Kapitel 2

UNTERNEHMEN

Digitale Souveränität – ein mehrdimensionales Handlungskonzept für die deutsche Wirtschaft

–

Privatheit und digitale Souveränität in der Arbeitswelt 4.0

V. Wittpahl (Hrsg.), *Digitale Souveränität*,
DOI 10.1007/978-3-662-55788-4_2, © Der/die Autor(en) 2017

Quellenangaben: Anhang, Quellenverzeichnisse der Zahlen und Fakten

__35 Prozent__ der deutschen Unternehmen verwenden Big-Data-Lösungen. __65 Prozent__ der Unternehmen nutzen Cloud Computing. __81 Prozent__ der Handwerksbetriebe sind generell aufgeschlossen für die Digitalisierung. __51 Prozent__ aller Unternehmen in Deutschland sind zwischen 2013 und 2015 Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden. __82 Prozent__ der Deutschen sind am Arbeitsplatz von Digitalisierungsprozessen betroffen, __30 Prozent__ sehr stark. __48 Prozent__ sagen, dass digitale Technologien für die Arbeit im Betrieb unverzichtbar geworden sind. __91 Prozent__ der Internetnutzer finden wichtig zu wissen, welche persönlichen Daten über sie im Internet gespeichert werden – gleichzeitig glauben __82 Prozent__, dass die meisten Unternehmen die Daten ihrer Kunden auch an andere Unternehmen weitergeben.

2.1 Digitale Souveränität – ein mehrdimensionales Handlungskonzept für die deutsche Wirtschaft

Christoph Bogenstahl, Guido Zinke

Digitalisierung, intelligente Algorithmen, Big Data, Internet der Dinge, Dienste und Energie, ermöglicht durch eingebettete Technologien (Embedded Technologies), besitzen enorme Innovationspotenziale für die Wertschöpfung. Parallel dazu digitalisiert sich die Arbeitswelt. Unternehmen nutzen Netzwerkstrukturen und offene Innovationssysteme. Und nicht erst durch die zu erwartende Reindustrialisierung wird das produzierende Gewerbe wieder aufleben – vor allem in Deutschland.

Um komparative Vorteile für die deutsche Wirtschaft zu erhalten, sind nicht nur Investitionen in digitale Technologien notwendig, sondern auch in die Fähigkeiten, diese selbstbestimmt zu nutzen und die Entscheidungshoheit – einhergehend mit einer hinreichenden Verfügbarkeit von Daten – im digitalen Raum zu bewahren. Für innovative Volkswirtschaften wird die digitale Souveränität zum entscheidenden Entwicklungsfaktor für die Zukunft.

Spezialisierungsvorteile in der Produktionstechnik aufgrund hoher Leistungsfähigkeiten in Forschung und Entwicklung sowie der Freisetzung von innovativen Produktionstechnologien waren seit jeher jene Triebfedern, die Deutschlands Aufstieg zu einer der weltweit führenden Industrienationen ebneten. Industrie 4.0 und der Ein-

Der lange Schatten der Industrie 4.0

Die Industrie 4.0 ist eine Folge von Trends, die zum Teil bereits seit 70 Jahren laufen. So waren „flexible Automatisierung" oder „Stückzahl Eins" Schlagworte, die schon in die 1980er Jahre – mit der Diskussion um die Folgen neuer Technologien, vollautomatische Produktion und maschinendominierte Arbeitswelten in Science-Fiction-Romanen – passten.

Und die Verschmelzung von Identifikations-, Kommunikations- und Informationssystemen mit Produktentwicklung, Produktion und Logistik hat ihren Ursprung bereits in Rohrpostsystemen, Telefonen und Telegrafen. Mit den neuen digitalen Technologien und der Ausprägung von Internet der Dinge, Internet der Dienste, Internet der Personen oder Industrial Internet wird ein vorläufiger Höhepunkt erreicht. Nun geht es um die komplexe Vernetzung eingebetteter Systeme miteinander und mit anderen Datenverarbeitungsgeräten über lokale und globale Netze, Daten- (Grid-/Cloud-Computing) und Kommunikations-(infra)strukturen.

Textbox 2.1.1: Der lange Schatten der Industrie 4.0

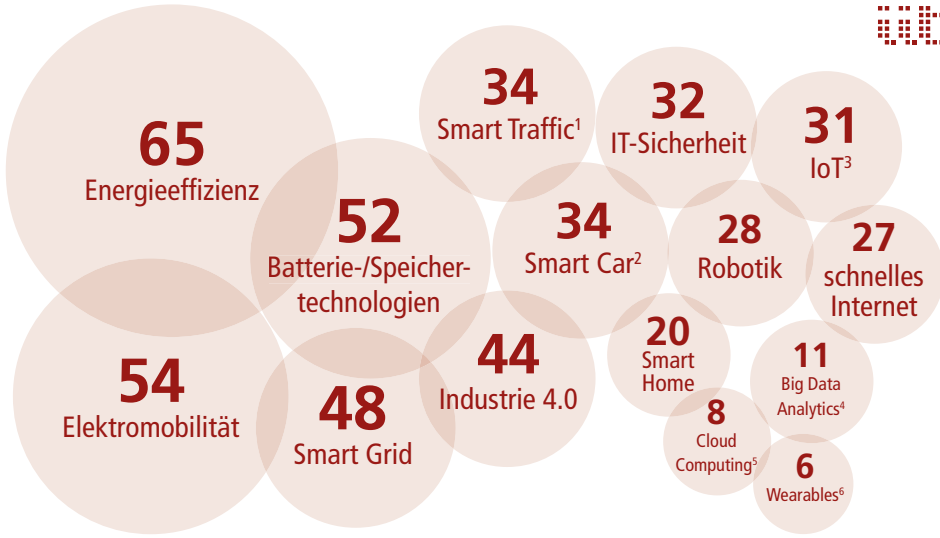

Abbildung 2.1.1: Technologiebereiche mit großen Potenzialen für den Standort Deutschland (in Prozent der Zustimmungen)[1]. Quelle: in Anlehnung an VDE 2016; eigene Darstellung

satz digitaler Technologien schaffen neue Potenziale für die deutsche Volkswirtschaft, die genutzt werden müssen, um Spitzenpositionen zu halten und weiter auszubauen.

Profitieren werden nicht nur solche Wirtschaftszweige, die man gemeinhin schnell mit digitalen Lösungen in Zusammenhang bringt, wie etwa die Branchen Informations- und Kommunikationstechnik, Elektronik, Maschinen- und Anlagenbau oder Automobilwirtschaft. Profitieren werden auch jene Wirtschaftszweige, bei denen die Digitalisierung kein unmittelbar offensichtlicher Bestandteil der Wertschöpfung ist. In der Agrar- und Landwirtschaft zum Beispiel sind digitale Vernetzung und eine über Navigationssatelliten geführte autonome Steuerung von Landmaschinen schon heute alltäglich. Auch einer plattformbasierten Integration vieler Klein- und Kleinstbetriebe wird erhebliches Potenzial zugesprochen, da Unternehmen sich so effizienter austauschen und höhere Sichtbarkeiten sowie größere Angebotsreichweiten erreicht werden können (vgl. Bauer et al. 2014).

[1] *Hinweise: (1) einschließlich intelligente Verkehrssteuerung; (2) einschließlich autonomen Fahren; (3) Internet of Things = Internet der Dinge; (4) einschließlich Data Mining (systematische Anwendung statistischer Methoden auf große Datenbestände / Big Data); (5) Bereitstellung von IT-Infrastruktur (Speicherplatz, Rechenleistung, Software) über das Internet; (6) tragfähige Datenverarbeitungsgeräte*

Große Potenziale aus der Digitalisierung werden für den deutschen Wirtschaftsstandort vor allem in den in der Abbildung 2.1.1 dargestellten Technologiebereichen erwartet (vgl. VDE 2016).

Zugleich macht die Digitalisierung nicht Halt vor der Arbeitswelt. Mittlerweile schaffen die internetbasierte Bereitstellung von IT-Infrastruktur (Cloud Computing) und technische Möglichkeiten zur virtuellen Realität (Wahrnehmung der Wirklichkeit in einer computergenerierten, interaktiven virtuellen Umgebung) erhebliche Erleichterungen am Arbeitsplatz (siehe Textbox 2.1.2). Reisezeiten und Umweltbelastungen können reduziert werden, wenn Meetings vermehrt in virtuellen Konferenzräumen, gegebenenfalls unterstützt von holografischen Projektionen, stattfinden.

Noch stärkeren Einfluss wird die künstliche Intelligenz auf bekannte Arbeitsformen haben. Lern- und sehr leistungsfähige neuronale Netze (Deep Learning) sind immer mehr in der Lage, eigentlich menschliche Fähigkeiten zu substituieren: Mimik zu erkennen, Maschinen zu warten und Krankheiten zu diagnostizieren. Nicht immer sichtbar, aber umfangreich wird künstliche Intelligenz schon in der Personalgewinnung, im Marketing als digitale textbasierte Assistenz (Chat Bots) oder in Legal Techs (siehe Textbox 2.1.3) eingesetzt. Im Bereich der autonomen Systeme und Robotik entlasten kollaborative Roboter, kurz Cobots, ihre menschlichen Kollegen, denn sie können mit dem Menschen – beispielsweise bei schweren körperlichen Montagearbeiten – sicher Hand in Hand zusammenarbeiten.

Autonome, intelligente und lernende Systeme werden so immer häufiger und immer unmittelbarer mit dem Menschen interagieren, und das bei immer komplexeren Aufgabenstellungen. Mehr und mehr entsteht somit eine allgegenwärtige Präsenz des Digitalen (Augmented Intelligence), die assistiert, menschliches Entscheiden in einer Vielzahl von Einsatzbereichen unterstützt – und auch ersetzt. Diese vorhersehbare

Virtuelle Präsenz am Arbeitsplatz

Orts- und zeitunabhängiges Arbeiten bietet große Chancen für die Flexibilisierung der Lebensarbeitszeit, ermöglicht individuelle Zeitsouveränität und verbessert die Vereinbarkeit von Familie und Beruf. Cloud Computing und virtuelle (Arbeitsplatz-)Realitäten werden dies enorm erleichtern. Noch werden erste Anwendungen für ihren professionellen Einsatz erprobt. Aber in den kommenden Jahren sind Sprünge in der Auflösung, der Tiefenschärfe, dem Sichtfeld, der Grafik und dem maschinellen Sehen zu erwarten, die die Durchdringung von Arbeitsplatz-Telepräsenz und das Eintauchen in die virtuelle Umgebung beschleunigen werden. Nicht zu vergessen ist dabei auch, dass eine virtuelle Präsenz negative Effekte des mobilen Arbeitens, wie etwa ein fehlender persönlicher Austausch oder das Gefühl der Desintegration, deutlich abmildern könnte. Virtuelles Arbeiten erfordert allerdings ein hohes Maß digitaler Souveränität, insbesondere ausgeprägte digitale Kompetenz und Akzeptanz digitaler Lösungen.

