Vision Europe | Juli 2020

Digitale Souveränität in der EU

Falk Steiner und Viktoria Grzymek

„Digitale Souveränität“ – ein oft genutzter Begriff in politischen Debatten auf nationaler wie europäischer Ebene. Was ist damit gemeint? Und ist die EU fähig, eigene Werte und Rechtsvorstellungen in der Digitalpolitik durchzusetzen?

Die Debatte um die „Digitale Souveränität“ ist derzeit nicht ausreichend evidenzbasiert. Bislang mangelt es sowohl an Konzepten zur Erkenntnis des tatsächlichen Abhängigkeitsgrades Deutschlands und der EU von Drittstaaten als auch am politischen Willen, diesen zu ermitteln. In Folge fehlt somit auch eine konzeptionelle Antwort auf die Abhängigkeitsproblematik. Dabei befindet sich Europa in einer grundsätzlich besseren Ausgangsposition als noch vor wenigen Monaten – und ist nicht zwingend auf sich allein gestellt.

Dieser Beitrag thematisiert zuerst die Ausgangslage und ihr Zustandekommen, skizziert anschließend Digitale Souveränität als Konzept für die Europäische Union und umreißt einen Ansatz zur Identifikation und Beurteilung von Abhängigkeiten. Im letzten Schritt werden mögliche Ableitungen und Rahmenbedingungen für eine digital souveräner agierende Europäische Union sowie dafür innerhalb der EU zu schaffende Voraussetzungen dargelegt.

Wenn dabei über europäische Kompetenzen und gemeinschaftliche Güter im Kontext der Digitalisierung nachgedacht wird, sind zwei Aspekte als nicht weiter zu erörtern voranzustellen:

1. Europa verfügt bereits heute über einen Digitalen Binnenmarkt, der auch in Corona-Zeiten weiterhin funktioniert.
2. Die einzelnen EU-Mitgliedstaaten für sich sind für jede Ausprägung der Digitalen Souveränität als zu leichtgewichtig zu erachten.

Aus letzterem Punkt folgt auch der Charakter der Digitalen Souveränität als öffentliches Gut, welches notwendigerweise auf der europäischen Ebene angesiedelt ist – lediglich im Rahmen der EU besitzen die Mitgliedstaaten das Markt- und Regulationsgewicht, das eine Ausgestaltung der Digitalisierung nach eigenen Standards und Werten erlaubt.

Gleichzeitig dürften viele Aspekte der Debatte um die Digitale Souveränität auch auf andere Bereiche anwendbar sein, in denen es aus strategischen Gründen dringend geboten scheint, eigene Kapazitäten und Fähigkeiten vorzuhalten oder aufzubauen, Abhängigkeiten neu auszutarieren und einen bewussteren Zustand der Globalisierung herbeizuführen.

Europas Handlungsfähigkeit unter Digitalisierungsdruck

Europa und das Digitale, das war in den vergangenen Jahren oftmals mehr zufälliges Trauerspiel denn gezielte Politik. Es mangelt an Verständnis, an definierten konkreten Zielen, an Fähigkeiten.

Dabei ist die Digitalisierung selbst wesentlich für das, was als europäisch gilt: In teilglobalisierten Gesellschaften und Öffentlichkeiten ist die Technologie die unmittelbar auf unser aller Lebensrealitäten einwirkende Macht – viel unmittelbarer als Gesetze oder Moralvorstellungen, Europäische Verfassungskonvente oder Ministerräte. Technologie wird immer – teils bewusst, teils unbewusst – in den Werten ihrer jeweiligen regionalen Entstehungs- und Einsatzkontexte gedacht, ob es dabei um Privatsphäre, Zulässigkeit oder Unzulässigkeit von Inhalten, die Zugriffsmöglichkeiten für staatliche Akteure oder den Umgang mit dem einzelnen Bürger geht.

In der Digitalisierung sind Technologien und deren jeweilige Anwendung die reale Umsetzung von Wertvorstellungen, von richtig, falsch, wünschenswert, abzulehnen – zum Beispiel, wenn es um die Grenzen der Meinungsfreiheit in der digitalen Öffentlichkeit geht. Werte und Normen im Digitalen verändern durch ihre technologische Implementierung, implizit oder explizit, und durch die Rückwirkung dieser Implementierung das Werteverständnis in Gesellschaften ganz real, was wiederum Niederschlag in zeitgenössischen Wertvorstellungen und der Interpretation des Wertekanons findet.

Charakteristisch für die Digitalisierung ist dabei: Sie erfolgt – was den Westen angeht – weit überwiegend durch private Akteure und ist somit von globalen Vertragsverhältnissen unter Privaten gekennzeichnet, obschon hierfür der Rechtsrahmen zur wirksamen Durchsetzung regelmäßig fehlt. Es gibt keinen nennenswerten öffentlichen Raum im Digitalen, es gibt nur öffentlich zugängliche Bereiche, also Dienstleistungen und Produkte, die meist von Privaten zur Verfügung gestellt werden. Doch zunehmend erwächst Handlungsdruck für die Politik – weshalb sich ein gleichsam eigenständiges wie fast alle anderen Bereiche durchdringendes neues Politikfeld entwickelt hat: die Digitalpolitik.

Digitalpolitik: Kollidierende Welten

Die Digitalpolitik ist ein zweiseitiges Politikfeld. Auf der einen Seite ist ihr Gegenstand das existierende originär Digitale, quasi die Betriebsmittel der digitalen Gesellschaft. Dies sind beispielsweise die digitalen Infrastrukturen wie Breitbandnetze, Mobilfunknetze, Knotenpunkte, Rechenzentren und digitale Dienstleistungen und deren Sicherheit, aber auch die politisch-rechtlichen, wirtschaftlichen und gesellschaftlichen Ordnungsmechanismen, technologisch-architektonischen Rahmenbedingungen und die impliziten normativen Annahmen, die sich in der (zumeist westlich geprägten) Erschaffung von digitalen Produkten und Dienstleistungen entwickeln.

