Digitale Souveränität: Die Selbstbestimmung im Wandel

Know-how Die Digitalisierung hat die gesellschaftlichen Strukturen in kürzester Zeit stärker verändert als seinerzeit die industrielle Revolution. Neben enormen Chancen haben sich jedoch auch Herausforderungen ergeben. Ein Einordnungsversuch als Denkanstoss.

Von Thierry Kramis

Digitale Souveränität zu definieren, ist eine Herausforderung. Vielleicht hat es damit zu tun, dass bis jetzt zu wenig darüber diskutiert wurde. Spätestens im Gespräch zum Thema merkt man, wie breit das Spielfeld ist, das sich hier eröffnet. Die Antworten zur Frage, was denn digitale Souveränität genau ist, fokussieren im Allgemeinen zuallererst auf die eigene Persönlichkeit und den Schutz eigener Daten. Doch das scheint zu kurz zu greifen. Denn digitale Souveränität hat gemeinhin verschiedene relevante Ebenen, die im Nachgang skizziert werden. Was bei jedem selbst als datenschutzzentrische Betrachtung beginnt, endet beim Staat und der Fähigkeit, souverän zu agieren. Doch damit ein Staat souverän agieren kann, braucht es Handlungsfreiheiten, erlangt durch Kompetenz, und es braucht eine demokratische Kontrolle. Das ist in der Betrachtung von digitaler Souveränität nicht unerheblich. Die Wirtschaft, so scheint es, steht überdies oft in einem Zielkonflikt mit der gesellschaftlichen Betrachtungsweise. Deswegen wird Regulierung hier oft auch als Verhinderung angesehen. Das ist so zu kurzsichtig: Im Kern stehen unsere gesellschaftlichen Werte. Sie gilt es zu berücksichtigen, gegebenenfalls weiterzuentwickeln.

Der Datenschutz im Fokus

Beginnen wir mit der Betrachtung digitaler Souveränität im Rahmen des Individuums. In diesem Rahmen versteht sie sich am ehesten als selbstbestimmte Nutzung der digitalen Infrastruktur und der Entscheidungshoheit darüber, welchen Schutz die eigenen digitalen Daten geniessen sollten. Den Menschen ist heute klar, dass die Nutzung digitaler Dienstleistungen eine Exposition der persönlichen Daten zur Folge hat und auch die Kontrolle der Verarbeitung dieser Daten schwierig geworden ist. Eine automatisierte Datenanalyse beispielsweise ist gängige Praxis der grossen Tech-Konzerne. Dies ist mit der bisher bekannten Wertehaltung aus der realen Welt kaum vereinbar. Wir leben also in einer Welt kommerzialisierter Daten. Entsprechend haben sich im Rahmen digitaler Souveränität des Individuums zwei Kernziele für den Schutz der eigenen Daten etabliert: Die Verschlüsselung, ohne Möglichkeit der Nutzung durch Dritte, und die Fähigkeit, die Datenverarbeitung durch Unternehmen zu kontrollieren. Damit fällt die heutige Sicht des Einzelnen auf digitale Souveränität sehr Datenschutz-zentrisch aus. Dies gilt zumindest für Europa, das tendenziell ein stärker ausgeprägtes Datenschutzverständnis kennt als andere Kontinente.

Im Spannungsfeld zwischen Sicherheit und Innovation

In Sorge um Industriespionage und staatliche Regulierung fokussieren Unternehmen ebenfalls auf Datenschutz. In zweiter Priorität sehen sie den konkreten Bedarf, sich vor Produktionsausfällen zu schützen – beispielsweise infolge von Ransomware oder Phishing-Angriffen. Digitale Souveränität wird demnach im wirtschaftlichen Kontext oft mit der Fähigkeit assoziiert, den Erhalt der eigenen operativen Tätigkeit über technische Sicherheit zu gewährleisten. Nicht zu vergessen ist die Lieferkette: Mit entsprechender Lizenzpolitik beispielsweise können Systeme innert kurzer Zeit zum Stillstand gebracht werden.