Textbox 2.1.2: Virtuelle Präsenz am Arbeitsplatz

Entwicklung weckt selbstverständlich auch Ängste. Denn da, wo Kollege Computer in den 1980er Jahren Arbeitsplätze umkrempelte, wird dies künftig der Kollege Roboter tun – oder genauer: der neue künstlich-intelligente Kollege (vgl. IBM 2017). Kaum ein deutsches Unternehmen wird sich der Digitalisierung, ihren Entwicklungen und Auswirkungen entziehen können oder auf ihre Potenziale verzichten wollen. Somit ist die Digitalisierung ein zentrales Innovationsfenster mit Blick auf die Zukunft der deutschen Volkswirtschaft.

Digitale Souveränität: Ableitung eines mehrdimensionalen Handlungskonzepts

Wenn das Innovationspotenzial der Digitalisierung voll ausgenutzt werden soll, müssen alle Beteiligten lernen, souverän mit neuen technologischen ebenso wie strukturellen Anforderungen umzugehen. Dementsprechend hat der Begriff der Digitalen Souveränität Konjunktur. Im Mittelpunkt der Diskussionen in Deutschland stehen Aspekte der IT-Sicherheit und vertrauenswürdige IT-Infrastrukturen.

Bereits in ihrem Koalitionsvertrag von 2013 identifizierte die Bundesregierung einen Handlungsbedarf und hat sich zur Rückgewinnung technologischer Souveränität bekannt sowie Maßnahmen angekündigt – darunter das Fördern vertrauenswürdiger IT- und Netzinfrastrukturen, sicherer Soft- und Hardware sowie sicherer Cloud-Technologien (vgl. BR 2013). Sie zielt vor allem darauf, digitale Autonomie und Souveränität als notwendige Voraussetzung für die Entwicklung eigener IKT-Systeme in Deutschland auszuprägen (vgl. BMWi 2014).

Automatisierte Rechtsberatung

In den USA entstanden innerhalb kurzer Zeit hunderte digitaler Rechtsberatungen (Legal Techs). Der Branchenprimus LegalZoom, der unter anderem in Fragen zu Urheber-, Immobilien- und Gesellschaftsrecht berät, hat bereits über zwei Millionen Kunden. Hierzulande stecken Legal Techs noch in den Kinderschuhen. Allerdings wird die digitale Rechtsberatung in Deutschland – weitgehend ohne öffentliche Wahrnehmung – stark vorangetrieben. Kürzlich schuf der Gesetzgeber das „besondere elektronische Anwaltspostfach" (beA), das Rechtsanwälten die sichere elektronische Kommunikation untereinander, mit Kammern sowie mit Behörden ermöglicht. Sämtliche Bundesgerichte nehmen bereits teil, ab 2020 auch alle Zivil-, Arbeits-, Finanz-, Sozial- und Verwaltungsgerichte.

Das Potenzial ist aus Sicht der Kunden groß, wenn oft teurer juristischer Rat erschwinglich wird, leichter zu bekommen ist sowie die Prüfung und Durchsetzung von Verbraucherrechten leichter erfolgen kann. Datensicherheit ist hier eine Grundvoraussetzung für die Akzeptanz von Legal Techs. Denn: Legal Techs benötigen im besonderen Maße sichere und vertrauenswürdige digitale Infrastrukturen.

Textbox 2.1.3: Automatisierte Rechtsberatung

Trotz aller Diskussionen und Ankündigungen fehlt in Deutschland bislang jedoch eine einheitliche Definition der digitalen Souveränität – gerade auch, um aus ihr ein Handlungskonzept für die Wirtschaft abzuleiten. Der Digitalverband Bitkom, der rund 2.400 Unternehmen der deutschen Digitalwirtschaft vertritt, versteht unter

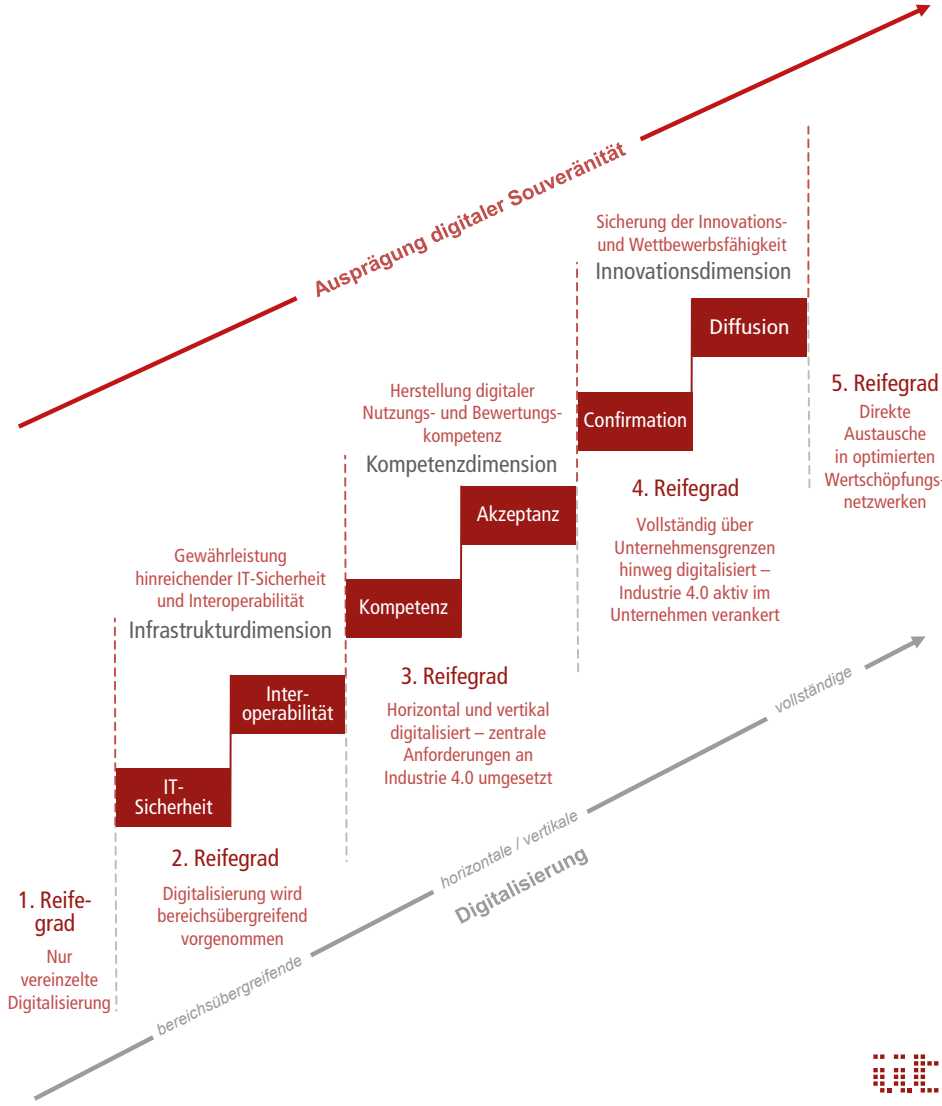

Abbildung 2.1.2: Dimensionen einer digitalen Souveränität als Erfolgsfaktoren im Reifemodell der Digitalisierung. Quelle: in Anlehnung an BMWi 2016 und Nissen et al. 2016; eigene Darstellung

digitaler Souveränität „die Fähigkeit zu Selbstbestimmung im digitalen Raum – im Sinne eigenständiger und unabhängiger Handlungsfähigkeit" von Unternehmen (Bitkom 2015, S. 4). Der Bundesverband der Industrie (BDI) fasst unter dem Begriff vor allem Cybersicherheit, Vorhandensein notwendiger Bewertungskompetenzen und auch eine Wettbewerbschance für deutsche Unternehmen zusammen. Mit Blick auf die skizzierten Heraus- und Anforderungen an eine digitale Souveränität versucht dieser Beitrag eine eigene Definition volkswirtschaftlicher digitaler Souveränität – über drei aufeinander aufbauende Dimensionen entlang eines Reifegradmodells der Digitalisierung in Unternehmen (siehe Abbildung 2.1.2).

Infrastrukturdimension

Ausgangsbedingung digitaler Souveränität ist eine leistungsfähige, sichere und interoperable IT-Infrastruktur, die den Schutz der darin stattfindenden Aktivitäten gewährleistet, sei es Forschung an neuen digitalen Technologien oder die Entwicklung digitaler Dienstleistungen und Produkte.

Die wachsende Ausgestaltung des Internet of Things[2] hin zu einem Internet of Everything, also einem Überall-Internet, stellt höhere Anforderungen an IT-Sicherheit. Damit einhergehend werden sich die Maschine-Maschine-Kommunikation (M2M) und das Cloud Computing weiterentwickeln. Aktuell häufigste Angriffsziele von Schadsoftware sind dementsprechend auch die internen IT-Systeme und Kommunikationsstrukturen der Unternehmen. Die Infrastrukturen müssen künftig nicht nur leistungsfähig sein, sondern auch sicher mit digitalen Plattformen und Netzwerken kommunizieren können. IT- und Datensicherheit ist somit die *conditio sine qua non* der digitalen Souveränität.

Neben der IT-Sicherheit erfordert die wachsende technologische Vernetzung zwischen Unternehmen und diejenige mit ihren Endkunden interoperable und flexibel integrierbare Systeme aus den teils sehr heterogenen digitalen Technologien. Die Komponenten der Infrastruktur sollten deshalb untereinander kompatibel und austauschbar sein, um die Flexibilität und Lebendigkeit des Innovationssystems zu erhalten und fortzuentwickeln. So können auch Netzwerkeffekte über einzelne Industrien hinweg erzeugt werden. Dies ist eine entscheidende Voraussetzung, um Effekte einer zunehmend vertikalen, digitalen Transformation in Richtung kollaborativer Wertschöpfungsnetze zwischen Unternehmen zu nutzen.

[2] *Das Internet of Things (IoT), auch als Internet der Dinge bezeichnet, ist ein Netzwerk physischer Objekte, in das Kommunikationstechnologien direkt eingebunden sind. Diese ermöglichen eine direkte Kommunikation und Interaktion sowohl zwischen den physischen Objekten im Netzwerk als auch mit externen Objekten.*

Kompetenzdimension

Aus all diesen Gründen brauchen Nutzer und Anbieter ausreichende digitale Kompetenzen, um souverän mit Daten umgehen und die Sicherheit und Vertrauenswürdigkeit vorhandener IT-Infrastruktur beurteilen zu können. Digitale Schlüsselkompetenzen sind dafür nicht nur aufzubauen, sondern auch kontinuierlich fortzuentwickeln, damit die Beteiligten die Entstehung neuer Kompetenzanforderungen erkennen und sich diese auch aneignen können (vgl. Krings 2015).