Auf der anderen Seite umfasst die Digitalpolitik auch jene Bereiche, die sich maßgeblich durch die Digitalisierung verändern – wodurch eben diese Veränderung zum Gegenstand der Digitalpolitik wird. Dies fängt an bei Immaterialgütern wie den klassischen Intellectual Property Rights oder der Wettbewerbspolitik, geht über die Frage der Rechtsdurchsetzung im digitalen Raum beispielsweise bei nach nationalstaatlichen Kriterien illegalen Inhalten, den Umgang mit neu entstehenden Abhängigkeiten in der Digitalisierung bei (teil-)autonomen Fahrzeugen oder in der Landwirtschaft bis hin zur Grundsatzfrage, wie eine adäquate

Steuer- und Abgabenerhebung bei hochautomatisierter Wertschöpfung politisch, rechtlich und sozial geboten und möglich ist.

Beide Bereiche sind eng miteinander verwoben, leiden aber unter zwei kollidierenden Perspektivproblemen: Während das originär Digitale sich in den vergangenen fast 50 Jahren als eigenständiger Bereich unter weitgehender Nichtbeachtung älterer etablierter Modelle staatlicher Regulierung und zwischenstaatlicher Koordination entwickelt hat, sind die sich digitalisierenden Bereiche in ihren jeweiligen Kontexten verhaftet, die dann regelmäßig mit einer gewissen Wucht von Teilaspekten der Digitalisierung und neuen Akteuren getroffen werden. Dies lässt sich in den vergangenen 25 Jahren am Beispiel des Versandhandels (Amazon und AliBaba Express vs. Neckermann, Quelle), der Musikindustrie (Streaming und MP3 vs. Single-CDs), der Fernsehsender (Netflix vs. ProSieben), der neuen Mobilitätsanbieter (Uber und Lyft vs. Taxigewerbe), der Vermietung von temporären Büroräumen (WeWork vs. Regus), Essenslieferdiensten (Lieferando vs. Call-a-Pizza), der Wissensorganisation (Brockhaus und Encyclopedia Britannica vs. Wikipedia) bis hin zu Rolle und Aufgabe der Telekommunikationsunternehmen (WhatsApp vs. SMS) und vielen anderen Beispielen exemplarisch aufzeigen.

Räumt man das Wortgeklingel von der Disruption beiseite, bleiben dennoch massive strukturelle Veränderungen ganzer Branchen und enorme Veränderungen an Geschäftsmodellen und Wertschöpfungsketten, die nicht zuletzt auf den beiden Faktoren Skalierung und Netzwerkeffekten (bis hin zu natürlichen Monopolen) auf allen technologisch, wirtschaftlich und kulturell erschließbaren Märkten beruhen. Doch die Voraussetzungen für diese Erschließung sind, auch durch die Herkunft der Akteure bedingt, überaus unterschiedlich – und das hat nicht zuletzt politische Gründe.

Digitalpolitik als staatliches Betätigungsfeld

USA: Die Welt als Markt für Technologie und Liberalismus

In den USA wurde die strategische Relevanz des Digitalen politisch früh erkannt, gefördert und in logischer Folge der Telekommunikationsmarktderegulierung in erster Linie als Vehikel einer globalen Verbreitung der liberalen Weltordnung und einer entsprechenden Weltwirtschaftsordnung verstanden – z. B. durch den damaligen US-Vizepräsidenten Al Gore, der in den 1990ern strategische Digitalpolitik betrieb. Bis heute hat sich die grundsätzliche Haltung zur Digitalisierung als positiver Gestaltungsmöglichkeit trotz wechselnder Präsidentschaften kaum verändert. In den USA gab es zudem eine lange Tradition der Förderung von Technologieentwicklung und -nutzung zwischen privaten und wissenschaftlichen Akteuren auf der einen und der militärischen bzw. der nachrichten- und geheimdienstlichen Community auf der anderen Seite. Die Nähe zwischen diesen Bereichen ist in Teilen Europas nicht gleichermaßen selbstverständlich, mitunter sogar ausdrücklich unerwünscht. Die USA fokussierten sich auf drei wesentliche politisch-strategische Bereiche: (1) Schaffen eines attraktiven Innovationsumfeldes mit adäquaten Kapitalisierungsmöglichkeiten innerhalb der USA, (2) Offenhalten von Märkten im Zuge internationaler Verträge bei (3) gleichzeitiger Verpflichtung zur Absicherung möglichst jeder Art von geistigem Eigentum und größtmöglicher Cybersicherheit, offensiv wie defensiv.

China: Der Staat regelt für den Binnenmarkt

In China wurden die ersten Jahre der vernetzten Digitalisierung weitgehend verschlafen. In den 2000er Jahren setzte im Zuge der fortschreitenden Industrialisierung jedoch ein deutliches Umdenken ein: Während Festlandchina erst zur Technologie-Produktionsstätte wurde, vor allem hochwillkommener US-amerikanischer und taiwanischer Unternehmen aus dem Halbleitersegment, wurde dies vom Aufbau eigener Fähigkeiten begleitet. Hierbei spielt eine spezifische Technologieaufgeschlossenheit in der chinesischen Politik eine große Rolle: Die Kommunistische Partei Chinas (KPC) hatte erkannt, dass das Wachstum in klassisch industriellen Bereichen endlich ist und die Vorsprünge anderer groß sind. Allerdings

bot die sich abzeichnende Digitalisierung hierbei gleich zwei Chancen. Zum einen die erweiterten Kontroll- und Steuerungsmöglichkeiten nach innen, zum anderen die gezielte Wirtschaftsförderung.

China hatte bereits ab 1997 begonnen, Internetverbindungen aus der Volksrepublik zu überwachen, der Zensur (2003 „Goldenes Schutzschild“) zuzuführen und im Ergebnis über die Great Firewall of China die Abtrennung des chinesischen Netzes betrieben. Zusammen mit den strikten Vorgaben für ausländische Direktinvestitionen, die in den meisten Fällen nur jenen Firmen Marktzugang erlaubten, die mit chinesischen Partnern Joint Ventures bildeten, sicherte die Volksrepublik wesentliche eigene Interessen. Oft verließen die ausländischen Partner den schwierigen Markt nach einiger Zeit, nachdem die ungleichen Bedingungen zum Vorteil der chinesischen Beteiligten ausgenutzt wurden.[1]

China wurde parallel durch die steigende Kaufkraft der eigenen Bürger ein immer attraktiverer Markt und profitierte in hohem Maß von dem Kompetenzaufbau und dem Zugang zu Technologien aus anderen Staaten und förderte das eigene Digitalökosystem zudem auch staatlicherseits massiv: die Ideologie der KPC begreift Technologie als Chance zur Durchsetzung der spezifisch interpretierten Gemeinwohlinteressen und hat in Testregionen immer wieder Realexperimente zur Bevölkerungsüberwachung und -steuerung eingeräumt.

