

Digitale Souveränität braucht Infrastruktur

GASTKOMMENTAR

von CHRISTOPH EBELL

Über digitale Souveränität wird in der Schweiz wie in Europa vor allem als politische oder regulatorische Frage diskutiert. Im Zentrum stehen Datenschutz, Governance-Modelle, Zertifizierungen und nationale Cloud-Strategien. Diese Debatte ist notwendig, bleibt aber unvollständig. Im Zeitalter grossskaliger künstlicher Intelligenz entscheidet sich Souveränität immer weniger auf der Ebene von Regeln. Sie ist heute vor allem eine Frage der Infrastruktur, es geht um Netzwerke, Energieversorgung und Industriekapazitäten.

Der Wandel ist offensichtlich. Während sich frühere Digitalisierungsdebatten um Software und Datenflüsse drehten, rückt mit KI die Rechenleistung ins Zentrum. Das Training grosser Modelle, sicherheitskritische Anwendungen in Verwaltung und Industrie erfordern hochintegrierte Rechenzentren mit spezialisierter Hardware und hohem Energiebedarf.

Operativ lässt sich digitale Souveränität auf drei Voraussetzungen reduzieren. Erstens sind Zugriff und Kontrollierbarkeit der Recheninfrastruktur zentral. Wer betreibt die Systeme? Wer entscheidet bei Knappheit? Juristische Zuständigkeit allein genügt nicht, wenn operative Kontrolle fehlt. Zweitens braucht es krisenfestе Lieferketten. KI materialisiert sich in Halbleitern, Netzwerktechnik und Firmware. Europa ist hier strukturell abhängig. Souveränität bedeutet unter solchen Voraussetzungen nicht eine

Grossskalige KI-Rechenzentren sind kapitalintensiv, langfristig aufzugleisen und politisch relevant.

in ferner Zukunft vielleicht erreichte Selbstversorgung. Stattdessen sind Diversifikation und Resilienz gefragt. Drittens geht nichts ohne verlässliche Energieversorgung. Wo der Strom fehlt – oder seine Preisstabilität nicht gesichert ist –, wandert die Rechenleistung ab. Rechenzentren, Glasfasertrassen und Energieanschlüsse sind die Verkehrsachsen der digitalen Wirtschaft. Ohne sie bleiben formale Nachweise («trusted clouds») und strategische Programme letztlich wirkungslos.

Initiativen wie die «Swiss Government Cloud» sind konsequent. Mit ihr will das Bundesamt für Informatik und Telekommunikation eine neue Cloud-Infrastruktur aufbauen, die auf die Anforderungen und Bedürfnisse des Bundes zugeschnitten ist. Die Schweiz markiert damit einen politischen Willen zu digitaler Souveränität. Allerdings bleibt bei solchen Initiativen häufig ein entscheidender Punkt offen. Stehen langfristig Rechenleistung und Energie zur Verfügung – und wie werden sie priorisiert, wenn Knappheit herrscht?

Europa beginnt, die neuen Realitäten digitaler Souveränität anzuerkennen. Grossskalige KI-Rechenzentren werden zunehmend als strategische Infrastruktur verstanden. Das ist konsequent. Ihre Logik ähnelt Stromnetzen oder Verkehrsachsen: Sie sind kapitalintensiv, langfristig aufzugleisen und politisch relevant. In Deutschland entstehen neue Grossrechenzentren mit Milliardeninvestitionen, teils durch internationale Anbieter, teils durch europäische Industriegruppen. In der Schweiz hingegen wird bis jetzt häufig auf externe Kapazitäten und ausländisches Kapital gesetzt.

Auch für die Schweiz gilt: Digitale Souveränität lässt sich nicht herbeiregulieren. Sie muss gebaut, finanziert und betrieben werden. Dabei zeigt ein einfaches Gedankenexperiment, ob ein Land auch bei gestörten Datenflüssen kritische Funktionen aufrechterhalten kann. Besteht operativer Zugriff auf Rechenleistung? Sind Energie und Netze vorbereitet? Wo Antworten darauf ausbleiben, wird auch die Souveränität fraglich.