Der digitalen Kompetenz von Anbietern sollte dabei eine hinreichende digitale Kompetenz der Nutzer gegenüberstehen, denn diese bestimmen letztlich über ihre Akzeptanz der Digitalisierung die Nachfrage. So erzeugen digital geprägte Produkte, Dienstleistungen und entsprechende Hybridformen auf der Nachfrageseite nur dann einen Mehrwert, wenn ein hohes Maß an Vertrauen in das Angebot aufgebaut werden kann (vgl. Bitkom 2016). Anbieterkompetenz einerseits und Nutzerkompetenz mit Digitalakzeptanz andererseits bedingen folglich einander.

Zusammengefasst erweist sich digitale Bildung als Grundvoraussetzung für die Ausprägung einer digitalen Souveränität. Eine solche Kompetenz erwerben Menschen durch die Vermittlung relevanten Wissens in der Schule oder anderen Bildungseinrichtungen, oder sie eignen sich diese individuell an – insbesondere, indem sie sich mit den Risiken und Möglichkeiten digitaler Technologien auseinandersetzen.

Abbildung 2.1.3: Bestandteile digitaler Bewertungskompetenz

Der Aufbau von (1) Hardware-Kompetenz ist ein übliches Ergebnis kontinuierlicher digitaler Bildung. Hierbei gilt es, grundsätzliche Kenntnisse über die Funktionsweise von Sensoren, Mikrocontrollern, Speicher- und Kryptochips sowie der Mikro- und Nanoelektronik zu vermitteln. Dies sollte mit der Entwicklung von (2) Software-Kompetenzen einhergehen, um technische Eigenschaften von Plattformen, Schnittstellen und anderen Bereichen zu verstehen. Besteht darüber hinaus (3) IT-Sicherheitskompetenz, ist der Nutzer in der Lage, Qualität, Sicherheit und Verlässlichkeit von digitalen Produkten und Dienstleistungen sachgerecht einzuschätzen sowie die geeigneten Mittel auszuwählen, um sich vor Missbrauch und Angriffen auf technische Einrichtungen zu schützen. Mit der Zunahme des Einsatzes von Big- und Smart-Data-Lösungen, Cloud Computing, Plattformen und Mobile-Business-Systemen steigen auch die Anforderungen an eine (4) Daten-Kompetenz. Sie umfasst nicht nur das Wissen um Auswertungsmöglichkeiten und Leistungsfähigkeit solcher Systeme und die rechtlichen Rahmenbedingungen des Datenschutzes. Vielmehr zählen hierzu auch Kenntnisse über die Möglichkeiten, Datenverluste zu vermeiden – insbesondere auch im mobilen Bereich – und unberechtigte Zugriffe Dritter zu verhindern. In einer entwickelten Plattformökonomie sollten Nutzern nicht zuletzt die Funktionsweisen von Plattformen und die damit verbundenen Gefahren von Marktabschottungen, Ausnutzen von Marktmacht und Datenmissbrauch bekannt sein (vgl. BMWi 2016).

Innovationsdimension

Mit der Ausprägung der Infrastruktur und Kompetenz erlangt ein Unternehmen Daten- und Technologiesouveränität. Die Innovation stellt sich darauf aufbauend über eine souveräne digitale Wertschöpfung (Wertschöpfungssouveränität) und souveräne Freisetzung digitaler Innovationen (Innovationssouveränität) ein. Die Innovationsdimension digitaler Souveränität ist also die abhängige Variable zur Infrastruktur- und Kompetenzdimension digitaler Souveränität, da sie der Ausprägung der Infrastruktur- und Kompetenzdimension bedürftig ist.

Digitale Wertschöpfungssouveränität erreicht ein Unternehmen, wenn es die Produktivität von Investitionen in digitale Technologien sichert. Unter der Voraussetzung, dass der Grad der Digitalisierung die Grenzproduktivität eines Unternehmens beeinflusst, entspricht dessen erste Ableitung, mathematisch ausgedrückt, dem Grad der digitalen Souveränität. Somit entscheidet digitale Souveränität letztendlich über den Ertrag aus den Investitionen in digitale Technologien. Investiert ein Unternehmen in digitale Technologien, nicht aber in Maßnahmen digitaler Souveränität, wird sich folglich relativ schnell eine abnehmende Grenzproduktivität der Digitalisierung einstellen. Der Grund hierfür ist einerseits, dass etwa aufgrund fehlender IT-Sicherheit Schadkosten oder aufgrund fehlender Interoperabilität hohe Wechsel- sowie Risikokosten einer technologischen Pfadabhängigkeit entstehen können. Derartiges beein-

trächtigt die Erträge aus der Digitalisierung erheblich. Andererseits wird die Grenzproduktivität der Digitalisierung abnehmen, wenn eine fehlende oder eine nur unzureichende Nutzungskompetenz die Investitionseffizienz digitaler Technologien sinken lässt, weil Mitarbeitende von ihnen nicht, nicht hinreichend oder falsch Gebrauch machen können. In diesem Fall bleibt der digitale Return on Investment aus oder zumindest hinter den Erwartungen zurück.

Wenn digitale Innovationen aus Kundensicht einen erkennbaren Mehrwert erzeugen, leicht zu übernehmen und beherrschbar sind, also eine nicht zu hohe Komplexität aufweisen, dann muss das anbietende Unternehmen Innovationssouveränität erlangen, die eng an einen Beitrag zur Konsumentensouveränität geknüpft ist. Über die Adaptions- und Diffusionsrate auch digitaler Innovationen entscheidet dann vor allem die Fähigkeit der Unternehmen, wie sie den Grad ihrer digitalen Souveränität als Mehrwertversprechen gegenüber potenziellen Kunden verdeutlichen können.

Dies gelingt nicht immer. So revidieren Konsumenten häufig ihre Entscheidungen für oder gegen innovative Produkte und Dienstleistungen, schlicht weil Informationen

Signalisierung digitaler Souveränität

Mag hohe Datensicherheit bei Musikempfehlungen für Streaming-Dienste noch keine große Rolle spielen, da viele Kunden sich nicht daran stören, wenn internationale Server Informationen über ihre Vorlieben speichern und verarbeiten, sieht das bei wissensintensiven Dienstleistungen anders aus.

Bei Legal Techs etwa müssen Dienstleister (=Anwaltskanzlei) und Kunden (=Mandanten) einander sehr viel mehr vertrauen können. Auch in der Telemedizin existiert eine mindestens ebenso sensible Beziehung: das Arzt-Patient-Verhältnis. In beiden Fällen – Legal Tech oder auch Telemedizin – muss die Technologie ein enorm hohes Sicherheitsversprechen einlösen und die extrem sensible, vertrauensbasierte Beziehung zwischen Erbringer und Empfänger einer wissensintensiven Dienstleistung unterstützen oder gar teilweise selbstständig erbringen.

Aus diesem Zusammenhang entstehen zugleich gänzlich neue Betreibermodelle – und zwar nicht trotz, sondern wegen der hohen Datenschutzanforderungen in Deutschland. So wird Microsoft die Server für seine Cloud-Computing-Systeme künftig in München ansiedeln. Damit verbunden ist das Mehrwertversprechen, dass die dort gespeicherten Daten gemäß der deutschen Datenschutzgesetzgebung deutlich sicherer vor Zugriffen wären als andernorts.

Auf IT-Sicherheit und Datenschutz „Made in Germany" setzt auch die ebenfalls in München ansässige Myra Security GmbH. Das innovative Technologieunternehmen ist einer der führenden Anbieter für Distributed Denial of Service DDoS-Schutz- und Web-Performance-Lösungen. Das deutsche Unternehmen profitiert ebenfalls von den hohen Datenschutzstandards in Deutschland und Europa. Inzwischen ist Myra auch deshalb ein ernst zu nehmender Konkurrent für einstige US-amerikanische Platzhirsche mit einem stetig wachsenden Marktanteil.

Textbox 2.1.4: Signalisierung digitaler Souveränität

fehlen. Und selbst typische frühe Anwender (Early Adopters) hören bei mangelnder Auskunft auf, Innovationen zu nutzen. Dies wiederum wird von Nachzüglern, den sogenannten „Late Adopters", beobachtet, die in einer solchen Situation ihre Konsumentscheidung möglicherweise weiter hinauszögern oder direkt negativ treffen. Unternehmen sind also gehalten, frühe Kundenakzeptanz aufzubauen, auch um eine späte und nachhaltige Kundenakzeptanz zu sichern.

Im digitalen Zeitalter gewinnt daher das Signalisieren digitaler Souveränität (Signalling) durch die Unternehmen erheblich an Bedeutung. Dieses signalling knüpft sich an die Vertrauenswürdigkeit des Produkts und an die digitale Souveränität des Anbieters. Statt den Konsumenten also mit seinen aktuellen Sorgen, Befürchtungen und auch Ängsten allein zu lassen, die er möglicherweise durch neues Wissen im Laufe der Zeit abbaut, können Unternehmen frühzeitig darstellen, dass ein hinreichendes Maß an digitaler Souveränität dank ausreichender Datensicherheit, flexibler, interoperabler und risikofreier Technologien und entsprechend kompetente Mitarbeitende vorhanden ist. Ist der daraus gewonnene relative Marktvorteil hoch, steht zu erwarten, dass die Diffusionsrate des Angebots sich erhöht. Und umgekehrt: Gelingt es dem Unternehmen nicht, glaubhaft einen Vorteil zu signalisieren, wird die Diffusionsrate durch höhere Abbruchraten beeinträchtigt.

Eine hinreichende IT-Sicherheit und Interoperabilität zu gewährleisten in Verbindung mit der Herstellung digitaler Nutzungs- und Bewertungskompetenz kann somit als notwendige Bedingung einer erfolgreichen Digitalisierung gelten. Gleichzeitig ist die digitale Souveränität Treiber von Wettbewerbsfähigkeit und Innovation und damit hinreichende Bedingung für eine erfolgreiche Digitalisierung.

Stand der digitalen Souveränität in Deutschland und Handlungserfordernisse

Hinter „Digitaler Souveränität" steckt also ein facettenreiches Konzept, das – von den Unternehmen – hohe Anforderungen an den Erhalt der Wettbewerbs- und Innovationsfähigkeit einer Volkswirtschaft stellt, aber auch Chancen schaffen kann. Doch wie steht es um die digitale Souveränität in der deutschen Volkwirtschaft? Und welche Handlungserfordernisse ergeben sich daraus?