Diese Kombination aus abgeschotteter Öffentlichkeit, abgeschottetem Markt, massiven Forschungsinvestitionen und staatlicher Förderung wurde in den vergangenen Jahren zudem durch gezielte Exportpolitiken unterstützt. Die Intransparenz chinesischer Staatsbeihilfen führt nach wie vor zu globalen Verzerrungen, zudem exportiert China massiv Technologien als Gesamtpaket im Zuge seiner globalen Aktivitäten in Drittstaaten und erzeugt dort strukturelle Abhängigkeiten von chinesischen Anbietern.

Europa: Zögerlich, doch langsam aufwachend

In der EU wurde die Reichweite der digitalen Entwicklungen massiv unterschätzt, vor allem die Mitgliedstaaten sahen sich mit nationalen Erfolgen und Strategien nach ersten Rahmensetzungen in den 1990er und behutsamen Anpassungen in den Jahren danach ausreichend gerüstet, um im Kielwasser der US-dominierten Entwicklungen in Richtung Informationsgesellschaft zu segeln.

Und lange Zeit schien das durchaus auch gut zu gehen: Immerhin erzielte Nokia noch 2007 einen Anteil von fast 50 Prozent am globalen Mobiltelefon-Markt, primär bedroht vom kanadischen Hersteller Research in Motion und seinen Blackberry-Business-Smartphones. Doch mit Apples iPhone kam ein komplett neuer Typus Mobiltelefone auf und schon zu Beginn 2012 war Nokias Marktanteil auf 7,8 Prozent abgeschmolzen und hat sich seitdem nicht mehr erholt. Aus dem berühmten Nokia-Klingelton, dem „Sound von Marktmacht“, war der Klang des Niedergangs hervorgegangen. Ein Schicksal, das auch andere zeitweilig erfolgreiche Hersteller in diesem Bereich ereilte, von Siemens bis Motorola. Doch auch im deutlich jüngeren Smartphone-Markt zeigt sich die Verlagerung: die eigentlichen Innovationen kamen aus dem nordamerikanischen Raum, gefertigt wurde in der Volksrepublik China und nach einiger Zeit konnten die europäischen Anbieter nicht mehr mithalten – Europa blieb zugleich aber einer der wichtigsten Absatzmärkte.

Die Bemühungen zur Gestaltung der Digitalen Welt in Europa beschränkten sich derweil weiter auf die Frage, ob Veränderung wirklich notwendig sei, ob in diesem Bereich wirklich mehr Europa erforderlich sei, zum Beispiel bei der Frage, ob der Binnenmarkt wirklich ein digitales Äquivalent benötige. Debatten um die ‚richtige‘ Digitalpolitik beschränkten sich maßgeblich auf Fragen der Telekommunikationsmarktregulierung, des Urheberrechts, Cybercrime und zunehmend auch auf Überwachungsmöglichkeiten und ein kontinentaleuropäisches Verständnis von Datenschutz. Doch erst die Empörung und Debatte um die potenziell massiven Zugriffsmöglichkeiten der US-

[1] Diese Bedingungen wurden erst zu Jahresbeginn 2020 und nach immer lauter werdender Kritik etwas gelockert („Foreign Investment Law“), nach wie vor unterliegen Direktinvestitionen in China jedoch einigen ansonsten unüblichen Einschränkungen.

Nachrichtendienste in Folge der Veröffentlichungen auf Basis des Snowden-Archivs führten zu breiteren, grundlegenderen strategischen Überlegungen, inwieweit die Abhängigkeit von Dritten möglicherweise das zulässige und zumutbare Maß überschritten hätten. Dies hatte unmittelbare Folgen für die Fragen, ob und inwieweit eine Schutzpflicht Europas im digitalen Raum über das bloße Territorialprinzip hinausgehend bestehen würde, und ob die existierenden Defizite der Rechtsdurchsetzung behebbar seien.

Grenzüberschreitend: Das Primat des Digitalen?

Wesentliche Akteure der Digitalisierung residieren nicht in den Mitgliedstaaten der EU – was in Folge bedeutet, dass europäisches Recht diesen gegenüber nicht per se durchsetzbar ist:

ABBILDUNG 1: **Akteursklassen**

Akteursklassen		Entität unterliegt EU-Regulierung	Entität weiteren Rechtsregimen unterworfen?
1	Sitz in der EU	Ja	Teilweise
2	Betriebsstätte in der EU	Ja	Ja
3	Geschäftstätigkeit in der EU	Ja	Ja
4	Geschäftstätigkeit außerhalb EU, aber Dienstleister für auch innerhalb EU-Tätige/-Ansässige.	Teilweise	Ja
5	Geschäftstätigkeit außerhalb EU und keine direkte Geschäftsbeziehung zu innerhalb EU Tätigen/Ansässigen.	Nein	Ja

Quelle: Eigene Darstellung. | BertelsmannStiftung

Bereits innerhalb der EU (1,2,3) bestehen erhebliche Unterschiede in der rechtlichen Behandlung von Sachverhalten – und auch das zugrundeliegende Regulierungsregime, zum Beispiel ob präventive oder nachlaufende Konzepte verfolgt werden, kann massiv voneinander abweichen. Der „Digitale Binnenmarkt“ weist nach wie vor erhebliche Uneinheitlichkeit auf – z.B. in der Frage der steuerlichen Behandlung, aber auch in medienregulatorischer Hinsicht.