Darüber hinaus öffnet sich in der wirtschaftlichen Betrachtung mit dem Thema Innovation ein weiteres grosses Spannungsfeld. Schliesslich gehört sie respektive die Erhaltung der eigenen Wettbewerbsfähigkeit zur Hauptaufgabe von Unternehmen. Hier stellt sich allerdings heraus, dass diese mit bisherigen Mitteln kaum mehr zu erhalten ist. Es braucht oft neue Herangehensweisen, wodurch Themen wie Big Data und Künstliche Intelligenz (KI) zum zentralen Bedürfnis der Unternehmen werden können. Es entstehen bewusst oder unbewusst neue Schnittstellen, Abhängigkeiten und ein enormer Datenhunger im Zielkonflikt einer möglichen Datenschutz-Regulierung. In diesem Kontext sehen Unternehmen den Regulator häufig auch als «Verhinderer von Innovation». Somit ergibt sich für Unternehmen ein Mosaik aus Sicherheit, Regulierung, Fähigkeit zum Betriebserhalt und dem Bedarf nach Innovation. Eine untergeordnete Rolle spielt jedoch die konkrete, selbstbestimmte Nutzung von IT-Systemen.

Eine riesige Herausforderung für Staaten

Vom Staat wird derweil erwartet, dass er sich um Bürger, Wirtschaft – insbesondere auch um deren Wettbewerbsfähigkeit –

Die individuelle digitale Souveränität wird heute durch zwei Faktoren geschützt: Verschlüsselung und die Kontrolle von Datenverarbeitungen durch Unternehmen.

Depositphotos.com

und Souveränität im Allgemeinen kümmert. Das ist eine riesige Herausforderung. All das kann ein Staat jedoch nur unter Wahrung von Souveränität leisten – und zwar in der realen und digitalen Welt gleichermassen. Dies bedingt jedoch eine demokratische Kontrollfähigkeit. Prozesse, welche die Bevölkerung in der Regel nicht hinterfragt. Doch gerade in der digitalen Welt sind diese elementaren Grundpfeiler nicht selbstverständlich.

Im Zentrum steht, ob ein territorial souverän agierender Staat auch digital befähigt ist, entsprechend zu agieren und welche rechtliche Durchsetzungsfähigkeit er (faktisch) überhaupt ausüben kann. Es ist sogar zentral die Frage zu stellen, ob digitale Souveränität eine territoriale Souveränität überhaupt erst ermöglicht. Denn das Digitale ist heute kein Zusatz mehr zur realen Welt. Vielmehr ist es ein kritischer Grundpfeiler eben dieser. Diese Frage kann allerdings nicht ohne eine Demokratie-politische Diskussion beantwortet werden.

Globalisierung und Digitalisierung stellen Souveränität infrage

Die rechtliche Durchsetzungsfähigkeit eines einzelnen Staates muss in einer globalisierten, digitalisierten Welt allerdings infrage gestellt werden. Denn gerade in Europa ist die digitale Souveränität (nicht einmal primär das digitale Wissen) faktisch kaum gegeben. Im Wesentlichen ist die europäische Gesellschaft heute abhängig von zwei grösseren Blöcken: China liefert den grössten Teil der Hardware, die USA den grössten Teil der Software. In Anbetracht dieser Tatsache haben sich logischerweise europäische Tendenzen ergeben, die Digitalisierung zu regulieren. Während in Deutschland der Datenschutz und dessen Regulierung ein sehr hohes Gewicht haben, forciert Frankreich die europäische Bereitstellung von Cloud Services. Aus globaler Perspektive ist das durchaus problematisch: Reguliert ein Nationalstaat den digitalen Raum selbst, so führt das zu einer starken Fragmentierung der Gesetzgebung und damit automatisch zur Frage der Durchsetzbarkeit dieser Gesetzgebung in einem globalen Kontext. Der Markt eines Staates ist vermutlich zu klein, um für ein global agierendes Unternehmen von Relevanz zu sein. Ein solches könnte folgerichtig entscheiden, sich aus dem einen Markt zurückzuziehen. Dies wäre für die Innovationskraft und die Wettbewerbsfähigkeit unter Umständen fatal. Faktisch wäre der Nationalstaat also nur theoretisch befähigt, eine Regulierung herbeizuführen. Ein fatales Statement für demokratische Kontrollprozesse.

