Digital Gipfel
Nürnberg 2018

Plattform Innovative Digitalisierung der Wirtschaft:

Fokusgruppe „Digitale Souveränität in einer vernetzten Gesellschaft“

Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen

Inhalt

1. Einleitung und Positionsbestimmung: Digitale Souveränität im Kontext Künstlicher Intelligenz

Die Digitalisierung ist eine der wichtigsten Entwicklungen der Gegenwart und hat sich fest im öffentlichen und politischen Diskurs manifestiert. Zugleich wird die Digitalisierung von manchen als ökonomische Bedrohung empfunden. Und in der Tat stehen Unternehmen aufgrund der zunehmenden Transformationsgeschwindigkeit vor der Frage, wie sie ihre Innovationspotenziale besser ausschöpfen, marktfähige Angebote entwickeln und sich somit „selbst behaupten" können.

Politisch wurde die Frage der Selbstbehauptung erstmalig 2013 im Kontext der Snowden-Enthüllungen gestellt und konzentrierte sich darauf, wie sich die Gesellschaft gegen Überwachung und Spionage durch Drittstaaten zur Wehr setzen kann. 2015 wurde im Rahmen des damaligen Nationalen IT-Gipfels der Bundesregierung der Begriff „Digitale Souveränität" geprägt.[1] Aus heutiger Perspektive ist die Frage der digitalen Souveränität jedoch breiter zu fassen und muss insbesondere die Konkurrenz verschiedener politischer und gesellschaftlicher Systeme adressieren. Dem Wettlauf um die Künstliche Intelligenz (KI) ist dabei eine besondere Stellung beizumessen, da sie als stark disruptive Querschnittstechnologie Teil aller vernetzten bzw. vernetzbaren Lebens- und Arbeitsbereiche werden wird. Ihr wird das Potenzial zugestanden, nicht nur einzelne Wirtschaftsbereiche, sondern ganze Gesellschaftssysteme[2] tiefgreifend zu verändern. Digitale Souveränität erfordert neben einer Betrachtung einzelner Technologiebereiche auch eine gesellschaftsethische Fundierung. So stellen gegenwärtig geführte digital-ethische Diskussionen, bspw. zum autonomen Fahren, zu Recht den Menschen in den Mittelpunkt der Betrachtung. Diese Humanzentrierung kann ein Markenkern europäischer KI-Entwicklungen werden und ist eine wesentliche Grundlage zur Entwicklung einer gegenüber dem Menschen verantwortlichen digitalen Transformation. Für Deutschland und Europa bietet sich die Chance, einen eigenen digital souveränen Weg zu beschreiten, der sich zum Wohle der sozialen Marktwirtschaft auf die europäische Tradition des Humanismus besinnt. Orientiert an den universellen Grundrechten sowie der Würde des Menschen schützt eine solche digitale Transformation in Europa verankerte Werte wie Freiheit, Respekt, Toleranz und Wertschätzung. Somit rückt die digitale Selbstbestimmtheit in den Fokus digitalpolitischer Entwicklungsziele. Damit wird es erforderlich, die Begriffsdefinition aus dem Jahr 2015 an diesen neuen Bedürfnissen auszurichten, zu schärfen und letztlich zur Gestaltung konkreter Politik zu nutzen.

Neben dieser Fokussierung muss eine erfolgreiche digitale Transformation aber auch auf eine gesellschaftliche Akzeptanz treffen. In einer rein ökonomischen oder politischen Betrachtung könnte man diese auf die Skalierbarkeit von Geschäftsideen beschränken und mit Blick auf Europa auf eine regulatorische Zersplitterung, einen noch nicht vollendeten digitalen Binnenmarkt oder auf Sprachbarrieren als hemmende Faktoren abstellen. Werden aber die gesamtgesellschaftlichen Implikationen, z. B. arbeitsmarkt- und sozialpolitische Entwicklungen, ebenfalls mit einbezogen, wird deutlich, dass Deutschland und Europa nicht einfach die Silicon Valley- oder Shenzhen-Strategien kopieren sollte. Vielmehr erscheint es aufgrund der gegenwärtig stark ausgeprägten US-Orientierung bei der Gestaltung der Digitalisierung in Europa geboten zu sein, dass wir den digitalen Wandel in Europa auf einem eigenen Weg gestalten müssen. Sonst werden die Digitalstrategien anderer aufstrebender Wirtschaftsregionen, der Aufbau neuer Internetkonzerne und zunehmende strategische Aufkäufe europäischer Unternehmen die Abhängigkeit Europas verstärken. Insofern muss gerade Deutschland – auch im eigenen Interesse – hier in Europa verantwortlich handeln.

Diese Publikation entwickelt daher die Definition des Begriffs digitaler Souveränität so weiter, dass ein selbstbewusster digitalpolitischer Gestaltungsanspruch entstehen kann. Ein mehrdimensionales Schichtenmodell im Anhang bietet Orientierung bei Entscheidungen über Maßnahmen zum Erhalt bzw. Aufbau digitaler Souveränität. Aufbauend auf diesem Klassifikationsschema wird dargelegt, in welchen Technologie- und Anwendungsfeldern Europa ein besonderes Interesse haben sollte, digital souverän zu sein. Welche besondere Rolle dabei KI spielt, zeigt der Exkurs zur Mustererkennung als ein Kernelement von KI-Systemen. Im abschließenden Kapitel wird beschrieben, welcher Akteur welche Verantwortung übernehmen muss, um dem aus der digitalen Souveränität ableitbaren Gestaltungsanspruch gerecht zu werden.

2. Zum Begriff der Digitalen Souveränität

2.1 Definition

Souveränität bezeichnet die Möglichkeit zur unabhängigen Selbstbestimmung von Staaten, Organisationen oder Individuen. Digitale Souveränität ist heute ein wichtiger Teilaspekt allgemeiner Souveränität, der die Fähigkeit zur unabhängigen Selbstbestimmung in Bezug auf die Nutzung und Gestaltung digitaler Systeme selbst, der darin erzeugten und gespeicherten Daten sowie der damit abgebildeten Prozesse umfasst.

Der Begriff der digitalen Souveränität kann einerseits auf Staaten, auf Organisationen (wie etwa Unternehmen oder die Forschungs- und Wissenschaftslandschaft), andererseits jedoch auch auf einzelne Individuen angewendet werden. Im Mittelpunkt dieses Papiers steht die digitale Souveränität von Staat, Wirtschaft und Wissenschaft. Sie ist eine entscheidende Voraussetzung für deren eigenständige Handlungsfähigkeit.[3]

Digitale Souveränität eines Staates oder einer Organisation umfasst zwingend die vollständige Kontrolle über gespeicherte und verarbeitete Daten sowie die unabhängige Entscheidung darüber, wer darauf zugreifen darf. Sie umfasst weiterhin die Fähigkeit, technologische Komponenten und Systeme eigenständig zu entwickeln, zu verändern, zu kontrollieren und durch andere Komponenten zu ergänzen.

Digitale Souveränität ist deswegen einerseits wichtige Grundlage für vertrauenswürdige Systeme und andererseits unverzichtbare Voraussetzung für unabhängiges staatliches Handeln. Sie begünstigt Wirtschaftlichkeit, Agilität und die Fähigkeit, mit Risiken umgehen zu können, denn digital souveräne Staaten und Organisationen können sich aufgrund geringerer Herstellerabhängigkeiten freier am Markt bedienen. Somit erhalten sie Gestaltungs- und Innovationsspielräume, da vorhandene Systeme schneller angepasst und im Bedarfsfall einfacher durch andere ersetzt werden können.