Grundsätzlich gilt in der EU das Herkunftslandprinzip: das Recht des Hauptsitzlandes eines Unternehmens ist maßgeblich. Allerdings trifft dies nicht uneingeschränkt zu: Sofern Verbraucherverträge geschlossen werden (z. B. über Nutzerkonten und AGB), kommt zwingend europäisches Verbrauchervertragsrecht zur Anwendung – unabhängig vom Sitz des Anbieters. Allerdings ist die Möglichkeit zur Rechtsdurchsetzung in vielen Fällen rein praktisch nicht gegeben, zum Beispiel gegenüber chinesischen Anbietern. Bei Unternehmen, die innerhalb der EU jedoch Betriebsstätten unterhalten (2), lässt sich Recht gegenüber diesen vollziehen.

Regulatorisches Neuland ist die Figur der sogenannten „virtuellen Betriebsstätte“, die zumindest steuerrechtlich solche Unternehmen erfassen soll, die keine klassische Betriebsstätte betreiben, jedoch am EU-Markt aktiv sind (3). Hier würde die „signifikante digitale Präsenz“ in der EU dafür herangezogen, Umsätze und Gewinne in der EU steuerlich zu behandeln.

Neuland hat die EU allerdings auch schon bei der Datenschutzgrundverordnung (DSGVO) betreten: diese gilt für alle Klassen von 1 bis 4 und knüpft konkret an der Tätigkeit an – grundsätzlich unabhängig vom Sitz: Wer personenbezogene Daten von in der EU ansässigen Bürgern verarbeitet (auch im Auftrag), um ihr Verhalten zu beobachten oder ihnen Dienstleistungen oder Waren anzubieten, wird dem regulatorischen Rahmen der DSGVO unterworfen. Dabei wird die Möglichkeit eröffnet, dass der Rechtsrahmen des Herkunftslandes als ein angemessenes Schutzniveau (das nicht zwingend identisch sein muss) gewährleistend eingestuft wird. Es handelt sich hierbei also um eine Erweiterung des Marktortprinzips, das über die eigenen Grenzen hinausreicht – ein Ausdruck der digitalen Souveränität Europas? Eine Debatte illustriert die bisherigen Schwierigkeiten damit.

Die 5G-Debatte: Europa macht sich das Leben schwer

Am Anfang stand 2015 ein Ziel: möglichst schnellen mobilen Datenfunk überall in der EU verfügbar zu machen. Was darauf folgte, war ein Paradebeispiel europäischer Digitalpolitik: Zwar hat man es geschafft, innerhalb Europas die notwendigen Frequenzen zu koordinieren – doch damit war es mit den europäischen Gemeinsamkeiten schon fast vorbei. 28 Mitgliedstaaten führten in nationalen Verfahren Frequenzvergaben durch. 28 Mal kamen unterschiedliche Bedingungen zum Tragen. Und 28 Mal unterschieden sich die jeweiligen Vorgaben für die Telekommunikationsanbieter. Nicht genug, im Zuge der Handelsstreitigkeiten der USA mit China kam auch das Thema der grundsätzlichen Vertrauenswürdigkeit chinesischer Netzwerkausrüster – mit Huawei und ZTE sind zwei der fünf weltweiten Anbieter chinesische Unternehmen – auf die politische Tagesordnung.

Auch in Europa hatte es bereits Kritik an einer möglicherweise zu starken Abhängigkeit von chinesischen Anbietern gegeben, angesichts der erwarteten Bedeutung von 5G als integrierter Netzwerktechnologie von Privathaushalten bis hin zu intelligenter Sensorik in Straßen, Brücken, Fabriken und der Rolle der Technologie für automatisierte und autonome Fahrzeuge. Doch nach der US-Entscheidung, die chinesischen Anbieter auszusperren und vorwiegend auf die beiden europäischen Anbieter Nokia und Ericsson zu setzen, stand Europa unter massivem Druck des transatlantischen Verbündeten, seinerseits ebenfalls chinesische Anbieter aus dem Aufbau der 5G-Infrastruktur herauszuhalten.

Drei Szenarien standen im Kern der Debatte: einmal die Befürchtung, dass die chinesischen Unternehmen nach dem Recht der Volksrepublik zur Mitwirkung an Spionageaktivitäten verpflichtet werden könnten und diese möglicherweise unerkannt und nicht einhegbar sein würden. Die zweite Befürchtung betraf das sogenannte Kill-Switch-Szenario, eine spezielle Form der Sabotage: chinesische Akteure könnten per Fernwartung einzelne Netzsegmente oder gar ganze Netze ausschalten. Das dritte Szenario war hingegen ein eher industriepolitisches: wenn Huawei und ZTE den europäischen Markt bedienen würden, droht mittelfristig das Verschwinden der anderen Anbieter und damit eine vollständige Abhängigkeit, die wiederum die Szenarien 1 und 2 noch wahrscheinlicher machen könnten. Eine besondere Qualität spielte in der Debatte die Frage, wie groß die Nähe der Unternehmen zur Staatsführung in Peking ist – tatsächlich wurde diese nie abschließend beantwortet, aber grundsätzlich sind derart große Unternehmen in China kaum ohne eine größere Nähe zur KPC überlebensfähig.

Die gesamte Debatte zeigte die Schwächen Europas: sie begann viel zu spät, die Mitgliedstaaten versuchten das Problem jeweils individuell zu lösen und auf eine gemeinsame Lösung drängten die wenigsten, während chinesische Vertreter – sowohl Angehörige des diplomatischen Korps als auch undiplomatische Firmenvertreter – in jedem Mitgliedstaat einzeln lobbyierten, die Problematik für inexistent erklären und auf die möglichen Folgen des Ausschlusses chinesischer Anbieter auch für die geschäftlichen Aktivitäten der Firmen aus diesen Staaten in China hinweisen konnten. Erst ein Dreivierteljahr nach Beginn der Debatte kamen im Januar 2020 konkrete Vorschläge aus Brüssel: die sogenannte „5G-Toolbox“, der Werkzeugkasten für den Mobilfunk der fünften Generation. Inhaltlich ist kaum mehr als ein nachdrücklicher Aufruf an die Mitgliedstaaten zur Einhaltung einheitlicher Mindeststandards.

