

Digitale Souveränität



Mit der Entdeckung der Digitalisierung durch die Politik hat der Begriff der „Digitalen Souveränität“ in die Diskussion Einzug gehalten. Verstanden wird darunter nicht immer dasselbe – aber das hat vielleicht mehr mit der Vielschichtigkeit des Problems als mit der Uneindeutigkeit der Begrifflichkeit zu tun.

Subsumiert wird darunter zunächst, wie schon im Positionspapier des Bitkom „Digitale Souveränität – Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa“ aus dem Jahr 2015 betont, aus der Perspektive der Anbieterseite die regulatorische Chancengleichheit europäischer IT-Unternehmen durch einheitliche Gesetzgebung einerseits und die gezielte Forschungsförderung von Digitaltechnik andererseits. Darüber hinaus wird auch über die Schaffung „europäischer Champions“ als Gegengewicht zu der schieren Übermacht der erfolgreichen Plattformen amerikanischer Hersteller diskutiert – wenn auch eine Marktdurchsetzung ohne eine technische Marktabschottung wie in China mit jedem Tag unwahrscheinlicher erscheint.

Aber auch auf der Nutzerseite ist Digitale Souveränität von Bedeutung. Darunter wird ein selbstbestimmter und aufgeklärter Umgang mit digitaler Technik verstanden – wohl wissend, dass auch hier möglicherweise regulatorische Eingriffe erforderlich sind, um z. B. dem „Lock-In“-Effekt entgegenzuwirken, der bei (so genannten) „Sozialen Netzwerken“ Anbieter vom Markt verdrängt, denen es nicht gelingt, die Mehrheit der Nutzer um sich zu scharen. Denn wenn es keine echten Alternativen zu einem Anbieter gibt, dann gibt es auch keine echte Wahlfreiheit für den Nutzer. Immerhin hat die Datenschutz-Grundverordnung mit der Forderung von Datenportabilität erste Schritte in diese Richtung unternommen.

Schließlich erfordert Souveränität auch Kompetenz und Verständnis – nur ein im vollen Wortsinne „aufgeklärter“ Kunde, der sich über den Preis und die Risiken einer Nutzung im Klaren ist und seine Gestaltungsmöglichkeiten (z. B. durch die Konfiguration von Anwendungen und Apps) kennt, kann mit digitaler Technik in vollem Umfang selbstbestimmt umgehen.

Auch hier sind die Anbieter gefordert: *Security by Design* und *Privacy by Default* müssen in den Lösungen auch umgesetzt sein – von der automatischen Verschlüsselung bis zur Möglichkeit, Datensparsamkeit (möglicherweise auch unter Verzicht auf bestimmte Dienstqualitäten) zu konfigurieren. Das beleuchtet das *Thesenpapier der Karlsruher Forschungseinrichtungen zur digitalen Souveränität* KIT, FZI und IOSB. Dazu sind Anforderungen an den Softwareentwicklungsprozess zu stellen, wie *Andreas Diepenbrock* und *Sabine Sachweh* in ihrem Beitrag ausführen. Möglicherweise benötigen wir auch ein Zertifizierungsverfahren, über das der Nachweis der entsprechenden Eignung einer Lösung für einen souveränen Nutzerumgang geführt werden kann – ein Vorschlag, der von *Timon Hackenjos*, *Jeremias Mechler* und *Jochen Rill* diskutiert wird. Und schließlich wird man die Hardwareentwicklung und weitere Elemente der „IT-Wertschöpfungskette“ nicht ausklammern können, denn auch hier kann Digitale Souveränität ihre Grenzen finden, wie *Arnd Weber*, *Steffen Reith*, *Michael Kasper*, *Dirk Kuhlmann*, *Jean-Pierre Seifert* und *Christoph Krauß* in ihrem Beitrag ausführen.

Die Diskussion – und die regulatorische Umsetzung – Digitaler Souveränität haben gerade erst begonnen. Auch dies ist, aller Digitalisierungserfahrung zum Trotz, noch Neuland.

Dirk Fox