2.2 Kriterien der digitalen Souveränität

Digitale Souveränität kann – wie auch die allgemeine Souveränität – in unterschiedlichen Bereichen unterschiedlich stark ausgeprägt sein. Eine vollständige digitale Souveränität ist in vielen Fällen nicht möglich und auch nicht erstrebenswert, da ein hoher Grad an digitaler Souveränität mit hohem Aufwand und Kosten verbunden sein kann.

Dies lässt sich etwa am Beispiel von Software zur Analyse des Besucherverhaltens von Webseiten verdeutlichen: Entsprechende Lösungen sind kostenfrei als „Software as a Service (SaaS)-Angebot“ verfügbar, sie lassen sich jedoch nur nutzen, wenn die Daten über das Verhalten der eigenen Nutzer an die entsprechenden Anbieter übertragen und von diesen auch für eigene Zwecke genutzt werden dürfen. Somit kann nicht mehr vollständig kontrolliert werden, wer Zugriff auf die Daten der Nutzer hat, und Analysen und Erkenntnisse können nur in dem Maße generiert werden, wie die betreffende Lösung es ermöglicht. Auch sind Kombination und Integration mit anderen Lösungen nur möglich, wenn der Anbieter dies erlaubt. Schließlich müssen Nutzer solcher Angebote befürchten, gar keinen Zugriff mehr auf ihre Daten zu haben, etwa, wenn ein Anbieter sein Angebot einstellt oder vertragliche Verpflichtungen aufgrund von Insolvenz nicht mehr einhalten kann. Die Nutzung solcher Lösungen führt also zu geringer digitaler Souveränität. Die Alternative ist der Aufbau eigener Systeme zur Besucheranalyse, bei der die Daten vollständig unter eigener Kontrolle stehen. Bei der Auswertung gibt es keine grundsätzlichen Beschränkungen, denn alles kann auch durch Modifikation vorhandener oder Einsatz neuer Software analysiert werden. Die so erreichte höhere digitale Souveränität ist aber mit zusätzlichem Aufwand für Aufbau, den sicheren Betrieb und ggf. sogar die Weiterentwicklung selbst betriebener Lösungen verbunden.

Staaten und Organisationen müssen deswegen entscheiden, in welchen Bereichen eine hohe digitale Souveränität elementar und von hoher strategischer Bedeutung ist und gegebenenfalls einen höheren Aufwand für ihren Erhalt rechtfertigt.

Allerdings sollten Lösungen, die hohe digitale Souveränität gewährleisten und hinsichtlich Leistungsumfang, Kosten und Aufwand mit Lösungen geringerer digitaler Souveränität vergleichbar sind, immer bevorzugt werden, um die damit verbundenen strategischen Vorteile nutzen zu können. Der Staat und andere Organisationen müssen als Einkäufer von Informationstechnologie bei Vergabeentscheidungen daher auch prüfen, in welchem Maß eine Lösung digitale Souveränität ermöglicht, und entsprechende Kriterien in ihre Entscheidungen einbeziehen.

Diese Kriterien lassen sich direkt aus der Definition digitaler Souveränität ableiten. Hohe digitale Souveränität ist demzufolge dann gegeben, wenn

- die grundsätzliche IT-Architektur den Austausch einzelner Lösungen und Komponenten so einfach wie möglich macht,
- um die zentralen Systeme der Gesamtarchitektur ein Ökosystem von Anbietern und Dienstleistern vorhanden ist, das zusätzliche Lösungen, Erweiterungen und Dienstleistungen zur Verfügung stellt, welche sich mit geringem Aufwand in das Gesamtsystem integrieren lassen,
- die von den Lösungen gespeicherten und verarbeiteten Daten vor unbefugtem Zugriff geschützt sind und sie unabhängig von der eigentlichen Software gelesen, gelöscht und bearbeitet werden können,
- Datenformate und Schnittstellen einen einfachen Wechsel zu alternativen Lösungen ermöglichen,
- neue Lösungen sich über offene Standards, die von jedermann lizenz- und kostenfrei verwendet werden können, leicht mit bereits eingesetzten Lösungen kombinieren lassen und
- der Quellcode der Lösungen unabhängig überprüft, verändert und angepasst werden kann – auch damit Staat, Wissenschaft und Wirtschaft Produkte und Technologien innovativ vorantreiben und weiterentwickeln können,
- sich der Anbieter in Deutschland bzw. in der Europäischen Union befindet und ausschließlich dieser Jurisdiktion untersteht und
- die wesentlichen Hardware-Komponenten in Deutschland oder der Europäischen Union produziert und beeinflusst werden können.

Die genannten Kriterien lassen sich in ein Schichtenmodell (siehe Anhang) bringen, mit dessen Hilfe Architekten und Entscheider im Einsatz befindliche oder neu zu beschaffende technologische Komponenten im Hinblick auf das damit einhergehende Maß digitaler Souveränität beurteilen und ins Verhältnis zu dem aufgrund der strategischen Bedeutung der betreffenden Komponente erforderlichen Maß setzen können. Weil hohe digitale Souveränität auch das Potenzial umfasst, mit Risiken umgehen zu können, hat dieses Modell viele Überschneidungen mit klassischen Modellen zum IT-Risikomanagement.[4]

3. Voraussetzung zum Aufbau und zum Erhalt digitaler Souveränität

Ungeachtet konkreter Anwendungsszenarien bestehen für den Aufbau und den Erhalt von digitaler Souveränität einige Voraussetzungen, die allen digitalen Anwendungen gemein sind. Hierzu zählen Netzinfrastrukturen und Rechenzentren ebenso wie IT-Sicherheit, Transparenz und digitale Kompetenzen. Diese generischen Anforderungen sind nachfolgend kurz erläutert.

3.1 Zuverlässige digitale Infrastrukturen

Digitalisierung in all ihren Ausprägungen hat stets einen großen gemeinsamen Nenner. Die Daten, die im Rahmen digitaler Prozesse anfallen und von einem Ort, Menschen oder einem „Ding" (IoT) zum anderen transportiert werden müssen, brauchen zuverlässige, digitale Kommunikationsnetze. Damit kommt insbesondere den Weitverkehrsnetzen im Kontext der Debatte über digitale Souveränität eine Schlüsselrolle zu. Die souveräne Kontrolle über diese Netze, ganz gleich ob leitungsgebunden oder auf Basis von Mobilfunktechnologien, ist existentiell. Besteht diese nicht, kann das Rückgrat der Digitalisierung im extremsten Fall im Rahmen zielgerichteter Cyber-Attacken oder durch drittstaatliche Einflussnahme einfach „ausgeschaltet" werden. Als Folge dessen kämen alle digitalen Prozesse, die nicht in einem lokal abgeschirmten Raum ablaufen, zu einem jähen Stillstand.

Um digitale Souveränität also zu ermöglichen, müssen unsere Kommunikationsnetze eine Reihe von Voraussetzungen erfüllen. Sie müssen zu jeder Zeit verfügbar sein, Menschen, Wirtschaft und Staat eine abhörsichere Kommunikation ermöglichen und Schutz vor Manipulation der transportierten Daten bieten. Im Kontext zunehmender digitaler Echtzeitkommunikation kommt zudem der Zuverlässigkeit dieser Netze eine wachsende Bedeutung zu. Ein ganz aktuelles Beispiel hierfür ist der kommende Mobilfunkstandard 5G. Die damit aufzubauenden 5G-Netze werden die zukünftige Basisinfrastruktur für unsere industrielle Wertschöpfung bilden, die für die Wettbewerbsfähigkeit unserer Wirtschaft insgesamt zentral ist. Niedrige Latenzzeiten und hohe Datenübertragungsraten ermöglichen drahtlose, digitale Anwendungen, die ohne ihre enorme Geschwindigkeit nicht realisierbar wären – bspw. im Kontext des autonomen Fahrens, aber auch im Kontext von KI.

