mehr Aktivitäten und Dienstleistungen erfolgen über digitale Wege und ein Ausfall von Systemen kann zumindest temporär zum Ausschluss aus Kommunikation und Nutzung von privaten sowie beruflich erforderlichen Diensten führen. Die Vertrauenswürdigkeit, dass diese nicht manipuliert wurden, wird umso bedeutungsvoller, umso mehr auf digitale Daten gesetzt wird. Die IT-Infrastruktur von Staat und Wirtschaft kann sowohl das Ziel feindlicher Attacken (Terrorismus, kriegerische Aktivitäten, externe politische Einflussnahme) als auch von Wirtschaftskriminalität (Identitätsdiebstahl etc., um sich fremden Besitz anzueignen) werden. Sie vor solchen Szenarien zu schützen, ist daher sowohl auf der Makroebene für den Staat, als auch auf der Mesoebene für Unternehmen und Vereinigungen, sowie auf der Mikroebene für die individuellen Bürger*innen sinnvoll.

Von einer derzeit nationalstaatlich organisierten Welt ausgehend, in der nur einzelne Themenfelder durch globale Institutionen und meist auf hohem Abstraktionsniveau reguliert sind, ist zu beobachten, dass die Bedürfnisse der Nutzer*innen digitaler Infrastrukturen realistisch nur von den Nationalstaaten oder institutionell dicht verfassten Regionalorganisationen abgesichert werden können. Einerseits unterscheiden sich die Interessen der beteiligten Unternehmen je nach Profitakkumulierungsstrategie, andererseits sind auch die Bedürfnisse der Bürger*innen abhängig von den jeweiligen Diskursen. Daher verwundert es nicht, dass auch die softwareseitigen Angebote regional variieren und beispielsweise auf Datenschutzinteressen unterschiedlich passend eingehen. Diskussionen beispielsweise in der EU über Ansätze zur Datenlokalisierung im EU-Raum verweisen auf die häufig anzutreffende Überzeugung, dass eigene wirtschaftliche und fachliche Kompetenzen Voraussetzung seien, diesen verschiedenen Interessen gerecht zu werden *(vgl. Pohle/Thiel 2019: 72)*. Damit einher geht die bereits angesprochene wirtschaftliche Stabilität als eines der Elemente des aktuellen Diskurses um digitale Souveränität. Soll die Umsetzung innerhalb eines politischen Systems ausgehandelter Standards nicht von Akteuren außerhalb der eigenen politischen Sphäre abhängig sein, müssen entsprechende Kapazitäten in der eigenen Region und von dort verankerten Institutionen geschaffen werden.

Regelungen zur Stärkung von Nutzer*innenrechten einschließlich der Gewährleistung von Datenschutz sind möglich, wie die Einführung der Europäischen Datenschutz-Grundverordnung von 2018 zeigte. Auch an den technischen Möglichkeiten einer Umsetzung besteht kein Zweifel – dies zeigen Anpassungen beispielsweise in gängigen Browsern oder auch bei der Konfigurationsfähigkeit von Webdiensten hinsichtlich der verwendeten Trackingdienste. Dass einige Unternehmen dadurch weniger Profit machen, steht außer Frage, aber offensichtlich können diese trotzdem wirtschaftlich arbeiten, und auch unabhängig davon könnte normativ argumentiert werden, dass es keinen Rechtsanspruch auf Profitmaximierungsmodelle gibt, die auf massivem Eingriff in die Grundrechte der Bürger*innen basieren. Selbstbestimmungsfähigkeit kann durch die Förderung der digitalen Kompetenzen der Nutzer*innen und durch eine rechtliche Verankerung ihres Anspruchs auf Dienste, die eine Adaption an ihre Bedürfnisse ermöglichen, hergestellt werden *(vgl. Goldacker 2017: 7 ff.)*. Dass auch kritische IT-Infrastruktur durch restriktivere Regelungen geschützt werden kann, zeigen die auf dem niedrigeren Niveau von Alltagsanwendungen und Unternehmenssoftware implementierten Sicherheitsmerkmale sowie die Existenz solcher Regelungen für konventionelle Teile der kritischen Infrastruktur. Problematischer erscheint die Möglichkeit des Aspekts wirtschaftlicher Stabilität: Offensichtlich ist diese sehr voraussetzungsreich, da sie vermutlich eine hohe Wirtschaftskraft der betreffenden Gesellschaft erfordert, um sich Produktions- und Bereitstellungsinfrastrukturen sowie hochspezialisierte Fachkräfte leisten zu können. Möglicherweise ist dies ein Kriterium, das nur für wirtschaftlich starke Gesellschaften erreichbar ist.

Offensichtlich ist digitale Souveränität, wie hier definiert, sinnvoll. Ob sie auch möglich ist, umfasst eine Reihe an Voraussetzungen, von denen die Wirtschaftskraft einer Gesellschaft womöglich die problematischste ist. Zumindest für westliche Demokratien, wie die der BRD oder auch im Rahmen der Europäischen Union, kann die Frage nach der Möglichkeit digitaler Souveränität bejaht werden. Beide erörterte Aspekte haben allerdings theoretischen Charakter, weswegen in der praktischen Umsetzung immer auch Herausforderungen zu erwarten sind. Da digitale Souveränität aber sinnvoll und möglich erscheint, kann durchaus von der Politik gefordert werden, dass sie sich um deren möglichst optimale Umsetzung bemüht.

Fußnoten

1 - Die These könnte durch ein einziges Gegenbeispiel, bei dem es nicht gelingt, den Fähigkeiten bzw. Möglichkeiten eines Individuums (oder Personengruppe) gerecht zu werden, widerlegt werden.

Literaturangaben zu den im Text referenzierten Veröffentlichungen finden sich in der Onlinefassung des Artikels auf der Internetseite des grünen blatts.