diesem Thema.<sup>7</sup> Das BMF hat die einschlägigen Kompetenzen vom ehemaligen BMDW übernommen und betreibt u. a. die Taskforce Digitale Kompetenzen.<sup>8</sup> Auch von einzelnen ParlamentarierInnen wird das Thema forciert.<sup>9</sup>

## Zitierte Quellen

- BITKOM (2015), Digitale Souveränität. Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa, abgedruckt in: *Datenschutz und Datensicherheit* 2018 (5), 294-300.
- Floridi, L. (2020), The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU, *Philosophy & Technology* 33, 369-378.
- Jäger, W. et al. (2022), Digitale Souveränität und politische Prozesse, in: Bogner, A. et al. (Hg.): *Digitalisierung und die Zukunft der Demokratie*, Berlin: Nomos, 189-204, [nomos-elibrary.de/10.5771/9783748928928-189.pdf?download\\_chapter\\_pdf=1&page=1](https://nomos-elibrary.de/10.5771/9783748928928-189.pdf?download_chapter_pdf=1&page=1).
- Müller Quade, J., et al. (2018), Karlsruher Thesen zur Digitalen Souveränität Europas, *Datenschutz und Datensicherheit* (5), 277-280.
- Nentwich, M., et al. (2019), *Kann es eine digitale Souveränität Österreichs geben? Herausforderungen für den Staat in Zeiten der Digitalen Transformation*. ITA Manu:scripts Nr. ITA-19-01 [epub.oeaw.ac.at/ita/ita-manuscript/ita\\_19\\_01.pdf](https://epub.oeaw.ac.at/ita/ita-manuscript/ita_19_01.pdf).
- RFTE (2021), 10 Thesen zur Technologiesouveränität, Diskussionsgrundlage, 18. Jänner, Rat für Forschung und Technologieentwicklung: Wien, [rat-fte.at/files/rat-fte-pdf/publikationen/2021/RFTE\\_Neujahrsempfang\\_2021\\_Thesenpapier.pdf](https://rat-fte.at/files/rat-fte-pdf/publikationen/2021/RFTE_Neujahrsempfang_2021_Thesenpapier.pdf).
- Strauß, S., Krieger-Lamina, J. (2017), Digitaler Stillstand: Die Verletzlichkeit der digital vernetzten Gesellschaft – Kritische Infrastrukturen und Systemperspektiven, Projekt-Endbericht, ITA: Wien, [epub.oeaw.ac.at/ita/ita-projektberichte/2017-01.pdf](https://epub.oeaw.ac.at/ita/ita-projektberichte/2017-01.pdf).

<sup>5</sup> [consilium.europa.eu/de/policies/a-digital-future-for-europe/](https://consilium.europa.eu/de/policies/a-digital-future-for-europe/).

<sup>6</sup> [ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030\\_de](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_de).

<sup>7</sup> [ispa.at/news-events/internet-summit-austria/](https://ispa.at/news-events/internet-summit-austria/).

<sup>8</sup> [bmf.gv.at/themen/digitalisierung/](https://bmf.gv.at/themen/digitalisierung/).

<sup>9</sup> Siehe zwei SPÖ-Anträge 2020 ([parlament.gv.at/PAKT/VHG/XXVII/A/A\\_01154/](https://parlament.gv.at/PAKT/VHG/XXVII/A/A_01154/)) und 2021 ([parlament.gv.at/PAKT/VHG/XXVII/A/A\\_01984/](https://parlament.gv.at/PAKT/VHG/XXVII/A/A_01984/)).