Die erste Grundvoraussetzung für zuverlässige digitale Infrastrukturen ist vertrauenswürdige Technologie. Alle aktiven Komponenten, die in unseren digitalen (Mobilfunk)Netzen für den Transport der Daten sorgen, müssen ein Höchstmaß an Vertrauenswürdigkeit aufweisen. Sie müssen sicherstellen, dass die Daten den richtigen Weg nehmen, den beabsichtigten Empfänger erreichen, nicht abgehört und nicht manipuliert werden.

Dies sicherzustellen ist eine immense Herausforderung. Durchgehende Sicherheitsevaluierungen werden aufgrund der steigenden technischen Komplexität (insb. bei 5G) und des damit steigenden Prüfaufwands immer schwieriger. Der Grund liegt in einer starken technologischen Abhängigkeit von Infrastrukturherstellern aus dem nicht-europäischen Raum, deren Technologien unsere Weitverkehrsnetze dominieren, die jedoch unsere europäischen Werte nicht bedingungslos teilen. Vertrauenswürdige Alternativen aus Europa sucht man auf dieser Ebene vergebens. Umso wichtiger sind die großen europäischen Initiativen im Bereich 5G. Hier hat Europa derzeit noch eine reale Chance, gemeinsam mit den europäischen Infrastrukturherstellern ein eigenes Angebot zu entwickeln, mit dem europäische Netzbetreiber eine vertrauenswürdige 5G-Infrastruktur aufbauen können.

Der zweite wesentliche Pfeiler für zuverlässige digitale Infrastrukturen ist die Kontrolle über unsere nationalen Kommunikationsnetze. Sie muss zwingend in deutscher, mindestens jedoch europäischer, Hand liegen. Ist dies nicht der Fall, gehen wir das Risiko ein, dass Konzerne aus nicht-europäischen Staaten darüber entscheiden können, ob diese Netze funktionieren oder ob sie ausgeschaltet werden. Nicht nur in diesem Kontext sind die jüngsten Verschärfungen im Bereich der Investitionskontrolle deutlich zu begrüßen. Flankierend sollten Ansätze wie das Schengen-Routing, bei dem innereuropäischer Datenverkehr nicht ohne zwingende Erfordernis über außereuropäische Datenleitungen geroutet wird, wohlwollend neu betrachtet werden.

Die hohen Ansprüche, die für unsere Weitverkehrsnetze gelten, sollten selbstverständlich auch für unsere Regierungsnetze zur Anwendung kommen. Auch sie müssen geprägt sein von einem Höchstmaß an Vertrauenswürdigkeit, Zuverlässigkeit und Kontrolle. Im Gegensatz zu den Weitverkehrsnetzen gibt es hier jedoch bereits heute ein Angebot technologischer Alternativen aus dem In- und Ausland, die grundsätzlich ein selbstbestimmtes Entscheiden ermöglichen. Selbiges gilt für unsere Forschungsnetze sowie für die Netze im Bereich der kritischen Infrastrukturen.

3.2 Leistungsfähige Rechenzentren

Rechenzentren sind neben der Netzinfrastruktur die zweite physische Säule der Digitalisierung von Wirtschaft und öffentlicher Verwaltung sowie der Nutzung des Internets der Bürger und Bürgerinnen. Die Frage, ob sich ein Rechenzentrum – und mit ihm die dort gespeicherten Daten – in Europa befindet, ist somit für die digitale Souveränität von großer Bedeutung. So muss etwa in Krisenfällen auch der physische Zugriff auf Rechenzentren möglich sein. Der Preis für elektrischen Strom ist mit Abstand der wichtigste Kostenfaktor beim Betrieb von Rechenzentren, deren Leistungen oftmals mit geringem technischen Aufwand auch an Standorten außerhalb Europas erbracht werden können. Der Standortwettbewerb um die Ansiedlung von Rechenzentren – gerade auch von Hyperscale-Rechenzentren – wird zukünftig zunehmen. Während öffentliche Verwaltungen aufgrund rechtlicher Vorgaben auf einen Rechenzentrumsbetrieb in Europa angewiesen sind, können private Rechenzentren ins Ausland ausweichen, um die hohen Stromkosten zu vermeiden.

Schon heute dominieren US-amerikanische und chinesische Anbieter alle drei Wertschöpfungsstufen des Cloud-Marktes. Auf der Infrastrukturebene [IaaS], die Rechen- und Speicherkapazität bereitstellt, kontrolliert ein US-Anbieter über 50 Prozent des weltweiten Marktes. Aber auch die darüber liegende Plattformebene [PaaS] und die Softwareebene [SaaS] werden von wenigen Anbietern dominiert, so dass plattformunabhängige Anwendungen (sog. Middleware mit offenen Schnittstellen zwischen Infrastruktur und Software) zunehmend verdrängt werden.

Da aber die Digitalisierung im Allgemeinen und KI im Speziellen auf die Speicherung und Verarbeitung von Daten angewiesen ist, müssen wir Cloud-Rechenzentren als kritische Infrastruktur in Europa betrachten. Die Speicherung von Daten deutscher Behörden, europäischer Unternehmen, Institutionen oder Verbrauchern fast ausschließlich in der Hand nicht-europäischer Cloud-Betreiber stellt einen strategischen wie kommerziellen Nachteil für Europa dar und kann den Schutz und die Sicherheit sensibler Daten nachhaltig gefährden.

Gleichzeitig steigt die Gefahr der Abhängigkeit von nicht-europäischen Anbietern, denn der globale Cloud-Markt wächst jährlich um ca. 20 Prozent. 2019 werden bereits 60 Prozent aller IT-gestützten Unternehmensaufgaben in der Cloud realisiert werden. Ohne eine politische Gegensteuerung wird 2020 die Cloud-Infrastruktur zu 80 Prozent aus USA und zu 15 Prozent aus China stammen.

3.3 IT-Sicherheit

Aufgrund der zunehmenden Bedeutung von KI muss deren Entwicklung und Anwendung höchsten Sicherheitsstandards genügen, da die Selbstlernfähigkeit eines vorsätzlich oder fahrlässig korrumpierten KI-Systems dessen Schadensrisiko erhöht. Die Fähigkeit, sichere KI zu entwickeln, ist elementar für die digitale Souveränität Deutschlands und Europas.

Dazu gehören vertrauenswürdige Netz-Infrastrukturen, sichere Soft- und Hardware sowie Cloud- und Verschlüsselungstechnologien auf höchstem Sicherheitsniveau. In einem digital souveränen Deutschland darf es keine IT-Schnittstellen geben, über die Dritte unbefugt Daten einsehen, kopieren oder verändern können.

Solange Unternehmen Verlust oder Manipulation sensibler Daten befürchten müssen, werden sie sich nur eingeschränkt digitalisieren. Daher müssen kleine und mittlere Unternehmen möglichst rasch ein Sicherheitsniveau erreichen, das dem von großen Unternehmen zumindest nahekommt.