Allerdings hat die 5G-Debatte auch einen positiven europäischen Aspekt mit sich gebracht: das Bewusstsein um die massiven Abhängigkeiten in der Digitalisierung von problematischen Akteuren ist deutlich gestiegen, verbunden mit der Erkenntnis, dass die gewohnt reaktive und nationale Herangehensweise derartige Probleme nicht adäquat adressieren kann. Dies ist ein Hauptgrund einer neuen Zielformulierung: der digitalen Souveränität.

Im Wirrwarr: Digitale Souveränität kann nicht binär sein

Der Begriff der Digitalen Souveränität hat vor allem in den vergangenen Monaten, noch einmal verstärkt durch die postulierte Ambition einer geopolitischen Kommission, eine enorme Konjunktur erfahren. Viele der diskutierten Aspekte sind dabei gar nicht zwingend spezifisch digital, sondern müssten genauso auch für andere Felder berücksichtigt werden. In politischen Reden und Forderungskatalogen findet er regelmäßig seinen Platz, ob in Debatten rund um 5G-Netzwerkausrüster oder im Kontext der Datenstrategie der EU-Kommission, deren Konzept gemeinsamer Data Spaces „Europas technologische Souveränität in Schlüsseltechnologien und -infrastrukturen für die Datenökonomie“ verbessern soll,[2] wortgleich auch im Whitepaper zur Künstlichen Intelligenz.[3] Auch die Industriestrategie der EU-Kommission vom März 2020 macht sich einen spezifischen Souveränitätsbegriff zu eigen: „Europas digitale Transformation, Sicherheit und künftige technologische Souveränität hängt von unseren strategischen, digitalen Infrastrukturen ab.“[4]

Die Spannbreite an Begriffsinterpretationen der „Digitalen Souveränität“ ist enorm. Doch kaum ein Politiker, kaum eine öffentliche Institution definiert diesen Begriff tatsächlich. Bundeskanzlerin Angela Merkel versteht unter Digitaler Souveränität:

> „…nicht Protektionismus oder Vorgabe von staatlichen Stellen, was an Informationen verbreitet werden kann – also Zensur –, sondern […] vielmehr die Fähigkeit, sowohl als Individuum, als einzelne Person, als auch als Gesellschaft die digitale Transformation selbstbestimmt gestalten zu können. […] Das heißt, wir brauchen Souveränität über das, was geschieht. Deshalb ist es gerade auch Ausdruck der Souveränität, für ein gemeinsames, freies, offenes und sicheres globales Internet einzutreten, wenn wir davon überzeugt sind, dass Abschottung kein Ausdruck von Souveränität ist, sondern dass wir ein gemeinsames Werteverständnis zugrunde legen müssen.“

Eine der wenigen harten Definitionen liefern Annegret Bendiek und Martin Schallbruch in ihrem SWP-Beitrag „Europas Dritter Weg im Cyberraum“[5]:

> Der Begriff digitale Souveränität bezeichnet die Fähigkeit eines Völkerrechtssubjekts zur Kontrolle und Steuerung des Cyberraums.

Diese legalistisch-technologische Perspektive ist ein guter Anfangspunkt, greift jedoch zu kurz. Denn was ist schon „Kontrolle und Steuerung des Cyberraums“, wenn man jenseits der Cybersicherheit auf Lieferketten, Dienstleistungsverflechtungen und weitere Interdependenzen schaut?

Es braucht daher einen anderen Begriff der digitalen Souveränität. Ein Arbeitsvorschlag wäre:

> Digitale Souveränität ist die Fähigkeit einer Entität, über die zukünftige Ausgestaltung festgestellter Abhängigkeiten in der Digitalisierung selbst entscheiden zu können und über die hierfür notwendigen Befugnisse zu verfügen.

Dies ist voraussetzungsvoll: Um selbst zu entscheiden, müssen konkrete Abhängigkeiten erkannt, analysiert und bewertet werden, eigene Fähigkeiten und Handlungsmöglichkeiten identifiziert werden – in formaler wie tatsächlicher Perspektive. Welche Kompetenzen sind hierfür nötig, welche Kompetenzen sind formal und welche real vorhanden? Sofern es an ihnen mangelt, lassen sie sich realistisch schaffen? In welchem Zeithorizont? Wie muss in der Zwischenzeit mit Problemen verfahren werden?

Hinzu kommt die strukturelle Schwierigkeit, digitale von sonstiger Entscheidungs- und Hand-

[2] EU-Kommission: Europäische Datenstrategie, S. 5; Brüssel, 20.02.2020 https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.
[3] EU-Kommission: Weißbuch Zur Künstlichen Intelligenz, S.3; Brüssel, 19.02.2020 https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_de.pdf.
[4] EU-Kommission: Eine neue Industriestrategie für Europa; Brüssel, 10.03.2020, S. 13 https://ec.europa.eu/info/sites/info/files/communication-eu-industrial-strategy-march-2020_en.pdf.
[5] Bendiek, Annegret / Schallbruch, Martin: Europas dritter Weg im Cyberraum. Der Beitrag der neuen Cybersicherheitsverordnung, S. 7; Berlin, 11.2019 https://www.swp-berlin.org/fileadmin/contents/products/aktuell/2019A60_bdk_Schallbruch_WEB.pdf.

lungsfähigkeit abzugrenzen, wenn die Digitalisierung in weite Teile des gesamtgesellschaftlichen Gefüges und der Wirtschaft hineinwirkt.

Daher müssen zunächst einmal Abgrenzungen vorgenommen werden, welche Bereiche grundsätzlich für unkritisch erachtbar sind, welche jedoch einem denkbaren, strukturellen Vorbehalt zur Ausübung digitaler Souveränität unterliegen sollten – sofern dies überhaupt sinnhaft scheint, angesichts der Vernetzungsgrade digitaler Produkte und Dienstleistungen.

Dies geht grundsätzlich wesentlich über den Bereich der „Kritischen Infrastrukturen“ im Cybersicherheitssinne (Energie, Wasser, Telekommunikation, Lebensmittel, Finanzwesen, Medien und Transport) hinaus, bei dem die Kritikalität entweder aus der Menge an Versorgungseinheiten oder aufgrund der besonderen Wichtigkeit für die Versorgung definiert wird.