Digitale Souveränität als notwendige Bedingung einer erfolgreichen Digitalisierung verstehen

Die Integration digitaler Technologien in deutsche Unternehmen erfolgt mit zunehmender Dynamik (vgl. BMWi 2014), wenn auch immer noch Nachholbedarf im internationalen Vergleich besteht (vgl. Bitkom 2016). So wuchs der Grad der Digitalisierung in der deutschen Wirtschaft zuletzt beständig: Erreichte er auf dem D21-Digital-

Index im Jahr 2015 noch 49 von 100 Indexpunkten, betrug der Wert 2016 bereits 55 und soll Voraussagen gemäß auf 58 Indexpunkte bis im Jahr 2022 steigen.[3]

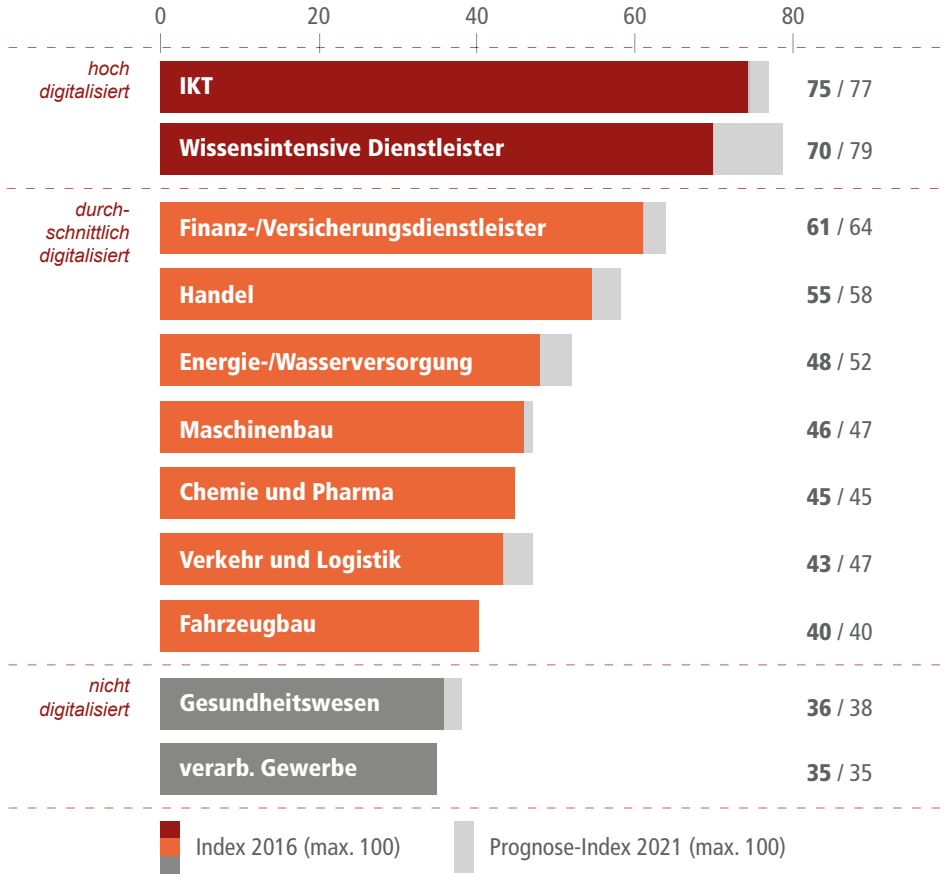

Abbildung 2.1.4: Wirtschaftsindex DIGITAL 2016 und 2021 nach Branchen. Quelle: BMWi 2016, BMWi 2014 und D21 2017; eigene Berechnung[4]

[3] *Der D21-Digital-Index stellt jährlich den Digitalisierungsgrad in Deutschland bevölkerungsrepräsentativ dar, indem er rund 30.000 Personen ab 14 Jahren einbezieht. Der D21-Digital-Index setzt sich zusammen aus den vier unterschiedlich gewichteten Dimensionen Zugang, Nutzung, Kompetenz und Offenheit und wird auf einer Skala von 1 bis bestmöglichen 100 Punkten berechnet. Internetseite: www.initiatived21.de*

[4] *Eigene Berechnung, n=924; Clusterung relativ zur gewerblichen Wirtschaft (Index 2016=55 Punkte): hoch digitalisiert: ≥70 Punkte; durchschnittlich digitalisiert: 40–69 Punkte, niedrig digitalisiert: ≤ 39 Punkte*

Dabei differenziert sich der Digitalisierungsgrad zwischen den Branchen deutlich aus (vgl. BMWi 2014). Und es sind vor allem kleine und mittelständische Unternehmen – also 99 Prozent aller deutschen Unternehmen –, bei denen großer Nachholbedarf besteht. Gleichwohl hat die Digitalisierung für die überwiegende Mehrheit (85 Prozent) eine hohe Bedeutung, zumal mittlerweile 43 Prozent der Unternehmen Umsätze überwiegend digital generieren (vgl. BMWi 2014).

Im internationalen Vergleich der digitalen Leistungsfähigkeit belegt Deutschland mit 53 von 100 Punkten im Digital-Index Platz sechs (vgl. BMWi 2014). Diese Platzierung resultiert aus einer vergleichsweise schwachen globalen Marktstärke (Angebot und Nachfrage, Umsätze und Exporte) der digitalen Wirtschaft, daneben werden aber auch Schwächen in der Infrastruktur (technische Infrastrukturen und wirtschaftspolitische Rahmenbedingungen) und Nutzungsintensität digitaler Technologien, Produkte und Services (Nutzung sowie Offenheit gegenüber technologischen Neuerungen) genannt.

Mit dieser Entwicklung und den Herausforderungen im internationalen Wettbewerb wird auch der Grad der digitalen Souveränität wachsen (vgl. BDI 2016). Allerdings müssen sich hierfür nicht nur Regularien und Rahmenbedingungen sowie die Unterstützung von Investitionen in Maßnahmen zur Steigerung digitaler Souveränität verbessern, sondern auch die Bemühungen um Standardisierung.

Investitionen in IT-Sicherheit stärken, um Staus bei Investitionen in digitale Technologien zu vermeiden

Bereits jedes zweite deutsche Unternehmen ist schon einmal Opfer eines IT-Angriffs (Spionage, Sabotage und Datendiebstahl) gewesen. Der damit verbundene volkswirtschaftliche Schaden beläuft sich auf rund 51 Milliarden Euro beziehungsweise auf 1,6 Prozent des Bruttoinlandsprodukts (2015) (vgl. bitkom reserach 2015). Die Mehrheit (65 Prozent) der deutschen Unternehmen ist sich darüber im Klaren und schätzt das Risiko von IT-Angriffen entsprechend hoch ein. Für drei von vier deutschen Firmen ist IT-Sicherheit deshalb nicht nur eine sehr wichtige, nicht zu vernachlässigende Aufgabe, sondern auch eine Grundvoraussetzung für die Digitalisierung. Technologisch sieht sich allerdings nur jedes zweite Unternehmen gut aufgestellt.

Es stellt sich in den Unternehmen weniger die Frage, ob es zu einem Cyber-Angriff kommt, sondern lediglich, wann dieser erfolgen wird. Herausfordernd für die digitale Souveränität ist, dass Sicherheitsbedenken im IT-Bereich das digitale Engagement in den Unternehmen und damit notwendige Investitionen bremsen können. Wird wiederum stärker in die Digitalisierung investiert, sind gleichzeitig Investitionen in Sicherheit notwendig. Auch dies kann Digitalisierungsaktivitäten verlangsamen. Wie auch immer diese Entscheidungen ausfallen, in jedem Fall haben sie erhebliche Auswirkungen auf die Unternehmensentwicklung (vgl. Bundesdruckerei 2016).

Standardisierung über offene Standards vorantreiben, um Interoperabilität sicherzustellen

Interoperabilität verhindert Lock-In-Risiken für Unternehmen, also systemische Technologieabhängigkeiten. Die Herstellung von Interoperabilität ist damit neben IT-Sicherheit ein zweiter zentraler Treiber zur Ausprägung der Technologiesouveränität und damit Teil einer notwendigen Bedingung digitaler Souveränität. Besonders für kleine und mittlere Unternehmen ist Interoperabilität ein strategischer Faktor, um Marktzugänge zu sichern oder zu ermöglichen. Dringenden Nachholbedarf sieht hier jede zweite deutsche Firma (vgl. acatech 2016).

Abhilfe schaffen offene und international einheitliche Standards, die mehr Flexibilisierung und Modularität ermöglichen. Zudem würden sie das Investitionsrisiko abbauen und damit auch den im Falle von Interoperabilität häufig auftretenden Pinguin-Effekt[5] minimieren können (vgl. acatech 2016). Hierzu sind die heterogenen Systeme, Architekturen, Datenaustauschformate, Semantiken, Taxonomien, Ontologien und Schnittstellen über interoperable Schnittstellen und offene Standards spezifisch zu standardisieren. Geschieht dies nicht, entstehen unverbundene proprietäre Insellösungen und digitale Ökosysteme werden geschwächt.

Digitale Bildungsangebote und lebenslange Kompetenzvermittlung ausbauen

In vielen deutschen Unternehmen mangelt es den Beschäftigten noch an der Fähigkeit zur Bewertung, was letztlich die digitale Souveränität schwächt und zu relevanten Entwicklungshemmnissen in der Digitalisierung führen kann. Auch diese Herausforderung ist den deutschen Unternehmen bereits bewusst: So ist die Digitalkompetenz der Mitarbeiter aus Sicht von neun von zehn Führungskräften für die weitere Unternehmensentwicklung auschlaggebend, und 70 Prozent der Firmen sehen gerade darin einen starken Nachholbedarf. Mit Blick auf den D21-Digital-Index ist ein leichter Rückgang des Digitalisierungs-Gesamtindex in der Gesamtbevölkerung von 52 auf 51 Punkte festzustellen, bedingt durch Negativtrends in den Teilindizes „Kompetenz" und „Offenheit" (vgl. D21 2017). Dies betrifft sowohl die Beschäftigten als auch die Bevölkerung insgesamt, wenngleich die Kompetenzen zur Bewertung seitens der Anbieter (Beschäftigte in Unternehmen) deutlich besser sind als diejenigen der Anwender (Bevölkerung).