Die deutsche IT-Sicherheitswirtschaft ist technologisch innovativ, im internationalen Vergleich jedoch eher kleinteilig. Damit IT-Sicherheit „Made in Europe“ auch mittelfristig bestehen kann, brauchen die heimischen Anbieter – öffentlich geförderte – Leuchtturmprojekte.

Für eine europaweit kohärente Cybersicherheitspolitik muss Deutschland seine Regulierungsvorhaben auf EU-Ebene abstimmen und die europäischen Initiativen zur Standardisierung von *Security by Design* und *Security by Default* vorantreiben.

3.4 Zugang zu Daten, Transparenz und Nachvollziehbarkeit

Damit Staat, Wirtschaft und Wissenschaft gleichermaßen von der Digitalisierung profitieren, müssen sie einerseits bestimmen können, wer auf die von ihnen generierten Daten zugreifen kann, wie diese genutzt werden, welche Schlüsse daraus gezogen und an wen die Ergebnisse übermittelt werden. Andererseits müssen sie in der Lage sein, in eigenen Systemen generierte sowie öffentlich verfügbare Daten möglichst weitgehend für eigene Produkte und Dienstleistungen zu nutzen. Ferner müssen sie die von ihnen verwendeten Systeme verstehen, modifizieren und mit anderen Systemen kombinieren, um Produkte möglichst einfach an neue Anforderungen anpassen und neue Produkte und Angebote selbst gestalten zu können. Diese Fähigkeit zur innovativen Schaffung neuer Produkte wird auch durch eine möglichst breite öffentliche Verfügbarkeit von Daten („Open Data“) und frei einsetzbarem Programmcode („Open Source“) gefördert. Staat und Unternehmen dürfen kritische Daten nur in Systemen verarbeiten, bei denen sie sowohl die Hoheit darüber haben, wer auf diese Daten zugreifen kann, und bei denen sie die betreffenden Daten jederzeit auch in andere Systeme übertragen und durchsetzbar im ursprünglichen System löschen können. In kritischen und strategisch wichtigen Systemen muss der Programmcode überprüfbar sein, um absichtlich oder unabsichtlich eingebaute Hintertüren aufspüren zu können. Der Programmcode muss anpassbar und in andere Systeme übertragbar sein, um Probleme notfalls eigenständig beheben (lassen) zu können, um Lösungen in andere Rechenzentren übertragen und um die Interoperabilität bereits eingesetzter Lösungen zu neuen Systemen gewährleisten zu können. In Bezug auf KI müssen sich die Ergebnisse dieser Systeme replizieren lassen und durch modifizierten Programmcode verbessert werden können. Dazu sollten Unternehmen und wissenschaftliche Institutionen in einen innovativen Wettbewerb um die jeweils beste Lösung treten können.

3.5 KI und technologische Kompetenzen

Die Querschnittstechnologie KI wird heute in vielen Anwendungsfeldern eingesetzt – eine KI-bezogene Untersuchung digitaler Souveränität muss daher diese Anwendungsszenarien mit ihren spezifischen technologischen Kompetenzen stets gemeinsam betrachten. KI-basierte Anwendungen umfassen in unterschiedlichen Anteilen die vier Kernfähigkeiten Wahrnehmen, Verstehen, Handeln und Lernen. Der rasante Fortschritt im Internet of Things macht den KI-Systemen zudem immer neue Daten und Prozesse zugänglich. Die stark wachsende Leistungsfähigkeit KI-basierter Systeme und die rasante Innovationsdiffusion führen zu einer gefühlten „permanenten Disruption“ und damit auch zu ernstzunehmenden Ängsten in Teilen der Bevölkerung, einem nicht mehr aufhaltbaren Prozess unterworfen zu sein, der den Alltag massiv verändert und die gesellschaftliche Verankerung in Frage stellt. Gleichzeitig ist eine moderne Informationsgesellschaft ohne KI nicht länger vorstellbar. Deutschland und Europa müssen bei der technologischen Entwicklung an der Weltspitze dabei sein – nicht nur im Bereich der KI, sondern auch in den eng mit KI verzahnten Technologiefeldern. Alles andere wäre ökonomisch und gesellschaftlich verhängnisvoll. Grundlegende digitale Technologien würden dann in Teilen der Welt entwickelt, in denen andere kulturelle Vorstellungen herrschen.

Blockchain & Distributed Ledger-Technologien (DLT) sind Kerntechnologien mit dediziert dezentralem Organisationsansatz, die das Oligopol der wenigen Anbieter sozialer Netzwerke und Plattformen brechen können. Die Verbindung von KI und dem Internet der Dinge schafft neue Marktmechanismen, bei denen Daten zunehmend als virtuelle Werte verstanden werden, deren digitale Einmaligkeit beim Austausch sichergestellt werden muss. Genau dies ermöglichen Blockchain- und DLT-Infrastrukturen, ohne dass marktbeherrschende digitale Handelsplattformen einen großen Teil der Wertschöpfungsgewinne vereinnahmen können.

Digitale Plattformen verändern die traditionelle Beziehung zwischen Lieferant und Kunde, indem sie selbst einen direkten Zugang zum Kunden herstellen. Der Plattformbetreiber wird bei jeder Transaktion mit einem Teil der Transaktionssumme beteiligt. Im Vergleich zu den USA und China spielt Deutschland als Plattformbetreiber derzeit keine wesentliche Rolle – mit entsprechenden Konsequenzen für die Verteilung der Wertschöpfung. Diese Entwicklung kann sich durch den zunehmenden Einsatz von KI-Technologien weiter verstärken. Eine chancenorientierte Regulierung auf deutscher und europäischer Ebene kann die Fähigkeit auch mittelständischer Unternehmen, digitale Plattformen zu entwickeln und möglichst weltweit zu vermarkten, jedoch stärken.

Mit **High Performance Computing (HPC)** lassen sich natürliche Prozesse modellieren oder simulieren sowie sehr große Datenmengen analysieren. HPC ermöglicht somit Erkenntnisse, die – sofern überhaupt anderweitig möglich – nur mit sehr aufwändigen Experimenten oder direkt in der Praxis erlangt werden könnten. Im Sinne digitaler Souveränität müssen diese Systeme auch in Deutschland und Europa entworfen und hergestellt werden können.

Quantum Computing kann ebenfalls Probleme lösen, die mit klassischen Computern niemals erreichbar wären, stellt dabei allerdings große Herausforderungen: Zum einen unterscheidet sich die Algorithmik stark von den bisher gelehrten Verfahren, zum anderen erfordert die Entwicklung von Quantum-Computern die Beherrschung von extremen physikalischen Zuständen. Im Sinne einer digitalen Souveränität ist die Ausbildung von Hardware- wie auch Software-Spezialisten für die Weiterwicklung des Quantum Computing erforderlich.

Die **Mikro- und Nanoelektronik** stellt grundlegende Bausteine für die Digitalisierung bereit, wobei Halbleiter die reale (analoge) Welt mit der virtuellen (digitalen) Welt verbinden. Dies gilt gleichermaßen für die Fertigungsindustrie wie auch für intelligente Infrastrukturen in den Bereichen Energie, Mobilität, Gesundheit sowie E-Government.

3.6 Digitale Kompetenzen

Für Aufbau und Erhalt der digitalen Souveränität sind – ausgehend von dem Schichtenmodell (s. Anhang) – insbesondere folgende Kompetenzen erforderlich.