Denn wenn Digitale Souveränität im Sinne einer eigenen Entscheidungs- und Handlungsfähigkeit das Ziel ist, dann ist nicht nur die Kritikalität des einzelnen Produkts oder Dienstleistung zum jetzigen Zeitpunkt, sondern auch die Kritikalität eines Produktes oder einer Dienstleistung zu einem späteren Zeitpunkt und in ihrem globalen Gesamtkontext maßgeblich. Keineswegs also reicht eine Antwort in der binären Form eines Abhängig = Ja oder Nein aus. Es handelt sich vielmehr um granulare, auf mehreren Ebenen und aus unterschiedlichen Perspektiven möglicherweise problematische Strukturen der Abhängigkeiten, deren Bewertung sodann ihrerseits noch einmal einer Differenzierung bedarf, wie sich im folgenden Abschnitt zeigen wird.

Vorhandene Abhängigkeiten: Tasten im Nebel

Es gibt bis heute keine überzeugenden empirischen Untersuchungen der realen Abhängigkeiten Europas in der Digitalisierung. Dies ist angesichts der Lautstärke der politischen Argumente in diesem Bereich überaus überraschend – sind viele Aspekte der Debatten doch keineswegs neu.

Wesentlich für die Frage der eigenen Abhängigkeiten sind alle Bereiche der Digitalisierung, die zu wesentlichen Teilen von Prozessschritten abhängen, die nicht maßgeblich innereuropäischer Entscheidungsgewalt unterliegen.

Hier sind zwei Ebenen zu unterscheiden: Erstens jene Teile von Prozessen, die außereuropäisch stattfinden und somit logisch zwingend grundsätzlich dem Einflussbereich anderer unterliegen. Zweitens aber auch alle Prozessschritte, die – ob in Europa oder in anderen Gebieten stattfindend – maßgeblich dem Machtbereich bzw. der Entscheidungsgewalt anderer, außereuropäischer Akteure zuzuordnen sind. Als Prozessschritte sind dabei alle einzelnen Komponenten (Hardware, Software, betriebsnotwendige Infrastrukturen, ggf. auch Personal) in ihrer Herstellung, in Betrieb und Wartung sowie in ihrem Zusammenwirken zu betrachten, gegebenenfalls sogar ihre einzelnen Produktbestandteile und deren Entstehensbedingungen. Hierbei sind wiederum unterschiedliche Kritikalitäten zu definieren: nur weil sich Prozessschritte in der Verfügungsgewalt von außereuropäischen Dritten befinden, sind diese noch nicht per se problematisch; dies ist von den jeweiligen Umständen abhängig.

Unter besonderer Berücksichtigung der Frage, welche Werte Europa mit dem jeweiligen Dritten teilt und welchen Grad der Stabilität diese Beziehung aufweist, ist eine abgestufte Betrachtung geboten. Norwegen, Kanada, Japan, Israel, USA, Südafrika, Brasilien, Indien, Russland, Saudi-Arabien und China sind auch in Fragen der digitalen Abhängigkeit auf sehr unterschiedlichen Ebenen zwischen enger Partnerschaft, kooperativer Handelsbeziehung, destruktivem Wettbewerber und Systemrivalen zu verorten.

Um spezifische Abhängigkeiten oder Handlungsnotwendigkeiten zu ermitteln, ist eine strukturierte Bestandsaufnahme notwendig.

- Sie muss das „**Wie**“ der konkreten Abhängigkeit(en) entsprechend eines Vertretbarkeitsrasters aufschlüsseln: Ist der jeweilige Prozessschritt
  - von geringer oder hoher Kritikalität für die Verfügbarkeit, Sicherheit oder künftige Abhängigkeit?
  - grundsätzlich auch durch andere leistbar (Diversifizierungs- und Substituierungspotenzial)?
  - konkurrierend zu innereuropäischen Akteuren? Wenn ja, wer verfügt tatsächlich über diese?
  - durch politische Entscheidungen außereuropäischer Akteure unzulässig befördert?
- Zudem muss das „**Warum**“ der konkreten Abhängigkeit(en) aufgeschlüsselt werden: Liegt es an
  - Ressourcen
  - Preisvorteilen
  - Marktgrößen
  - Subventionen
  - technologischem Vorsprung
  - …?

Um das Gewicht dieser Abhängigkeiten realistisch einschätzen zu können, ist die differenzierte Betrachtung zwingend geboten: Gibt es Bereiche, in denen diese Akteure ihrerseits maßgeblich von innereuropäischen Prozessschritten, Dienstleistungen, Produkten abhängig sind? Wie resilient sind die Anbieter oder Produzenten gegen unerwünschte Einflussnahme durch Dritte (z.B. Übernahmen, Anteilserwerb, eigene Abhängigkeiten)?

Auf Basis einer derartigen Bestandsaufnahme ließe sich qualifiziert ein Instrument des strategischen Abhängigkeitsmanagements entwickeln, für das in Folge wiederum passende (vorwiegend vermutlich Handels- und Wettbewerbs-) Rechtsinstrumente folgen können.

Abhängigkeiten verstehen: Fallanalysen sind Grundlage

Um zu verstehen, welche Komplexitäten sich hier darstellen, müssen Dienstleistungen und Produkte und ihre Vorleistungen und notwendigen Betriebsvoraussetzungen einzeln analysiert und in ihrer Wirkung gemeinsam betrachtet werden. Dabei ist es wichtig, mit dem weiten Begriff der Digitalisierung zu arbeiten. Zur Verdeutlichung der so entstehenden Fragen folgt ein naturgemäß immer noch stark vereinfachtes Beispiel. Würde man es konsequent zu Ende verfolgen, müsste man bei jedem Bauteil bzw. Prozessbestandteil die Lieferketten bis in die Rohstoffe hinein prüfen – sofern diese nicht vollständig substituierbar sind.