---

[5] *Pinguin-Effekt: Der Pinguin-Effekt beschreibt das Phänomen, dass die Ausbeute einer bestimmten Anwendung umso geringer ist, je kleiner die Anzahl der Nutzer ist. Wie hungrige Pinguine, die aus Angst vor Fressfeinden zunächst abwarten, bis der erste Artgenosse ins Wasser springt, verhalten sich auch häufig investierende KMU. Diese halten ihre Investitionen, trotz hohen Interesses, solange zurück, bis Standards oder Interoperabilität etabliert sind. Andernfalls besteht für sie ein Lock-In-Risiko.*

Ursächlich dafür ist, dass sich drei Viertel der Beschäftigten ihre digitalen Kompetenzen überwiegend im Arbeitsalltag angeeignet haben, wobei der Einsatz niedrigschwelliger digitaler Arbeitsmittel (Textverarbeitungsprogramme, Kommunikationstools) überwiegt. Zugleich besteht ein ausgeprägter Informationsbedarf über die Möglichkeiten digitaler Technologien in Firmen. Immerhin erwarten acht von zehn Beschäftigten in großen Unternehmen, dass sie dank digitaler Lösungen effizienter arbeiten könnten. Andererseits beeinträchtigt neben fehlendem Wissen um die Nutzungsmöglichkeiten auch eine gewisse Verschlossenheit, wenn nicht gar Ablehnung, der Mitarbeiter gegenüber digitalen Lösungen die Effizienz der betrieblichen Investitionen in digitale Technologien. So befürchtet jeder fünfte Beschäftigte, mit der Einführung digitaler Technologien schnell überfordert zu sein (vgl. Sopra Steria 2016). Zugleich sind die Bürger in Deutschland noch weniger in der Lage, die Digitalisierung zu bewerten. Ursächlich sind im Kern die gleichen Defizite: mangelnde schulische Vermittlung, Fehlen geeigneter Weiterbildungen, emotionale Ablehnung digitaler Technologien und Misstrauen sowie Überforderungsängste gegenüber der sehr dynamischen Entwicklung (vgl. D21 2017).

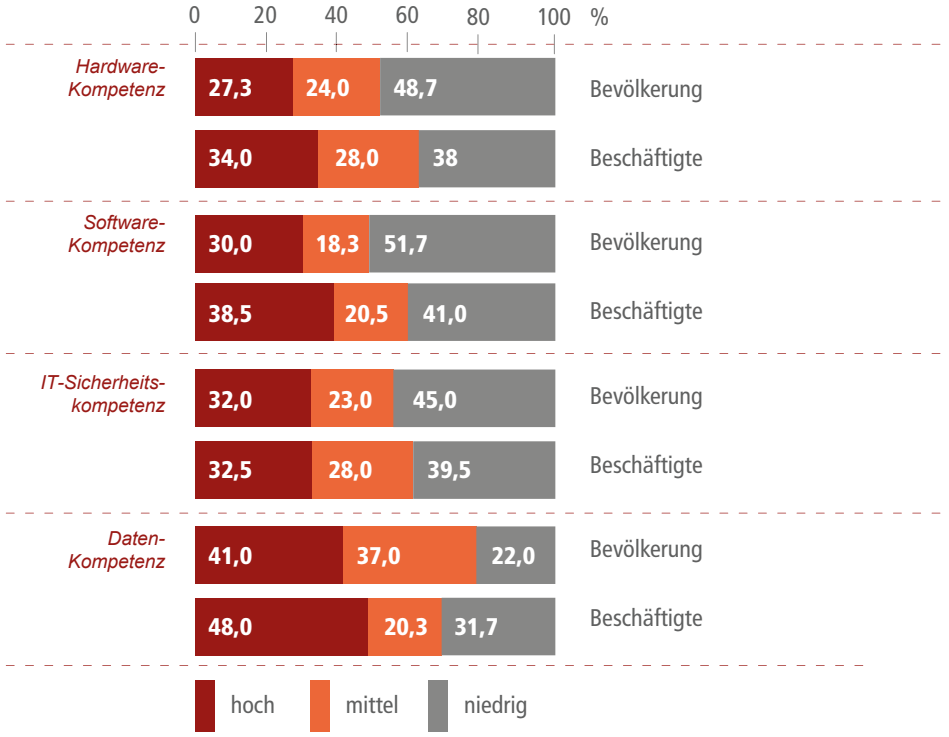

Abbildung 2.1.5: Ausprägung der Bestandteile einer Bewertungskompetenz Anbieter und Anwender. Quelle: D21 2017; eigene Berechnungen

Auf die digitale Souveränität wirkt sich diese Situation ungünstig aus. So kann der Mangel an digitaler Bewertungskompetenz dazu führen, dass Sicherheitsrisiken nicht richtig eingeschätzt werden, wodurch die Gefahr von erfolgreichen IT-Angriffen wächst. Diese Schwäche kann zudem die Einführung digitaler Technologien behindern, da Beschäftigte diese nicht oder nicht im effizienten Maße nutzen können. In der Folge beeinträchtigt sie auch die digitale Souveränität der Konsumenten. Insofern gilt es, digitale Bildungsinhalte frühzeitig in schulische Aus- und lebenslange Weiterbildungskonzepte umfangreich zu integrieren. Darüber hinaus ist feststellbar, dass der Technologieeinsatz zumeist der Kompetenz der Mitarbeiter folgt und nicht umgekehrt. Das heißt, dass diese Gradmesser der Entscheidung für oder gegen die Implementierung digitaler Technologien in Unternehmen sind. Insofern besteht in deutschen Unternehmen noch erheblicher Nachholbedarf, das Personal altersunabhängig digital zu befähigen, vorhandene Ängste abzubauen und die Akzeptanz von digitalen Technologien zu steigern.

Digitale Souveränität als komparativen Vorteil nutzen

Die „Digitale Agenda der Bundesregierung 2014 – 2017" zielt im Kern darauf ab, die Sicherheit und den Schutz der IT-Systeme und Dienste zu verbessern sowie die technologische Kompetenz der Bürger für vertrauenswürdige IT und somit letztlich die digitale Souveränität zu stärken und dauerhaft zu sichern (vgl. BR 2014). Sie reagiert damit auf die Bedarfslage in der deutschen Wirtschaft. So sehen acht von zehn Unternehmen IT-Sicherheit als die zentrale Herausforderung in der Digitalisierung (vgl. EY 2016). Ursächlich für diese Einschätzung sind aktuell das Internet der Dinge (51 Prozent aller Unternehmen) und kritische Infrastrukturen (45 Prozent). Im vergangenen Jahr löste vor allem die wachsende Ausprägung von Cloud Computing Investitionen in IT-Sicherheit aus. Letzteres bleibt aber ein sehr relevantes Sicherheitsthema. Daher werden Investitionen dieser Art weiter wachsen (vgl. eco 2017). Auf die Nachfrage kann die deutsche IT-Sicherheitsindustrie umfassend reagieren, wenngleich die auf dem deutschen Markt führenden Anbieter meist aus anderen Ländern stammen. Die Stärken der deutschen IT-Sicherheitswirtschaft liegen im Bereich der Dienstleistungen und der Hochsicherheit. Durch diese Entwicklung hat sich in den vergangenen Jahren ein Zukunftsmarkt für Security Services herausgebildet – getragen durch eine hohe Innovationskraft, die die Unternehmen nicht trotz, sondern gerade wegen der hohen Standards des deutschen Datenschutzes generieren.

Ausblick

Die aufkeimende Stärke der Anbieter in der digitalen Souveränität der deutschen Volkswirtschaft zeigt sich als komparativer Vorteil, besonders gegenüber Ostasien und den USA. Diesen Vorzug gilt es zu festigen, indem man einerseits Forschung im Bereich digitaler Souveränität fördert und anderseits die Herausbildung der Wirt-

schaftsstruktur vorantreibt. So kann Deutschland letztlich Standortvorteile gewinnen.

Dabei gilt grundsätzlich, digitale Souveränität auch in der Wirtschaft als ein holistisches, mehrdimensionales Konzept zu verstehen. Es genügt nicht, nur an einzelnen Stellen zu optimieren. So ist für eine hohe digitale Souveränität, wie oben beschrieben, Datensicherheit und Interoperabilität wichtig – aber nicht ausreichend. Erst wenn es gelingt, in einem branchenübergreifenden Netzwerk Kompetenzen zu bündeln, weiterzuentwickeln und damit Produkte und Dienstleistungen zu generieren, die auf eine hohe Digitalakzeptanz stoßen können, ist ein wichtiger, nächster Schritt vollzogen. Sinnvoll erscheint es hier, anstatt das Silicon Valley imitieren zu wollen, auf klassische Stärken der deutschen Volkswirtschaft zu setzen: verlässliche, ausgereifte Produkte mit einem hohen Maß an Funktionalität und digitaler Souveränität. Je allgegenwärtiger Digitalisierung wird, desto entscheidender könnten diese Vorteile genutzt werden, um die Annahme und Diffusion von digitalen Innovationen zu beschleunigen.

Literatur

acatech (2016). Industrie 4.0 im globalen Kontext. Strategien der Zusammenarbeit mit internationalen Partnern. Verfügbar unter: www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/Projektberichte/acatech_de_STUDIE_Industrie40_global_Web.pdf, zuletzt zugegriffen am 21.07.2017.

Bauer, W.; Schlund, S.; Marrenbach, D.; Ganschar, O. (2014). Industrie 4.0 – Volkswirtschaftliches Potenzial für Deutschland. Bitkom; Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO (Hrsg.). Verfügbar unter: www.produktionsarbeit.de/content/dam/produktionsarbeit/de/documents/Studie-Industrie-4-0-Volkswirtschaftliches-Potential-fuer-Deutschland.pdf, zuletzt zugegriffen am 21.07.2017.

Bitkom (Hrsg.) (2015). Digitale Souveränität. Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa. Verfügbar unter: www.bitkom.org/noindex/Publikationen/2015/Positionspapiere/Digitale-Souveraenitaet/BITKOM-Position-Digitale-Souveraenitaet.pdf, zuletzt zugegriffen am 21.07.2017.

Bitkom (Hrsg.) (2016). Industrie 4.0 – Die neue Rolle der IT. Leitfaden. Verfügbar unter: www.bitkom.org/noindex/Publikationen/2016/Leitfaden/Industrie-40-Die-neue-Rolle-der-IT/160421-LF-Industrie-40-Die-neue-Rolle-der-IT.pdf, zuletzt zugegriffen am 21.07.2017.

bitkom reserach (2015). Digitale Wirtschaftsspionage, Sabotage und Datendiebstahl. Vortrag Prof. Dieter Kempf am 16.04.2015. Verfügbar unter: www.bitkom.org/Presse/Anhaenge-an-PIs/2015/04-April/Digitale-Angriffe-auf-jedes-zweite-Unternehmen/BITKOM-Charts-PK-Digitaler-Wirtschaftsschutz-16-04-2015-final.pdf, zuletzt zugegriffen am 21.07.2017.

Bundesdruckerei (2016). IT-Sicherheit im Rahmen der Digitalisierung. Eine empirische Untersuchung in deutschen Unternehmen – Erstellt von der Bundesdruckerei GmbH in

Zusammenarbeit mit bitkom research 2016. Verfügbar unter: www.bundesdruckerei.de/en/system/files/whitepaper/whitepaper-studie-it-sicherheit.pdf.pdf, zuletzt zugegriffen am 21.07.2017.