Nehmen wir die Schweiz als Beispiel, mit einem Markt von knapp neun Millionen Einwohnern. Im Vergleich dazu verfügt die USA über einen Markt von circa 330 Millionen, Europa über einen solchen von 746 Millionen und China über einen von 1,4 Milliarden Menschen. Aufgrund dessen dürfte es einer supranationalen Organisation wie der EU deutlich einfacher fallen, eine Regulierung durchzusetzen, als einem Staat wie der Schweiz. Denn wer würde auf einen Markt von 746 Millionen Nutzern verzichten? Facebook hat in früheren Diskussionen beispielsweise bereits kundgetan, dass das nicht von Interesse wäre.

Von Autarkie bis zur vollständigen Abhängigkeit

Um als Staat souverän zu agieren, braucht es trotzdem ein Mindestmass an digitaler Souveränität. Das heisst ein Mindestmass an Fähigkeit, und vor allem die damit verbundene Kompetenz, digitale Systeme autonom aufrecht zu erhalten. Dabei ist klar, dass es genauso falsch wäre, eine weitgehende Autarkie anzustreben, wie sich in komplette Abhängigkeit Dritter zu geben.

Auch hier lohnt sich ein Blick auf die beiden Extrempole: Staaten wie China und Russland streben nach sehr starker Autarkie und haben sogar begonnen, ihre Datenverbindungen vom Rest der Welt abzukoppeln. Damit geht die Fähigkeit einher, die eigene Infrastruktur autark betreiben zu können. Während diese Staaten dies aus totalitären Tendenzen tun, gibt es solche Bemühungen durchaus auch in Europa (z.B. das Schengen-Routing), hier jedoch aus anderen Beweggründen. Vor- und Nachteile solcher Überlegungen müssen gut abgewogen wer-

den. Insbesondere das Schengen-Routing wird häufig als wenig zielführend zurückgewiesen.

Auf der anderen Seite steht die völlige digitale Abhängigkeit. Die Ära Trump zeigte etwa relativ klar, dass sich Interessen sehr schnell und sehr unilateral ändern können, was bilaterale Abkommen so schwierig macht. Obwohl solche unilateralen Entwicklungen im Grundsatz zurückzuweisen sind, so sind sie dennoch oft unveränderbare Realität. Per Sanktion untersagte die USA beispielsweise – obgleich nur für kurze Zeit – die Nutzung sämtlicher Adobe Services in Venezuela und spricht sich mittlerweile sogar für Exportbeschränkungen von hochmodernen Halbleitern nach China aus. Im Verlaufe des Ukraine-Kriegs wurde ausserdem deutlich, wie stark Staaten von globaler Infrastruktur abhängig sind: Innert Tagen und Wochen war Russland vom internationalen Zahlungstransfer, von Kreditkartenzahlungen und von Lieferungen technologischer Produkte weitestgehend abgeschnitten.

Obwohl diese Massnahmen aus Sicht des europäischen Betrachters nachvollziehbar sind, so führen sie dennoch vor Augen, warum die Diskussion zu digitaler Souveränität so elementar geworden ist. Unter dem Strich geht es darum, die eigene Souveränität mit Partnerschaften auf Augenhöhe zu stärken, langfristig stabil zu agieren, offene Schnittstellen zu fördern und lokale Kompetenz aufzubauen respektive weiterzuentwickeln.

Kompetenzen für die digitale Souveränität

In der Europäischen Union gibt es Bestrebungen, die zentralen Bausteine digitaler Infrastruktur als eigene Kompetenz zu etablieren. Hierzu gehören etwa die Fähigkeit zur Bereitstellung einer eigenen Cloud-Infrastruktur, Kompetenzen im Bereich Big Data und KI, aber auch unabhängigere Zahlungssysteme sowie eigene Datenräume. Themen, die durch US-amerikanische Unternehmen bereits ausführlich bearbeitet werden. Man kann darüber diskutieren, ob es Sinn macht, diese Kompetenz in Europa selbständig aufzubauen. Unabhängig von der konkreten Antwort steht die Bildung und auch die digitale Wissenschaft am Anfang des Kompetenzaufbaus. Beide sind im europäischen Raum sehr stark staatlich gelenkte Themen. Man spricht daher oft auch von einer «engen Verzahnung von digitaler Bildung und digitaler Souveränität». Dabei sind weder technologische Bildung noch Medienkompetenz in sich ausreichend, vielmehr sind vielschichtige Kompetenzen erforderlich.