- **Ebene der Daten:** Erforderlich sind technische und methodische Kenntnisse (grundlegende Informatik- und IT-Kenntnisse, mathematische Kenntnisse, statistische Methoden, Data Analytics), um den Wert der Daten für das Unternehmen einschätzen zu können und Daten-bezogene Anwendungen (z. B. Analysen, Business Intelligence, Machine Learning etc.) zielorientiert nutzen zu können.

- **Ebene der Schnittstellen und Infrastrukturen:** Zentrale Kompetenz ist die Fähigkeit, offene Schnittstellen und (De-facto-)Standards zu entwickeln, die die souveräne Gestaltung von Ökosystemen oder die sichere Integration externer Lösungen erlauben.

- **Ebene der Quellcodes:** Ein souveräner Umgang mit Quellcodes im Sinne von Entwicklung, Prüfung, Veränderung und Verständnis erfordert erweiterte Software-Kompetenzen (Programmierfähigkeiten sowie analytisch/konzeptionelle Lösungskompetenzen).

- **Ebene der Kontrolle/des Verständnisses:** Hier sind v. a. Hintergrundwissen über und Verständnis der hinter den Technologien und Plattformen stehenden Prinzipien erforderlich.

Übergreifend über alle Schichten erscheint es zudem unabdingbar, gezielt Kompetenzen im Kontext der KI als zukünftig disruptive Querschnittstechnologie aufzubauen. Diese umfassen technisch-analytische Kompetenzen (v. a. Machine Learning) in gleicher Weise wie (Meta-)Kompetenzen wie Kreativität, um KI-basierte Lösungen und Anwendungen weiter- und neu entwickeln zu können.

EXKURS: Case Study: Mustererkennung in der Gesundheitswirtschaft

Welche Aspekte der digitalen Souveränität im Zusammenhang mit KI berücksichtigt werden müssen, ist Gegenstand der folgenden Auseinandersetzung. Sie konzentriert sich auf die zunehmende Anwendung der bildgestützten Mustererkennung in medizinischen Daten.

Digitalisierung und Medizin

Die Digitalisierung der Medizin ist bereits weit vorangeschritten. Im Bereich medizinischer Bilddaten, wie Computertomographie (CT) und Magnetresonanz-Tomographie (MRT), liegen teils jahrzehntealte Bestände in den Archiven der Kliniken, die sich prinzipiell für retrospektive Analysen anbieten. Zudem können moderne CT- und MRT-Scanner immer detailliertere Bilder in kürzerer Zeit aufzeichnen, so dass die Datenmenge und damit Arbeitsbelastung der Radiologen schnell zunimmt. Der Druck, computerbasierte Methoden zur Effizienzsteigerung einzusetzen, ist entsprechend hoch. Daher wurden KI-Algorithmen vor allem im Bereich der medizinischen Bildgebung bereits in beachtlicher Zahl und Qualität implementiert und validiert, und die ersten schon mit behördlicher Zulassung versehen. Das sind datengetriebene Algorithmen, die der Mustererkennung in Bildern dienen. Eine Vielzahl populärer Methoden wird mit dem Begriff *Deep Learning* zusammengefasst. Die Lösungen, die mithilfe KI entwickelt werden, sollen dem Arzt eine neue Perspektive auf den Patientenstatus bieten. Solche Anwendungen dürfen allerdings nicht als Arzt-Ersatz betrachtet werden. Mediziner müssen weiterhin die Möglichkeit haben, die aus den Daten extrahierten Merkmale zu validieren. Die Ergebnisse von Entscheidungsunterstützungssystemen müssen nachvollziehbar sein und dürfen lediglich zur Unterstützung benutzt werden. Bilderkennung ist dabei ein sehr relevantes Werkzeug, das eine bessere Behandlung und dadurch eine Verbesserung der Lebenserwartung bedeuten kann. Allerdings sind die Erfahrung und das Wissen des Experten unabdingbar, um dieses Ziel zu erreichen.

Die Datenproblematik

Noch gibt es kaum Erkenntnisse darüber, wie viele Daten genau benötigt werden, um KI-Algorithmen zu trainieren, denn die genaue Komplexität der zugrundeliegenden biomedizinischen Problemstellung ist prinzipiell unbekannt. So ist im Widerspruch zum Grundsatz der Datensparsamkeit häufig ein „je mehr, desto besser“ die Richtschnur bei der Datensammlung. Sicher ist, dass die für robuste Ergebnisse notwendige Menge mit der Variabilität der Daten korreliert, so dass zu erwarten ist, dass die aufgabenangemessenen Datenmengen weiter steigen und die Nachfrage an großen Datensammlungen zunehmen werden. Der Umgang mit solchen sensiblen, persönlichen Daten braucht eine Vertrauensbasis, die institutionalisiert werden sollte. Diese Vertrauensbasis hat mehrere Ebenen. Auf der individuellen (Patienten-)Ebene muss garantiert werden, dass die Daten nicht unkontrolliert weitergegeben werden. Aber auch ein Vertrauen in die Wissenschaftler und in die, die KI-Algorithmen trainieren und vermarkten möchten, ist notwendig, denn sie sind auf Datenzugang angewiesen. Dabei kommt es nicht darauf an, die Krankheitsgeschichte Einzelner zu rekonstruieren. Der Schutz der Persönlichkeitsrechte durch Anonymisierung der Daten ist deshalb gut mit dem Forschungsinteresse vereinbar, das auf die Analyse von Gruppeneffekten abzielt.

Transparenz der Algorithmen

Wer heute ein Verfahren des maschinellen Lernens und der Künstlichen Intelligenz einsetzt, muss sich immer der Tatsache bewusst sein, dass es das eine Verfahren, das alle Probleme löst und alle Fragen beantwortet, nicht gibt. Eine Person muss bewusst Modelle auswählen und konfigurieren, eine Person wählt die Daten aus, und eine Person wählt die Verfahren aus, mit denen die Modelle letztlich trainiert werden. In jede dieser Entscheidungen fließen Anforderungen, Fragestellungen und Vorwissen ein. Auf diese Weise ist sichergestellt, dass neue, bessere Verfahren auf neuen Erkenntnissen gebaut werden können. Doch in jede dieser Entscheidungen fließen immer auch Annahmen, Vorurteile und vor allem Ziele ein. Aber man sieht einem KI-System die einwirkenden Annahmen und Ziele nicht mehr an. Denn das Grundprinzip des maschinellen Lernens ist ja, dass der Mensch ab einem bestimmten Punkt beim Lernen

nicht mehr eingreift. Spätestens dann muss man zwischen KI-Systemen unterscheiden, die beispielsweise autonom technische Anlagen steuern, und solchen, mit denen eigenständig entschieden würde, ob einer Person ein Kredit gewährt oder ein Medikament verschrieben wird. Diese Systeme unterscheiden sich kaum in ihrer Technik, sie unterscheiden sich darin, wer die Folgen zu spüren bekommt. Vertrauen spielt eine wesentliche Rolle bei der Anwendung solcher datengetriebenen Algorithmen. Menschen können nicht mehr vollständig kontrollieren und beweisen, welche Merkmale in den Daten ein Ergebnis begründen. Das läuft vielen Zulassungsverfahren und rechtlichen Grundforderungen zuwider, die die Erklärbarkeit von Algorithmenergebnissen einfordern. Aber vor allem die Akzeptanz bei Ärzten und Patienten würde von Mechanismen profitieren, die eine Einsicht in die Arbeitsweise des Algorithmus bieten und für jedes Ergebnis die Faktoren aufzeigen, die in den individuellen Daten den Ausschlag gaben. Denn viele Ängste und moralische Bedenken sind mit KI-Algorithmen verknüpft, weil Gesundheitsdaten wohl zu den persönlichsten und intimsten Daten gehören, die es gibt.