Die *Nahrungsmittelversorgung* ist bereits heute Teil der *kritischen Infrastruktur*, da die Versorgung der Bevölkerung mit Grundnahrungsmitteln zwingend erforderlich ist. Ausgangspunkt dieser Versorgung ist die Herstellung eines Produktes; nehmen wir an, es handele sich um Kartoffeln. Diese werden heutzutage mit modernen Methoden auf Feldern von Landwirten ausgesät, gepflegt und geerntet. Hierfür kommen in aller Regel landwirtschaftliche Großmaschinen zum Einsatz, die hochdigitalisierte Produkte sind. Unter der Annahme, dass die Sicherstellung der Kartoffelversorgung zwingend zu gewährleisten ist, müssten also diese Maschinen auf ihre digitale Betriebssicherheit geprüft werden. Verwenden wir ein vereinfachtes Prüfschema, um uns der Komplexität der Kartoffel zu nähern:

- Wer stellt diese Maschinen her? Aus welchen Komponenten? Wo werden diese gefertigt?
  - Ostwestfälischer Landmaschinen-Hersteller
  - Hardware wird von deutschen und US-Herstellern bezogen, Fertigung der IT-Komponenten in VR China, Taiwan und Südkorea, Rohstoffe aus Europa, China, USA und Südamerika.
- Wer besitzt Entscheidungsgewalt über den Hersteller?
  - Aktiengesellschaft, zu 60 Prozent in Familienbesitz, 40 Prozent andere Inhaber, davon 10 Prozent außereuropäische Investoren.

- Woher stammen Software und Daten für den Betrieb der Maschinen (Motor- und Maschinensteuerung, Sensoriksteuerung)?
  - Motorsteuerung: Software-Eigenentwicklung
  - Maschinensteuerung: Software-Zulieferung von großem Dienstleister aus UK, der Software in Indien entwickeln und Qualitätssicherung in USA betreiben lässt.
  - Sensoriksteuerung: von deutschem Hersteller bezogen, Entwicklung und Wartung in Japan.
- Wer ist für ihre Wartung/Pflege zuständig?
  - Service-Level-Agreement (SLA) mit Herstellerfirma
- Ist das Produkt standardisiert und sind seine Teile kurzfristig durch andere substituierbar?
  - Teile des Produktes sind standardisiert.
  - Substitution auf Hardwareebene teilweise möglich.
  - Substitution auf Softwareebene derzeit rechtlich (SLA)/technisch (Code nur jetzigem Softwareanbieter bekannt) nicht möglich.
- Zusammenfassung:
  Wer besitzt die tatsächliche Entscheidungsgewalt (Software, Hardware) über die Maschine?
  - Qualitätssicherungsteam Softwareentwicklung USA
  - Besitzerfamilie in Deutschland
- Umständewürdigung: Ist davon auszugehen, dass der Anbieter auf absehbare Zeit in einem verlässlichen, stabilen rechtlichen und politischen Rahmen agieren wird?
  - Nein, denn das chinesische Rechtssystem ist kein unabhängiges Rechtssystem, sondern Instrument politischen Willens.
- Ist davon auszugehen, dass der Anbieter in absehbarer Zeit unter den Einfluss problematischer Akteure gerät?
  - Ja.

Anhand dieser freihändigen, kursorischen Prüfung steht bereits fest: Ob es in Deutschland Kartoffeln im Regal gibt oder nicht, das entscheidet sich derzeit nicht zwingend beim Bauern oder beim Landmaschinenhersteller selbst.

Stellen wir die gleichen Fragen für deutsche Telekommunikationsnetzanbieter und Aufbau der 5G-Infrastruktur:

- Wer ist Anbieter der eingesetzten Hardware? Wo werden diese gefertigt? Aus welchen Komponenten?
  - Hardware: Chinesischer Anbieter Huawei
  - Fertigung der IT-Komponenten in VR China, Taiwan und Südkorea
  - Rohstoffe aus China und Südamerika
- Wer besitzt Verfügungsgewalt über die Hersteller?
  - Huawei: Chinesische Limited (kein Einblick in Eigentümerstruktur)
- Woher stammen Software und Daten für den Betrieb der Geräte (Funknetz, Verteilernetze, Steuerungselemente)?
  - Software Verteilernetze Cisco
  - Software Steuerungselemente Open Source
  - Software Funknetz von chinesischem Hersteller
- Wer ist für ihre Wartung/Pflege zuständig?
  - Service-Level-Agreement (SLA) mit Herstellerfirma
  - Service-Level-Agreement (SLA) mit Dienstleister
  - Eigenwartung
- Ist das Produkt standardisiert und sind seine Teile kurzfristig substituierbar?
  - Teile des Produktes sind standardisiert.
  - Substitution auf Hardwareebene möglich.
  - Substitution auf Softwareebene derzeit rechtlich (SLA)/technisch (Code nur jetzigem Softwareanbieter bekannt) nicht möglich.
  - Substitution auf Softwareebene möglich.
- Zusammenfassung:
  Wer besitzt heute die tatsächliche Verfügungsgewalt (Software, Hardware) über die Maschine?
  - Qualitätssicherung China
  - Eigentümer in China
- Umständewürdigung:
  Ist davon auszugehen, dass der Anbieter auf absehbare Zeit in einem verlässlichen, stabilen rechtlichen und politischen Rahmen agieren wird?
  - Nein, denn das chinesische Rechtssystem ist kein unabhängiges Rechtssystem, sondern Instrument politischen Willens.

- Ist davon auszugehen, dass der Anbieter in absehbarer Zeit unter den Einfluss problematischer Akteure gerät?
  - Ja.

Es zeigt sich bereits mit dieser oberflächlichen Prüfung, auf wie vielen unterschiedlichen Ebenen hierbei Probleme vorhanden wären, die in einer informierten Entscheidung unter dem Aspekt digitaler Souveränität berücksichtigt werden müssten.

Derartige Analysen sind für fast alle Bereiche, in denen digitale Technologie zum Einsatz kommt, möglich und zielführend, wenn es darum geht, Abhängigkeiten zuerst einmal systematisch zu erfassen.