Insbesondere die wissenschaftliche Forschung braucht in diesem Kontext eine enorme, ständig zunehmende Menge von Daten. Dabei wird offensichtlich, dass eine einzige Organisation – sei dies eine Forschungseinrichtung, ein Unternehmen oder sogar der Staat – nicht über eine zureichende Menge an entsprechenden Daten verfügen kann. Im Rahmen von Big Data verfügen heute nur global agierende Firmen wie Google über einen entsprechenden Ressourcenpool. Es gibt denn auch staatliche Bemühungen zur Demokratisierung solcher Daten im Sinne von Open Data. Daten sollen möglichst allgemein zugänglich sein und über Datenräume entsprechende Kooperationen gefördert werden.

Was Open Source und Blockchain verbindet

Nicht zuletzt drängt sich in Zusammenhang mit digitaler Souveränität, gerade auf staatlicher Ebene, oftmals auch die Frage auf, ob proprietäre Software ein Problem darstellt. Und in der Tat muss wohl nüchtern festgehalten werden, dass die Nachvollziehbarkeit von proprietärer Software – insbesondere im Bereich Datennutzung – doch einige Hürden mit sich bringt. Interessanterweise setzen viele grosse Tech-Konzerne allesamt auf Open-Source-Technologie als Basis der eigenen Angebote. Sie können es sich nicht leisten, ihr Geschäftsmodell durch Abhängigkeiten von Dritten zu gefährden. Sei dies infolge abgekündigter Schnittstellen oder ständig teurer werdenden Nutzerlizenzen. Solche Hürden können ein Geschäftsmodell zu Fall bringen.

Auch bei staatlichen Akteuren gibt es folgerichtig starke Tendenzen, ausschliesslich auf Open Source zu setzen. Die Argumentation ist dabei simpel: Durch offenen Quelltext kann jeder nachvollziehen, was ein System genau macht. Das Ziel der Blockchain ist letztlich das gleiche: Ein Akteur alleine kann Fakten nicht autonom verändern, die Nachvollziehbarkeit respektive das Vertrauen wird gestärkt. Insofern scheint man mit einer Strategie für offene Software nicht völlig auf dem Holzweg. Auf der anderen Seite ist Dogmatismus per se hier trotzdem unzureichend. Vielmehr gibt es auch im Closed-Source-Bereich in Europa ein enormes Wissen, das man nutzen sollte.

Eine Frage der Werte und Handlungsoptionen

Der Begriff der digitalen Souveränität ist vielschichtig, eine exakte Definition nicht möglich. Eine individualisierte, datenschutzorientierte Betrachtung greift allerdings deutlich zu kurz. Systemsicherheit und Innovationsfähigkeit sind nur zwei von vielen weiteren Puzzlesteinen. Im Grundsatz stellt sich die elementare Frage, wie demokratische Prozesse in einer globalisierten und digitalisierten Welt überhaupt greifen können und welche Kompetenzen selber aufgebaut werden sollten, um Unabhängigkeit zu garantieren. Denn in der heutigen digitalisierten Welt müsste man sonst formulieren: «Der Souverän, wir haben ihn schon lange zu Grabe getragen.» Dies würde zum Umdenken elementarer Grundpfeiler führen, die sich Europa hart erarbeitet hat und die es in die digitalisierte Welt zu übertragen gilt. Denn die reale und die digitale Welt sollten sich nicht zu Paralleluniversen entwickeln. Sie müssen zwingend die gleichen Werte teilen, ansonsten führt dies zu einem enormen Spannungspotential. Welche Entscheidungen auch immer getroffen werden: Es wird Sinn machen, sich dabei jeweils mehr Handlungsoptionen zu sichern als weniger. Das führt oft auch zu besseren Lösungen. ■

DER AUTOR

Thierry Kramis führt den Telekommunikationsanbieter und Managed Service Provider Seabix. Hier verantwortet er die strategische Entwicklung und das Produkteportfolio. Gleichzeitig ist er Gemeindepräsident einer kleinen Luzerner Gemeinde, wo er sich um die digitale Transformation der Service-Bereitstellung und der demokratischen Prozesse bemüht. Seabix betreut KMU und den öffentlichen Sektor in den Bereichen Telekommunikation und Managed IT Services mit einem starken Fokus auf Sicherheit, Schnittstellen und KI-gestützter IT Service-Orchestrierung, die Seabix über die hauseigene Automatisierungsplattform Seabix IO sicherstellt.