Alle technischen Systeme und Prozesse implementieren die Werte und Ziele dessen, der sie baut. Das sind nicht unbedingt die Menschen, die direkt von den Ergebnissen der Algorithmen betroffen sind. Insbesondere dann, wenn Patienten nicht frei entscheiden können, ist gesellschaftlich verantwortliches Denken und Handeln erforderlich. In einer offenen Gesellschaft müssen Ziele und Zielkonflikte stets artikulierbar und verhandelbar sein. Genau das macht uns als Gesellschaft und als Akteure souverän. Es ist noch eine der größten Herausforderungen der Forschung, das „Wissen“ einer Künstlichen Intelligenz lesbar oder zumindest sichtbar zu machen. Einen Schachcomputer zu bauen, der jeden Menschen schlägt, ist eine Sache. Einen Schachcomputer zu bauen, der seine Art des Schachs auch nur einem Menschen beibringen könnte, eine ganz andere.

Datenhoheit

Eine weitere wichtige Frage im Sinne der Datensouveränität betrifft das „Eigentum“ an den Daten. Gehören sie dem Patienten, dem Krankenhaus, der Versicherung? Die Frage nach den Rechten an datengetriebenen Algorithmen und der Teilhabe an Gewinnen, die mit ihnen erzielt werden, ist damit eng verknüpft. Gesundheitsdaten sind „Eigentum“ der Patientinnen und Patienten. Im Allgemeinen fallen diese Daten unter einen strengen Schutz des Gesetzes, solange sie personenbezogen sind. Anonymisierte Daten dagegen unterliegen nur einer weitaus schwächeren Restriktion. Nun ist der Tatbestand der Anonymisierung daran gekoppelt, welchen Aufwands es bedarf, auf die Person zurückzuschließen. Bei vielen Daten ist eine Anonymisierung daher ausgeschlossen, da sie die Person sofort preisgeben. Genetische Daten gehören dazu, und selbst ein Schädel-CT kann mit wenig Aufwand so dargestellt werden, dass etwa ein Abgleich mit der Facebook-Gesichtserkennung möglich wäre.

Wenn also Gesundheitsdaten laut Gesetz nicht mehr verwendet werden dürften, aber andererseits viele Menschen vermutlich bereit wären, ihre Daten für bestimmte wissenschaftliche Studien (oder marktwirtschaftliche Verwertung) an bestimmte Einrichtungen (oder Firmen) zur Verwendung freizugeben, auch wenn Rückschlüsse auf ihre Person möglich wären, ist eine Regelung angezeigt, die eine Datenverwendung auch auf einfache Weise ermöglicht. Datensouveränität könnte bedeuten, dass Patienten frei entscheiden können dürfen, wo ihre personenbezogenen Daten gesammelt werden und vor allem wer darauf Zugriff erhalten soll – ganz im Sinne einer „Datenspende“. Zudem geht es um die Entscheidung darüber, wem sie welche Verwertungsrechte auch an anonymisierten Derivaten einräumen wollen – und für welche Gegenleistung. Die Umsetzung der Möglichkeit zur Einwilligung der Datennutzung ist allerdings noch weit vom Wünschenswerten entfernt. Beides, das souveräne Recht, die eigenen Daten gegen Verbreitung gesichert zu wissen, wie das Recht, sie für bestimmte Zwecke freizugeben, ist also durch die heutige Implementierung behindert.

4. Rollen, Verantwortlichkeiten und Handlungsempfehlungen zur Sicherung der digitalen Souveränität

Bei der (Wieder-)Herstellung und Sicherung digitaler Souveränität in Deutschland und Europa ist für die Zuschreibung von Rollen und Verantwortlichkeiten ein Mehr-Ebenen-Ansatz zwingend. Vor allem angesichts eines internationalen Wettbewerbsumfeldes, welches sich im KI-Kontext auch politisch motiviert weiter zuspitzen wird, ist ein innovationsdynamisierender, Hand in Hand gehender Ansatz von Politik, Wirtschaft sowie Wissenschaft und Forschung notwendig. In einem entsprechend konzertierten Ansatz können die unterschiedlichen Kräfte der Akteursgruppen essentiell wirken und mit Blick auf die Stärkung der digitalen Souveränität auf europäischer Ebene koordiniert und integriert werden, um Ineffizienzen durch überlappende Strukturen zu vermeiden. Der Ansatz eines Coordinated Action Plan on AI zwischen den Mitgliedstaaten sollte also konsequent verfolgt werden.

Flankierend ist eine neue Ausrichtung des öffentlichen Diskurses notwendig, bei dem auch zivilgesellschaftliche Akteure eine besondere Bedeutung besitzen. Zur Erhöhung der digitalen Selbstbehauptung Europas und auch zur digitalen Selbstbestimmtheit des Einzelnen ist eine grundsätzlich innovationsoffene Debattenkultur zielführend. Denn vor allem im Kontext von KI-Entwicklungen spielt ein Wertebezug eine entscheidende Rolle, so dass auch in der gesellschaftlichen Aufklärung Ansätze fruchten sollten, die die Entwicklung von auf europäischen Werten fußenden Produkten und Anwendungen ermöglichen.

4.1 Politik und Verwaltung

Künstliche Intelligenz muss zu einem wichtigen Gegenstand der europäischen Industrie- und Standortpolitik werden. Wenngleich die Prinzipien des möglichst freien Welthandels erstrebenswert sind, darf, unter Berücksichtigung der mit Deutschland bzw. der EU abgeschlossenen Handelsverträge, nicht außer Acht gelassen werden, dass Europa sich in einem globalen Wettbewerbsumfeld hochinnovativer Regionen befindet. Deswegen kann auch ein Ansatz zur Gestaltung des europäischen Digital-Binnenmarkts als geschützter Innovationsraum erwogen werden. Dazu zählt u. a. ein echtes Level-Playing-Field und auch, dass öffentlich geförderte KI-Grundlagenforschung stärker auf konkrete Anwendungsbereiche ausgerichtet werden sollte. Im Kontext der Forschungsförderung ist der Aufbau überregionaler Forschungs- und Kompetenzzentren, z. B. nach dem Vorbild des Deutschen Forschungszentrums für KI (DFKI), sowie länderübergreifender Forschungs- und Innovationsnetzwerke für die Wettbewerbsfähigkeit Europas bei KI entscheidend. Zudem besitzt der Staat aber auch eine weitergehende Verantwortung als Leitinvestor und Treiber von Leuchtturmprojekten. Darüber hinaus verantwortet die Politik die Gestaltung regulatorischer Rahmenbedingungen. Anstelle einer Ex-ante-Regulierung für KI sollte der bestehende Rechtsrahmen aufgrund möglicher neuer Anforderungen – etwa an die Cyber- und Informationssicherheit oder an das Wettbewerbsrecht – weiterentwickelt werden. So sollte zur Sicherung eines wettbewerblichen Marktumfelds das Wettbewerbsrecht mit dem notwendigen Instrumentarium ausgestattet werden, um Marktmachtmissbräuche beim exklusiven Zugang zu Daten und Plattformen zu ahnden und sich mit neu aufkommenden Fragen wie der algorithmischen Preisgestaltung auseinanderzusetzen. Um Innovations- und Investitionspotenziale in KI bestmöglich zu heben und im EU-Binnenmarkt zu taxieren, ist auch das EU-Vergaberecht entsprechend zu prüfen.