Bundesministerium für Wirtschaft und Energie (BMWi) (2014). Monitoring-Report Digitale Wirtschaft 2014. Innovationstreiber IKT. Langfassung. Verfügbar unter: http://ftp.zew.de/pub/zew-docs/gutachten/Monitoring_Report_2014_Langfassung.pdf, zuletzt zugegriffen am 21.07.2017.

Bundesministerium für Wirtschaft und Energie (BMWi) (2016). Leitplanken Digitaler Souveränität. Verfügbar unter: www.de.digital/DIGITAL/Redaktion/DE/Downloads/it-gipfel-2015-leitplanken-digitaler-souveraenitaet.pdf?__blob=publicationFile&v=1, zuletzt zugegriffen am 21.07.2017.

Bundesregierung (BR) (2013). Koalitionsvertrag. zwischen CDU, CSU und SPD. 18. Legislaturperiode. Verfügbar unter: www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf, zuletzt zugegriffen am 21.07.2017.

Bundesregierung (BR) (2014). Digitale Agenda 2014 - 2017. Verfügbar unter: www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda.pdf?__blob=publicationFile&v=6, zuletzt zugegriffen am 21.07.2017.

Bundesverband der Deutschen Industrie e. V. (BDI) (2016). Grundsatzpapier Cybersicherheit. Voraussetzungen für die digitale Souveränität in Deutschland und Europa. Verfügbar unter: https://bdi.eu/media/themenfelder/digitalisierung/publikationen/Broschuere_Grundsatzpapier_Cybersicherheit_fin.pdf, zuletzt zugegriffen am 21.07.2017.

eco (2017). eco Umfrage IT-Sicherheit 2016. Ein report der eco Kompetenzgruppe Sicherheit. Verfügbar unter: www.eco.de/wp-content/blogs.dir/eco-report-it-sicherheit-2016.pdf, zuletzt zugegriffen am 21.07.2017.

Ernst & Young (EY) (2016). Industrie 4.0 – das unbekannte Wesen?. Verfügbar unter: www.ey.com/Publication/vwLUAssets/EY-industrie-4-0-das-unbekannte-wesen/$FILE/EY-industrie-4-0-das-unbekannte-wesen.pdf, zuletzt zugegriffen am 21.07.2017.

IBM (2017). IBM: AI Should Stand For 'Augmented Intelligence' – InformationWeek. Verfügbar unter: www.informationweek.com/government/leadership/ibm-ai-should-stand-for-augmented-intelligence/d/d-id/1326496?, zuletzt zugegriffen am 21.07.2017.

Initiative D21 e.V. (D21) (2017). D21-Digital-Index 2016. Jährliches Lagebild zur digitalen Gesellschaft. Verfügbar unter: http://initiatived21.de/app/uploads/2017/01/studie-d21-digital-index-2016.pdf, zuletzt zugegriffen am 21.07.2017.

Krings, G. (2015). Digitale Souveränität. In: Bitkom (Hrsg.). Digitale Souveränität. Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa. Berlin, S. 351–356. Verfügbar unter: www.bitkom.org/noindex/Publikationen/2015/Positionspapiere/Digitale-Souveraenitaet/BITKOM-Position-Digitale-Souveraenitaet.pdf, zuletzt zugegriffen am 21.07.2017.

Nissen, V.; Stelzer, D.; Straßburger, S.; Fischer, D. (Hrsg.) (2016). SIMMI 4.0 – Vorschlag eines Reifegradmodells zur Klassifikation der unternehmensweiten Anwendungssystemland-

schaft mit Fokus Industrie 4.0, Multikonferenz Wirtschaftsinformatik (MKWI) 2016: Technische Universität Ilmenau, 9.–11. März 2016; Band II.

Rogers, E. (1995). The Diffusion of Innovations. New York: Free Press.

Sopra Steria (2016). Digitale Überforderung im Arbeitsalltag 2016. Verfügbar unter: www.digitaleschweiz.ch/wp-content/uploads/2017/02/digitale-ueberforderung-im-arbeitsalltag.pdf, zuletzt zugegriffen am 21.07.2017.

Verband der Elektrotechnik Elektronik Informationstechnik e.V. (VDE) (2016). VDE Trendreport 2016. Frankfurt am Main.

2.2 Privatheit und digitale Souveränität in der Arbeitswelt 4.0

Wenke Apt, Julia Seebode, Stefan G. Weber

Der Einsatz digitaler Assistenzsysteme und cyberphysikalischer Technologien lässt neue Formen der Arbeitsorganisation und der Arbeitsteilung entstehen. Routinetätigkeiten können in vielen Bereichen automatisiert und die Prozessqualität verbessert werden. Durch den stetig wachsenden Einfluss von Daten und digitalen Assistenzsystemen im Arbeitsalltag ergeben sich aber auch neue Risiken für die Sicherung von Privatheit, Persönlichkeitsrechten und digitaler Souveränität. Hier kommt es darauf an, zu einem fairen Ausgleich der Interessen zu kommen.

Unternehmen und Organisationen erheben und verarbeiten auf unterschiedlichsten Wegen eine Vielzahl personenbezogener Daten. Zu den klassischen Beispielen zählen Systeme zur Arbeitszeiterfassung, Überwachungskameras zur Absicherung des Betriebsgeländes oder auch die Kommunikation über E-Mails. Bereits aufgrund der Daten digitaler Workflow- und Projektmanagementsysteme können weitreichende und detaillierte Dokumentationen über die Beschäftigten und ihre tagtäglichen Verrichtungen entstehen. Ursprüngliches Ziel der Datenerfassung und -auswertung war, Betriebskennzahlen wie Kosten, Produktivität oder Lieferzeit zu optimieren. Die Erfassung von Beschäftigtendaten war dabei eher eine Begleiterscheinung der Optimierung von betrieblichen Prozessen. Zwar wurden die technischen Arbeitsmittel seit jeher „auch zur Überwachung der Beschäftigten verwendet, um das Transforma-

Digitale Assistenzsysteme

Zentrale Fähigkeiten gegenwärtiger digitaler Assistenzsysteme sind die Wahrnehmung der Umgebung, reaktives Verhalten, die Steuerung der Aufmerksamkeit und Einschätzung der Situation. Art und Umfang der adaptiven und individualisierten Unterstützung werden durch die sensorische Erfassung des Kontextes und des Verhaltens einzelner Mitarbeiter bestimmt. Ziel ist eine personalisierte Arbeitsunterstützung, zum Teil auch mit tutorieller Assistenz durch die Systeme. Dies reicht von der einfachen Anzeige von Arbeitsanweisungen (Montage- oder Wartungsanleitungen, Qualitäts- oder Sicherheitshinweise) über die Bereitstellung von Wissen am Arbeitsplatz (Prozesswissen, Qualifikationsmanagement), die individuelle Anpassung an ein Arbeitsumfeld (kontextsensitive Informationsbereitstellung, Arbeitsplatzanpassung hinsichtlich Tischhöhe, Sprache, Bedienoberfläche) bis hin zu komplexen Mensch-Maschine-Kollaborationen oder auch elektronisch gestütztem Lernen am Arbeitsplatz (BMWi 2015).

Textbox 2.2.1: Digitale Assistenzsysteme

Cyberphysikalische Systeme

Cyberphysikalische Systeme stehen für die Verbindung von physikalischer und informationstechnischer Welt (Geisberger und Broy 2012). Sie entstehen durch die komplexe Verbindung mechanischer oder elektronischer Teile mit einem Netzwerk (z. B. Internet) und ermöglichen eine ortsunabhängige Kontrolle und Steuerung in Echtzeit. Sensoren registrieren und verarbeiten eine Vielzahl von Daten aus der physischen Welt, ziehen Schlussfolgerungen und lösen Handlungen aus (Arntz et al. 2016). Ziel ist, dass die in den Maschinen und Werkstücken eingebetteten Systeme durch einen automatisierten Datenaustausch große Teile der Wertschöpfungskette selbsttätig steuern, um die Flexibilität und Effizienz zu erhöhen (Krause 2017).

Textbox 2.2.2: Cyberphysikalische Systeme

tionsproblem der Umwandlung menschlicher Arbeitskapazität in ökonomisch verwertbare Arbeitsresultate zu bewältigen" (Krause 2017, S. 7).

Mit der Einführung weiterer technischer Systeme im Rahmen der sich rasch vollziehenden Digitalisierung der Arbeitswelt wachsen die Möglichkeiten der Erfassung und Auswertung personenbezogener Daten mithilfe komplexer Analysemethoden jedoch rasant an. Diese werden häufig unter den Schlagworten Big Data, Smart Data oder Data Mining zusammengefasst. Häufig sind solche Analysetools Bestandteil einer Steuerungssoftware oder eines intelligenten Unterstützungssystems – und zunächst intransparent und oft wenig fassbar im Hintergrund aktiv. Für den Einzelnen wird es somit zunehmend schwieriger zu durchschauen, wem welche Informationen zur eigenen Person bekannt sind und wie diese tatsächlich verwendet werden. Da die Beschäftigten in einem Abhängigkeitsverhältnis zu ihren Arbeitgebern stehen, fällt es ihnen wegen der bestehenden Machtasymmetrie individuell schwer, ihre Grundrechte auf informationelle Selbstbestimmung durchzusetzen. Folglich wird mit der Datenerfassung häufig die Bedrohung assoziiert, als „gläserner Mitarbeiter" Ziel von betrieblichen Rationalisierungsmaßnahmen, nachteiligen Personalentscheidungen oder Diskriminierung zu werden. Die Gewährleistung von Privatheit als Grundlage für die digitale Souveränität erweist sich somit als ein zentraler Akzeptanzfaktor für die Arbeitswelt 4.0 und deren erfolgreicher Ausgestaltung.