Neben die Frage der Entscheidungsfähigkeit über externe Abhängigkeiten tritt jedoch eine zweite Dimension: die Frage der europäischen Handlungsfähigkeit nach außen und nach innen. Diese wird maßgeblich dadurch determiniert, inwiefern die eigenen Strukturen in der Lage sind, die Digitalisierung nach europäischen Vorgaben inhaltlich, wirtschaftlich, regulatorisch, exekutiv und politisch zu durchdringen und zu gestalten.

Hierbei sind wiederum zu unterscheiden:

- Die Möglichkeit zur politischen Gestaltung und Rechtsetzung auf allen vier Ebenen, also EU, Mitgliedstaat, Land und Kommune durch adäquate rechtliche, institutionelle und personelle Kompetenzzuweisung (Politik)
- die Möglichkeit des Rechtsvollzugs durch öffentliche Stellen (Aufsichts- und Ermittlungsbehörden, Gerichte)
- die Möglichkeiten zur Rechtsdurchsetzung durch Private (Bürger, Unternehmen und Gemeinwohl-Organisationen)
- die tatsächliche Standardsetzung in Gremien zur technischen Normierung und die internationalen (Rechts-)Rahmenbedingungen in Abkommen und Organisationen
- die Umsetzbarkeit durch privatwirtschaftliche Akteure am Markt (Rentabilität)
- die Befähigung der Abnehmer und Verbraucher zu bewussten Entscheidungen (Entscheidungssouveränität)

Das Ziel: Ein gemeinsames europäisches strategisches Abhängigkeitsmanagement

Es spricht viel dafür anzunehmen, dass Digitale Souveränität für die EU als europäische Werte berücksichtigende, europäische Grundprinzipien bewahrende Gestaltung der Digitalisierung als gesamtgesellschaftliche Aufgabe europäisch eng koordiniert, wahrscheinlich sogar am besten zentralisiert stattfindet. Dies liegt allein schon daran, dass die leistungsfähigste nationale Digitalpolitik angesichts der internationalen Dimension der Problematik auch bei großen europäischen Staaten ungeeignet erscheint, um mit jenen Akteuren auf Augenhöhe verhandeln zu können, die hier derzeit die wesentliche Rolle spielen.

Allerdings benötigte dies ein klares Mandat – und gerade aufgrund der Querschnittlichkeit der Digitalpolitik in fast alle anderen Politikbereiche wäre die konsequente Verfolgung dieser Ziele nah an einer zumindest temporären Vollintegration der notwendigen Kompetenzen, was realistisch betrachtet illusorisch ist. Zugleich ist das Wissen um die Unzulänglichkeit der eigenen Verhandlungsposition auch den meisten Mitgliedstaaten in den vergangenen Jahren schmerzlich bewusstgeworden. Die geopolitische Dimension der Digitalpolitik könnte somit ein Hebel sein, die Bereitschaft zu einer zeitlich und inhaltlich begrenzten weiteren Integration zu prüfen.

International böte ein integriertes europäisches Vorgehen große Chancen: wesentliche Teile der westlich geprägten Demokratien (namentlich die meisten OECD-Staaten) sind durchaus nicht gewillt, sich dem technologischen und damit auch politischen Einfluss Chinas zu unterwerfen. Doch derzeit ist der schlichte Mangel an ernstzunehmenden Alternativen, kombiniert mit einer durchaus geschickten Außenwirtschaftsdigitalstrategie der Volksrepublik, für viele eine scheinbar unüberwindbare Hürde. Doch auch kritisch zu würdigende Staaten wie China legen es nicht auf eine massive Konfrontation an, da diese ihren eigenen, primär internen wirtschaftlichen Interessen zuwiderlaufen würde, was wiederum für die Handlungsmöglichkeiten der EU und ihrer Mitgliedstaaten zu berücksichtigen ist.

Ziel entsprechender Maßnahmen müsste dabei ein gemeinsames europäisches strategisches Abhängigkeitsmanagement sein. Im ersten Schritt wären die existierenden und erwartbaren künftigen Abhängigkeiten zu identifizieren, in einem zweiten Schritt diese Abhängigkeiten zu klassifizieren und nach Kritikalität und Mitigierbarkeit zu priorisieren. In einem dritten Schritt ließen sich mit dem Ziel des Ausbaus eigener Fähigkeiten, der bewusst gewählten oder in Kauf genommenen Abhängigkeiten oder der Akzeptanz irrelevanter Abhängigkeiten strategische Gleichgewichte, langfristig vielleicht sogar Übergewichte herbeiführen, die den eigenen Handlungsspielraum wieder erweitern würden.

Die EU muss dazu auch in die Position gelangen, ihre eigenen Werte und Rechtsvorstellungen aktiv gegenüber jenen durchzusetzen, die aus Drittstaaten in der Union tätig sind, und muss zugleich seine eigene Rolle als eine für die Bürger positiv erfahrbare EU neu finden. Dauerhaft anlassbezogen einzelne Akteure wie Huawei oder ZTE zu prüfen erscheint hierfür jedenfalls keine sinnvolle Strategie zu sein, da dies den spontanen Aufbau von Substitutionsmöglichkeiten für problematische Akteure nicht ausschließen würde - im Fußball würde dies als Manndeckung gelten. Stattdessen muss Raumdeckung das Ziel sein: Europa muss sich selbst in die Lage versetzen, dass andere Akteure in der Digitalisierung mindestens so abhängig von seiner Spielteilnahme sind, wie Europa es von ihrer ist.

Bild: Shutterstock / maradon 333

Adresse | Kontakt

Katharina Gnath
Senior Project Manager
Programm Europas Zukunft
Bertelsmann Stiftung
Werderscher Markt 6, 10117 Berlin
Telefon 030 275788-128
katharina.gnath@bertelsmann-stiftung.de
www.bertelsmann-stiftung.de/europe

Falk Steiner war von März 2019 bis Mai 2020 als Senior Expert für Digitalpolitik im Programm Megatrends der Bertelsmann Stiftung tätig.

Viktoria Grzymek ist Project Manager im Projekt „Ethik der Algorithmen“ der Bertelsmann Stiftung und beschäftigt sich mit den gesellschaftspolitischen Auswirkungen algorithmischer Systeme.