Handlungsempfehlungen:

- Schaffung investitionsfreundlicher und -fördernder Rahmenbedingungen für den Aufbau notwendiger Infrastrukturen, in denen es nicht mehr allein auf Bandbreite, sondern zusätzlich auf Rechenleistung, Latenz und Datenintegrität ankommt (Stichworte 5G, Edge-Computing, Rechenzentren). Hier sollte auch eine staatliche Förderung entsprechender Infrastrukturen geprüft werden.

- Errichtung eines echten Level-Playing-Fields auf europäischer Ebene, so dass wettbewerbsfähige europäische Angebote entstehen können. Darüber hinaus sollte die öffentliche Hand bei entsprechenden europäischen Lösungen selbst auch als Leitnachfrager fungieren (Stichworte: Cloud-Computing, Datenpolitik).

- Kontroll- und Innovationsfähigkeit müssen dadurch gesichert werden, dass kritische Daten der Verwaltung nur in Systemen verarbeitet werden, bei denen staatliche Organe nicht nur die Hoheit darüber haben, wer auf diese Daten zugreifen kann, sondern bei denen sie die betreffenden Daten jederzeit auch in andere Systeme übertragen und durchsetzbar im ursprünglichen System löschen können.

- Bei öffentlicher Beschaffung sollten Software- und Cloud-Angebote grundsätzlich bevorzugt werden, bei denen der Quellcode geprüft und geändert werden kann; bei kritischen und für digitale Souveränität strategisch wichtigen Systemen darf ausschließlich Software verwendet werden, bei der das der Fall ist. Ebenso sollte ein mit staatlichen Mitteln erstellter Programmcode als Open Source veröffentlicht werden, analog zu der für Bundesbehörden in den USA geltenden Source Code Policy.

- Daten sind die Essenz jeglicher Digitaltechnologie. Daher ist auch unter Souveränitätsaspekten die Frage nach der Verfügbarkeit von und der Zugriff auf Daten von besonderer Wichtigkeit. Insofern braucht es eine Datenpolitik, die dort, wo möglich, Daten nutzbar macht (bspw. nicht-personenbezogene Daten öffentlicher Stellen) und gleichzeitig entsprechende Sicherheitsansprüche an die Datenverarbeitung in kritischen IT-Systemen stellt. Dies beinhaltet aber auch eine kritische Reflexion bestehender Regulierungen (Stichworte: Open-Data, DSGVO, ePrivacy, EU-Urheberrecht/Text-and-Data-Mining).

- Die Programme der Forschungsförderung sollten finanzielle Anreize setzen, dass die Zuwendungsempfänger ihre Forschungsergebnisse, Codes und Daten veröffentlichen. So könnten heute nicht vollumfänglich genutzte Forschungsergebnisse einer breiteren Basis von Unternehmen und Forschungseinrichtungen zugänglich gemacht werden, um darauf aufbauend mehr Innovation zu ermöglichen. Auch sind Modelle zur intensiveren Kooperation von Forschung und Wirtschaft zur Entwicklung markt- und anwendungsnaher Angebote anzustreben.

- IT-Sicherheit ist als Grundvoraussetzung digitaler Souveränität Design-Prinzip auch für KI-Entwicklungen und kann in dieser Funktion auch Standortvorteil für Europa werden. Dazu bedarf es aber eines umfassenden Maßnahmenpaketes, welches sich nicht nur auf den kleinsten gemeinsamen internationalen Nenner beschränkt, sondern, gepaart mit der Marktstärke Europas, weltweit gültige Standards setzt. Vor allem angesichts der zunehmenden KI-basierten Mensch-Maschine-Interaktionen steigt die Bedeutung der Gewährleistung von IT-Sicherheit als Voraussetzung für die Produktsicherheit und als Bestandteil selbstbestimmten Handelns. Daher ist die regulatorische Fokussierung auf Betreiber kritischer IT-Infrastrukturen zu hinterfragen und eine adäquate Verpflichtung für Hard- und Softwarehersteller auf adäquate Sicherheitsstandards und -maßnahmen im Sinne der Stärkung des Marktortes Europa anzustreben (Stichworte: IT-Sicherheitsgesetz/NIS-Richtlinie, Cybersecurity Act, Produktsicherheitsrichtlinie).

- Europa muss leistungsfähige KI-Forschungs- und Innovationscluster aufbauen, die mit denen in den USA und in China konkurrieren können. Dies erfordert verstärkte und koordinierte Anstrengungen von Wissenschaft, Industrie und Regierungen in ganz Europa. Wesentliche Bausteine sind eine bessere Mittelausstattung der KI-Forschungsförderung, stärkere Anreize für Gründungen und Wachstum von Unternehmen sowie die höhere Attraktivität des hiesigen Standortes für (inter-)nationale KI-Spezialisten, um Abwanderung ins Ausland zu vermeiden und Spezialisten aus dem Ausland ansprechen zu können (Stichworte: Anwendungsorientierte Forschungsförderung, steuerliche Forschungsförderung für alle Unternehmen).

- Erforderlich ist die Stärkung der Aus- und Weiterbildung gemeinsam mit den Bundesländern, Wirtschaft und Wissenschaftseinrichtungen mit dem Ziel, digitale Kompetenzen der Menschen (v. a. analytische, mathematische, IT-technische und Programmierkenntnisse (MINT-Technologien)) auszubauen, Experimentierräume/Lernlabore für die Entwicklung kreativer Lösungen zu ermöglichen und die Anreize für eigenverantwortliche Weiterbildung zu erhöhen (Stichworte: Digitale Anschlussfähigkeit, Qualifikation von Lehrkräften, Aus- und Weiterbildung von Fachkräften/Fachkräftemangel).

4.2 Wirtschaft

Nicht nur aus Eigen- und Marketinginteresse muss sich die Wirtschaft an der öffentlichen Debatte über die Chancen und Herausforderungen der Digitalisierung im Allgemeinen und der KI im Speziellen ausgewogen beteiligen. Damit einher geht die Notwendigkeit einer intensiveren Aufklärungsarbeit hinsichtlich Transparenz und Nachvollziehbarkeit von Funktionalitäten und Entscheidungsrationalitäten von KI-Systemen sowie die Stärkung der Selbstbestimmtheit des einzelnen Nutzers. Zudem muss die Wirtschaft Verantwortung für die von ihr entwickelten digitalen Technologien übernehmen. Dazu gehört allen voran die Gewährleistung der Sicherheit von Produkten und Anwendungen gerade im KI-Umfeld (inkl. einer Prüfpflicht für „zugekaufte" Komponenten) sowie die Schaffung von Diensten, Anwendungen und Angeboten, die dem oben dargestellten Anspruch an Transparenz und Nachvollziehbarkeit Rechnung tragen.