Wissen ist Macht: Intelligente Assistenzsysteme

Intelligente Unterstützungssysteme können den Beschäftigten auf vielfältige Art und Weise die Arbeit erleichtern. Voraussetzung sind jedoch individualisierte Nutzerkonten, bei denen personenspezifische Informationen hinsichtlich Arbeitsverhalten und -leistungen zusammengeführt und ausgewertet werden (Krause 2017). Intelligente Assistenzsysteme sind bereits heute in der Lage, Fähigkeitsprofile der Nutzer zu erstellen und sich in ihrer Unterstützungsleistung an deren Bedürfnisse und konkrete Wünsche anzupassen. Dabei kommen unterschiedliche Technologien zum Einsatz,

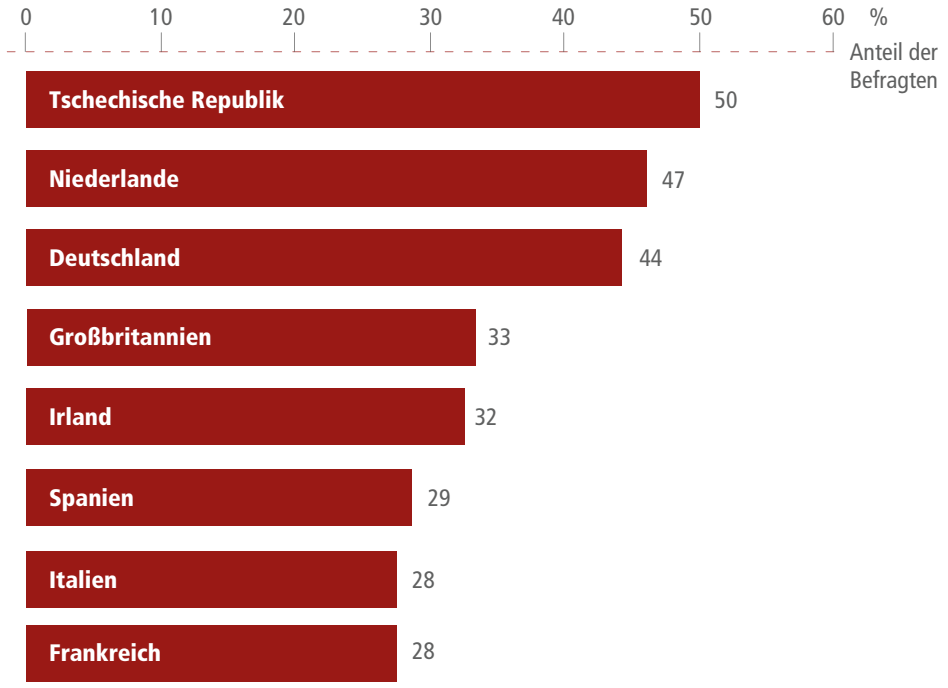

Abbildung 2.2.1: Umfrage zum Vertrauen in Arbeitgeber bei der Nutzung privater Daten in Europa 2015. Quelle: Statista 2016

vor allem um Informationen (z. B. Arbeitsschritte, Bauteile und Anweisungen) mittels mobiler Endgeräte, interaktiver Visualisierungssysteme und anderer Hilfsmittel zu liefern, aber auch um den Arbeitenden physisch zu entlasten. Die Kontexterfassung erfolgt beispielsweise über Bilder, Ortung oder die Aufzeichnung von Arbeitsverhalten, Bewegungen, Emotionen und Vitalparametern.

Die Prozessqualität und Fehlerreduktion, die sich mit intelligenter Unterstützung erreichen lassen, sind besonders relevant für komplexe Arbeitsprozesse oder sicherheitskritische Tätigkeiten, bei denen menschliches Versagen weitreichende Konsequenzen haben kann. So stehen denn auch Assistenzsysteme für bestimmte, die Sicherheit gefährdende Beschäftigungsfelder im Fokus aktueller Forschungsarbeiten. Eine relevante Personengruppe sind zum Beispiel die Teams in einem Operationssaal, deren Fehler direkt Leben bedrohen können.

Um hier Verbesserungen zu erreichen, wird angestrebt, die Operationsdauer möglichst kurz zu halten und Arbeitsabläufe sowie die Arbeitsumgebung im Operationssaal so auszulegen, dass Komplikationen für Patienten vermieden werden. Aus diesem Grund entwickeln Forscher aktuell technische Assistenzsysteme für einen „auf-

merksamen Operationssaal", die abhängig vom Arbeitsablauf, dem Arbeitskontext und der Kompetenz der Mitglieder des Operationsteams kontextsensitive Handlungsempfehlungen ableiten.[6] Und auch bei der Ausbildung von Chirurgen sollen technische Systeme helfen, die das Training von Operationen überwachen und so den angehenden Chirurgen wertvolle Hinweise zur Weiterqualifizierung liefern können.[7]

Weitere Beispiele für Teams, die in sicherheitskritischen Umgebungen arbeiten, sind Fluglotsen oder Mitarbeiter in Kraftwerksleitständen und Stellwerken der Eisenbahn. Auch für diese Arbeitsfelder forschen Wissenschaftler an Assistenzsystemen, die das Kooperationsverhalten in einem Team inklusive der zugrundeliegenden Emotionen der einzelnen Beteiligten erkennen und daraufhin angepasste Handlungsempfehlungen geben können.[8] Eine steigende Anzahl von Anwendungen kann also die emotionale Verfassung und sogenannte weiche Arbeitsfaktoren wie das Kommunikationsverhalten erfassen.

Die erweiterten Möglichkeiten einer digitalen, datenbasierten Entscheidungsunterstützung schaffen allerdings auch den Raum für ein – zunächst implizites – Risiko: Die systematische Verknüpfung und automatisierte Auswertung der im großen Umfang vorliegenden Daten ermöglicht es, die Belegschaft ohne Anlass und flächendeckend zu überwachen sowie Fehler- und Leistungskontrollen erheblich zu verschärfen. Das Zusammenführen von Datenbeständen aus unterschiedlichen Quellen vereinfacht zudem wesentlich die Personalisierung vorliegender Daten. So lassen sich auch aus anonymen Daten sensible Informationen, beispielsweise zu persönlichen Gewohnheiten oder zum Gesundheitszustand, ableiten. Unabhängig von Anlass und Zweck der Datenerfassung können immer leistungsfähigere Algorithmen und eine immer umfassendere Datenverarbeitung „Antworten auf Fragen liefern, die keiner gestellt

---

[6] *Siehe hierzu: Projekt „KonsensOP – Unterstützung von Arbeitsabläufen und Kommunikation im Operationssaal durch eine technische Assistenz." BMBF-Bekanntmachung „Sozial- und emotionssensitive Systeme für eine optimierte Mensch-Technik-Interaktion" (Verfügbar unter: www.technik-zum-menschen-bringen.de/projekte/konsensop, zuletzt zugegriffen am 28.07.2017).*

[7] *Siehe hierzu: Projekt „SurMe – Chirurgische Simulationen unterschiedlicher Schwierigkeitsstufen – The Surgical Mentor System." BMBF-Bekanntmachung „Erfahrbares Lernen" (Verfügbar unter: www.technik-zum-menschen-bringen.de/projekte/surme, zuletzt zugegriffen am 28.07.2017).*

[8] *Siehe hierzu: Projekt „MACeLot – Assistenzsystem für die Teamarbeit an technischen Systemen." BMBF-Bekanntmachung „Sozial- und emotionssensitive Systeme für eine optimierte Mensch-Technik-Interaktion" (Verfügbar unter: www.technik-zum-menschen-bringen.de/projekte/macelot, zuletzt zugegriffen am 28.07.2017).*

hat". Diese Entwicklungen haben schwer absehbare Auswirkungen auf das Grundrecht auf informationelle Selbstbestimmung, das jedem Einzelnen das Recht einräumt, seine personenbezogenen Daten nur für fest definierte Zwecke nutzen zu lassen (Jerchel 2015).

Amazon nutzt in seinen Logistikzentren bereits Handscanner, die lückenlose Bewegungsprofile der Beschäftigten liefern, die in den Lagerhallen einfache Arbeit ausführen und beispielsweise zu Fuß die bestellten Produkte einsammeln und zu den Packstationen bringen. Jeder Arbeitsschritt und jede außerplanmäßige Pause wird damit

Abbildung 2.2.2: Treiber und Hebel des Beschäftigtendatenschutzes in der digitalen Arbeitswelt. Quelle: in Anlehnung am BMAS 2016, S. 13; eigene Darstellung

nachvollziehbar. Die detaillierten Aufzeichnungen ermöglichen dem Management die Erstellung individualisierter Leistungsprofile und einen systematischen Vergleich des Arbeitsverhaltens der Beschäftigten, auch wenn das Unternehmen angibt, in Übereinstimmung mit den deutschen Datenschutzregeln keine personenbezogene Auswertung der Bewegungsdaten vorzunehmen. Aber nicht nur in Logistik- oder Produktionshallen halten Systeme Einzug, die mittels Big Data und kontrollrelevanter Softwareanwendungen „individualisierte Evaluationssysteme neuer Qualität" schaffen (Staab und Nachtwey 2016, S. 28). Bereits heute findet man sie auch in den Büros, wo das Nutzerverhalten an stationären und mobilen Endgeräten umfassend dokumentiert und ausgewertet werden kann. Beispielsweise ist Monitoring-Software wie mSpy oder Orvell Monitoring in der Lage, sämtliche Aktivitäten an Desktops und Smartphones aufzuzeichnen. Am unternehmensinternen Arbeitsplatz zählen dazu Screenshots, Tastatureingaben, Dauer von Aktivitäten bzw. Inaktivität, zum Einsatz gekommene Programme und Anwendungen sowie der Internetverlauf. Bei mobilen Endgeräten lassen sich zusätzlich die GPS-Daten und Anrufstatistiken des Nutzers auswerten (Krause 2017).

Derartige Kontrolltechnologien verstärken den Druck auf die Bemessung und Standardisierung von Arbeitsschritten der Kopfarbeit, wie es in der Vergangenheit nur für Fließbandarbeit üblich war. Das kann dann bedeuten: „10 Minuten im Schnitt für eine E-Mail, 30 Minuten für ein Rechnungsformular, ein halber Tag, um einen Software-Fehler zu beseitigen." (Böhme 2017) Einerseits verlieren hochqualifizierte Beschäftigte durch derartige Kontrollprozesse Privilegien, insbesondere in den Bereichen Flexibilität und Autonomie, die Positionen auf der mittleren Arbeitsorganisationsebene bisher üblicherweise kennzeichnen. Andererseits erhöht die engmaschige Überwachung von Arbeitsprozessen die Konkurrenz unter den Beschäftigten: Fehler können schnell und systematisch aufgedeckt werden. Damit verschärfen Digitalisierungsprozesse nicht nur die scheinbar „objektive" Leistungskontrolle. Im Bereich der qualifizierten, wissensintensiven Angestelltenarbeit findet vielmehr eine professionelle Formalisierung statt, die, analog zur Einfacharbeit, zu Intensivierungs- und Abwertungsprozessen von Arbeit führt (Staab und Nachtwey 2016).

