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: 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.[41]

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[42]) 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). Es wäre für den Staat zweckmäßig, sich auf den möglichen Ausfall dieser wichtigen Funktionen vorzubereiten und Überlegungen anzustellen, wie die Souve-

[41] futurezone.at/netzpolitik/von-breitband-bis-egovernment-das-plant-die-regierung/302.588.659.

[42] Vgl. etwa derstandard.at/2000078770407/IT-Blamage-Chat-des-Bundeskanzleramts-war-fuer-jeden-zugaenglich.

ränität im Sinne von Kontrolle über hoheitliche Infrastrukturen aufrechterhalten werden könnte.

Zitierte Quellen

BITKOM (2015), Digitale Souveränität. Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa, abgedruckt in: Datenschutz und Datensicherheit 2018 (5), 294-300.

Müller Quade, J., Beyerer, J. und Reussner, R. H., 2018, Karlsruher Thesen zur Digitalen Souveränität Europas, Datenschutz und Datensicherheit (5), 277-280.

Strauß, Stefan, Krieger-Lamina, Jaro (2017): Digitaler Stillstand: Die Verletzlichkeit der digital vernetzten Gesellschaft – Kritische Infrastrukturen und Systemperspektiven, Projekt-Endbericht, Institut für Technikfolgen-Abschätzung: Wien, epub.oeaw.ac.at/ita/ita-projektberichte/2017-01.pdf .

(MN)