Verantwortung trägt die Wirtschaft aber auch im Kontext der industriellen KI-Forschung. Hier sind die Unternehmen noch intensiver gefordert, ihre Innovationen besser in marktfähige Angebote zu transferieren. Dabei hilft Standardisierung, höhere Qualitätsniveaus zu erreichen und zu einer verbesserten Interoperabilität von IT-Systemen beizutragen. Gegenwärtig ist der Standardisierungsgrad bei KI aber noch geringer ausgeprägt als in anderen Teilbereichen der Informatik. Der Bedarf für einheitliche Standards wächst in der KI jedoch mit der zunehmenden Verbreitung ihrer Anwendungen. Hier gilt es an Vorarbeiten und Erkenntnisse, z. B. der Plattform Industrie 4.0 oder der 3GPP zu 5G, anzuknüpfen. Standards zu schaffen ist vorrangige Aufgabe der Industrie. Offen zugängliche Standards erleichtern zudem die Implementierung neuer Technologien insbesondere für den Mittelstand und über europäische Ländergrenzen hinweg. Dabei gilt es, für internationale Akzeptanz europäischer Standards zu werben. Standardisierungsorganisationen wie DIN und ISO haben bereits Arbeitsgruppen eingesetzt, die Qualitätsstandards für KI-Systeme definieren.

Angesichts der Investitionspotenziale außereuropäischer Anbieter sind auch höhere Forschungsinvestitionen der Unternehmen notwendig. Die Beteiligung der Industrie an anwendungs- und marktnahen Forschungskooperationen muss wettbewerbsrechtlich gesichert werden, ohne die Möglichkeiten für globale Kooperationen einzuschränken. Unternehmen sollten weniger auf eine Status-quo-bezogene digitale Transition ausgerichtet sein, sondern eine „radikale" Innovationsoffenheit an den Tag legen, die nachhaltige Wachstumschancen offerieren kann. Darüber hinaus sind, neben Anreizen der öffentlichen Hand, vor allem private Kapitalgeber gefordert, Investitionen in Gründungen als auch in das Wachstum von Start-ups zu intensivieren, damit diese es schaffen, über die Frühfinanzierungsphase hinaus zu bestehen, und ihr Wachstumspotenzial in Deutschland entfalten können.

Handlungsempfehlungen:

- Die Wirtschaft muss die Aufklärung der Öffentlichkeit intensivieren sowie verstärkt in Infrastruktur, Forschung und Entwicklung sowie in (Weiter-)Bildung investieren.

- Gemeinsam mit der Politik sollte der Aufbau und Betrieb einer zentralen, nationalen, vertrauensvollen allgemein zugänglichen Daten- und Analyseinfrastruktur inklusive des Aufbaus einer zugrundeliegenden Cloud-Plattform mit skalierbarer Speicher- und Rechenkapazität, auf Basis offener und interoperabler Standards, forciert werden, um aus Deutschland heraus Europa als starken Wirtschafts- und Wissenschaftsstandort in einer digitalisierten Welt nachhaltig zu sichern.

4.3 Wissenschaft und Forschung

Auch die Wissenschaft und Forschung wird sich stärker im Sinne der digitalen Souveränität ausrichten müssen. Ihr obliegt es zudem, politische und wirtschaftliche Steuerungsbedarfe zu artikulieren. Aufbauend auf dem bürgerlichen Grundrecht der Freiheit von Wissenschaft und Forschung ist die Wissenschaft i. S. der digitalen Souveränität gefordert, eine dem Gemeinwohl verpflichtete Grundausrichtung einzunehmen und weniger einer ausschließlich absoluten Begriffsbestimmung zu folgen. So wäre eine Festlegung von Forschungsschwerpunkten mit Bezug zur Sicherung der digitalen Souveränität erstrebenswert. Wissenschaft kann und sollte auch zu einer Stärkung der Innovationskultur und Erhöhung der Innovationsdynamik beitragen.

Handlungsempfehlungen:

- Ein kontinuierliches Technologie-Monitoring sollte möglichst konkrete Angaben über Einsatzgebiete und möglichen wirtschaftlichen Nutzen enthalten (Stichworte: „KI-Landkarte“, Forschungsfokussierung/anwendungsorientierte Forschung).

- Aufbau von Technologiekompetenzen durch entsprechende Grundlagen- und Anwendungsforschung, die die digitale Souveränität in verschiedenen Technologie- und Marktumfeldern stärkt (Stichworte: Blockchain- und Distributed-Ledger-Technologien, plattformökonomische Entwicklungen, High-Performance Computing, Quanten- und Edge-Computing).

Anhang: Schichtenmodell digitaler Souveränität

Grad digitaler Souveränität **Kategorien digitaler Souveränität**	**niedrige Ausprägung (= hohe Abhängigkeit)**	**mittlere Ausprägung**	**hohe Ausprägung (= keine Abhängigkeit)**
Daten	Der Anbieter und nicht der Anwender entscheidet, welche Daten er wem zur Verfügung stellt und wie er diese nutzt.	Anwenderorganisation hat vollständige Kontrolle darüber, wer Zugriff auf Daten hat und kann diese jederzeit löschen.	Daten können unabhängig von der eingesetzten Softwarelösung gelesen, geändert und gelöscht werden.
Schnittstellen	Keine oder nur proprietäre Schnittstellen verfügbar	Unterstützung einer hohen Anzahl offener Standards und Schnittstellen	Zugriff auf alle Daten und Funktionen über offene, frei nutzbare Schnittstellen mit quelloffener Referenzimplementierung
Quellcode	Quellcode nicht verfügbar	Quellcode prüfbar/Quellcode bei Ausfall des Herstellers verfügbar („Escrow“)	Quellcode veränderbar/verändert nutzbar
Hardware	Muss komplett zugekauft werden	Bestehende Lösungen können durch eigene Hardware ergänzt werden.	Alle Hardware-Komponenten können selbst produziert und beeinflusst werden.
Kontrolle	Die Lösung ist nur bei einem einzigen Anbieter verfügbar, es gibt keine Kontroll- oder Migrationsmöglichkeiten.	Wichtige Teile können kontrolliert und zu anderen Anbietern migriert werden, der Aufbau einer selbst betriebenen Lösung ist möglich.	Anwenderorganisation betreibt Lösung selbst und hat Kontrolle über alle Komponenten (Quellcode, Hardware, ...).
Kompetenzen	Kein Verständnis für Prozesse und Datenverwendung, keine Kompetenz zur Anpassung vorhanden	Verständnis von Daten und Prozessen ist vorhanden, Möglichkeiten zur Anpassung existieren in begrenztem Rahmen.	Kompetenzen für Veränderung von Daten, Programmcode und Prozessen sind vorhanden und verfügbar.
Jurisdiktion	Anbieter untersteht Nicht-EU-Recht.	Anbieter untersteht Nicht-EU-Recht, aber es bestehen verlässliche Verträge, welche die Einhaltung europäischer Standards sicherstellen.	Anbieter befindet sich in Deutschland bzw. in der Europäischen Union und untersteht ausschließlich dieser Jurisdiktion.

1 Leitplanken digitaler Souveränität, Positionspapier der Fokusgruppe 1 zum nationalen IT-Gipfel 2015, Berlin 2015, S. 1 (https://www.de.digital/DIGITAL/Redaktion/DE/Downloads/it-gipfel-2015-leitplanken-digitaler-souveraenitaet.pdf).

2 Vgl. Dai, Xin: Toward a Reputation State – The Social Credit System of China, Shandong Sheng 2018.

3 Im politischen Diskurs wird auch die „Datensouveränität“ (in Abgrenzung zu volkswirtschaftlicher digitaler Souveränität) als (Teil-)Bestandteil der individuellen digitalen Souveränität verstanden.

4 Siehe z.B. Westermann/Hunter: IT Risk: Turning Business Threats into Competitive Advantage by George Westerman (2007-08-21). Harvard Business Review Press. ASIN: B01JXQ8ORW.