Die Digitalisierung überholt geltendes Recht: Neue Regelungsbedarfe

Nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) steht dem Betriebsrat ein Mitbestimmungsrecht bei der Einführung und Anwendung von technischen Einrichtungen zu, wenn diese das Verhalten oder die Leistung von Beschäftigten erfassen können. Das Mitbestimmungsrecht ist unabhängig davon, ob Arbeitgeber derartige Verhaltens- und Leistungskontrollen überhaupt durchführen wollen und ob überhaupt eine „Überwachungsabsicht" vorliegt. Vielmehr tritt dieses Recht bereits in Kraft, wenn eine technische Einrichtung personenbezogene Daten erfassen kann und entsprechende Verhaltens- und Leistungskontrollen ermöglicht. Damit können

Betriebsräte zwar grundsätzlich an der Ausgestaltung von betriebsinternen IT-Systemen mitwirken und die Beschäftigten vor technisch unterstützten Leistungs- und Verhaltenskontrollen ihrer Arbeitgeber schützen, der kollektivrechtliche Rahmen gerät aber aufgrund von Änderungen in der Arbeitsorganisation unter Druck (Wedde und Spoo 2015). Deutlich wird dies beim Einsatz digitaler Assistenzsysteme und der zunehmend betriebsübergreifenden Organisation von Wertschöpfungsprozessen in der Industrie 4.0.

Im Falle digitaler Assistenzsysteme dürfen die im Arbeitsrahmen gewonnenen Daten nach aktueller Rechtslage zwar zur Analyse von Qualifizierungsbedarfen und Ableitung von Schulungsmaßnahmen verwendet werden, nicht jedoch für allgemeine Verhaltens- und Leistungskontrollen. Weiterhin müssen die Arbeitenden ihre Überwachung in Assistenzsystemen in leicht wahrnehmbarer Weise erkennen können. Eine Ortung von Beschäftigten darf im Arbeitsbereich etwa nur in Ausnahmefällen permanent erfolgen. Jedoch konterkariert die Funktionsweise von digitalen Assistenzsystemen, die eine kontinuierliche Erfassung benötigen, diesen Regelungsansatz. Schließlich müssen Assistenzsysteme nach dem aktuellen Stand der Technik über 3D-Kameras oder Tiefensensoren kontinuierlich den Arbeitsbereich, Arbeitsablauf und die Bewegungen eines Werkers in der Produktion erfassen, um diesen mittels kontextsensitiver Hilfestellung zu entlasten.[9]

Zur gezielten Personalförderung darf ein Arbeitgeber erforderliche Fähigkeiten der Beschäftigten (z. B. Fremdsprachenkenntnisse) analysieren. Zudem darf er andere objektiv nachvollziehbare Parameter wie deren individuelle Arbeitsleistung zweckgebunden erfassen. Persönlichkeitsanalysen, die im Hintergrund stattfinden, ohne dass ein Betroffener weiß, welche Bewertungsmaßstäbe angelegt werden (People Analytics), sind jedoch arbeitsrechtlich wie datenschutzrechtlich unzulässig. Die Vorgabe ist dabei recht klar: „Menschen sollen wissen, was mit ihnen [und ihren Daten] passiert." (Mansmann 2017, S. 78f.)

Datengetriebene Entscheidungen können zudem den Gleichbehandlungsgrundsatz verletzen. Eine Ungleichbehandlung von Beschäftigten, etwa hinsichtlich der Bezahlung, ist nur akzeptabel, sofern sie sich nachvollziehbar an objektiven Leistungskriterien orientiert. Algorithmische Entscheidungen basieren jedoch auf der Erkennung abstrakter Muster und sind für die Betroffenen wenig transparent. Hier sind also

[9] *Siehe hierzu: BMBF-Forschungsprogramm „Technik zum Menschen bringen" (Verfügbar unter: www.technik-zum-menschen-bringen.de, zuletzt zugegriffen am 28.08.2017) und BMWi-Technologieprogramm „Autonomik für Industrie 4.0" (Verfügbar unter: www.digitale-technologien.de/DT/Navigation/DE/Foerderprogramme/Autonomik_fuer_Industrie/autonomik_fuer_industrie.html, zuletzt zugegriffen am 28.07.2017).*

neue Regelwerke und Maßstäbe notwendig, um zu definieren, welche Maßnahmen ethisch vertretbar und somit rechtlich zulässig sind. Allein die geltende Zustimmung von Beschäftigten und eine Zweckbindung der gewonnenen Daten reichen dafür nicht aus.

Den Analyseverfahren wird zudem die Fähigkeit zugeschrieben, menschliches Verhalten potenziell vorhersehbar zu machen – und in der nächsten Stufe die Beschäftigten sogar aktiv zu steuern, denn ein Arbeitgeber könnte „aus der Ferne und automatisierbar […] mit Informationsimpulsen direkt und im vielversprechendsten Augenblick in den Prozess der individuellen Willensbildung" (Roßnagel et al. 2016) eingreifen. Die technischen Möglichkeiten bewegen sich dabei zwischen einer Unterstützung bei der Entscheidungsfindung und Maschinen, die bereits algorithmisch und auf Basis fortgeschrittener Verfahren künstlicher Intelligenz selbst die Entscheidungen treffen und den Menschen entsprechend lenken. In diesem Raum realer und sich andeutender Möglichkeiten besteht die Gefahr, dass der Verlust der Kontrolle über die eigenständige Entscheidungsfindung unbemerkt geschieht.

Mit der Zunahme digital assistierter Arbeitsplätze finden sich die Beschäftigten also in einer Arbeitsumgebung wieder, in der die Erfassung und Verarbeitung ihrer personenbezogenen Daten eine neue Dimension erreicht – entweder als Nebeneffekt, wenn diese Techniken Arbeitsprozesse erleichtern, oder gezielt zum Zweck der Effizienzsteigerung. Ungeachtet der Potenziale für eine vollständige Automatisierung in bestimmten Arbeitsbereichen, in denen auch die Anforderungen an den Arbeitnehmerdatenschutz zurückgehen, werden die Herausforderungen der informationellen Selbstbestimmung für die weiterhin benötigten Beschäftigten komplexer, da diese in viel größerem Ausmaß als bisher, entweder wissentlich oder unwissentlich, mit intelligenten Systemen interagieren (Hornung und Hofmann 2015).

Dieser Effekt verstärkt sich noch, wenn Arbeit, Produktion und Dienstleistungen im Zuge der digitalen Vernetzung verstärkt betriebsübergreifend organisiert werden. So können intelligente Produktionssysteme, wenn sie standardisiert sind, über Unternehmensgrenzen hinweg miteinander kommunizieren und Zustands- und Prozessdaten austauschen. Mitarbeiter- und personenbezogene Daten finden somit potenziell auch Verwendung in betriebsübergreifenden Wertschöpfungsnetzwerken, die es den beteiligten Unternehmen erlauben, auf alle darin verfügbaren Informationen zurückzugreifen. Damit wird deutlich, dass die digitale Arbeitswelt das Arbeitsrecht als gesellschaftsregelnde und gestaltende Instanz vor ganz neue, grundlegende Herausforderungen stellt, die mit den Gegebenheiten in der klassischen Industriegesellschaft nichts mehr gemein haben. So werden im Zuge der Digitalisierung neue Arbeitsweisen (z. B. Crowd Working) möglich, die das bestehende Recht kaum abbildet, da es sich vor allem auf traditionelle Arbeitsverhältnisse bezieht.

Privatheit durch Technik: Chancen und Hemmnisse

„Datenschutz durch Technik" gilt oft als die wirksamste Methode zur Umsetzung der geltenden Datenschutzgrundsätze, da diese direkt in den technischen Systemen verankert werden. So muss nicht mühsam nachträglich verboten werden, was technisch gar nicht möglich ist (Hornung und Hofmann 2015, S. 175).

Dieser oft auch als Privacy by Design bezeichnete Grundsatz erfordert die Berücksichtigung von Privatheit, und zwar über alle Phasen der Erarbeitung und Herstellung intelligenter Systeme, beginnend bei Konzeption und Entwurf über die Implementierung, die Konfiguration bis hin zur Weiterentwicklung von Systemen (Hansen und Thiel 2012). Der Anspruch, Risiken für Privatheit und Persönlichkeitsrechte zu vermeiden bzw. zu minimieren, ist in der Praxis allerdings nicht einfach umzusetzen, da Technikentwicklung von Geschäftsmodellen abhängt und von der umfassenden Erhebung, Auswertung und Verknüpfung von Daten getrieben wird, nicht aber von deren zwangsläufiger Beschränkung und Kanalisierung durch Privacy-Erwägungen. So verwundert es nicht, dass bereits verfügbare technologische Möglichkeiten zum Schutz von Privatheit nicht umfassend genutzt werden.[10] Dies dürfte insbesondere für kleine Unternehmen gelten, die sich im Rahmen des digitalen Wandels mit für sie häufig noch völlig unbekannten Auswirkungen auf die Privatheit ihrer Mitarbeiter konfrontiert sehen.

Big-Data-Verfahren eröffnen also weitreichende Möglichkeiten, persönliche Merkmale zu bestimmen, Mitarbeiterprofile zu erzeugen und sogar menschliches Verhalten zu prognostizieren und zu beeinflussen. Traditionelle Datenschutzprinzipien wie die Zweckbindung, Datensparsamkeit beziehungsweise -minimierung, Verhältnismäßigkeit und die begrenzte Verarbeitung arbeits- und personenbezogener Informationen geraten daher unter Druck und erscheinen nicht mehr als zeitgemäß. Deshalb ist es notwendig, die Grundprinzipien des Datenschutzes neu zu gestalten. Die Chancen und Risiken datengetriebener Innovationen sollten in diesem Prozess allerdings nicht getrennt und unabhängig voneinander erörtert werden (Morlok et al. 2016).

„Datenschutz durch Technik" muss dabei über vereinzelte, fragmentierte Forschungs- und Gestaltungsansätze hinausgehen und sich zu einem systematischen, nachvollziehbaren Prozess, besser einer vollständigen Methodik erweitern (Fischer-Hübner et al. 2011). Auf diesem Weg werden zahlreiche noch ungelöste Fragen zu beantworten sein. Etwa: Wann besteht tatsächlich ein Personenbezug? Schließlich unterschei-

[10] *Siehe hierzu: Projekt ProPrivacy – Technische und rechtliche Untersuchung von Privatheit unterstützenden Technologien (Verfügbar unter: www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Abschlussbericht-Pro-Privacy.pdf?_=1446452292, zuletzt zugegriffen am 28.07.2017).*

det das Recht zwischen personenbezogen und anonym. In der Praxis ist diese Unterscheidung allerdings nicht mehr einfach zu treffen. Wie lässt sich also überhaupt feststellen, ob eine verlässliche Anonymisierung vorliegt?

Ausblick

Der hinreichende Schutz der Privatheit, der informationellen Selbstbestimmung und das Vertrauen in die Gewährung des Datenschutzes sind zentral für die Akzeptanz von digitalen Unterstützungssystemen. Dies gilt auf der operativen, einzelbetrieblichen Ebene genauso wie auf der gesellschaftlichen Ebene einer digitalen Transformation der Arbeitswelt.

Recht, Technik und Arbeitsorganisation sowie die Mitarbeiterkompetenz in Bezug auf Privatheit und Selbstbestimmung müssen daher gemeinsam und ganzheitlich betrachtet werden, etwa um Standards für anonymisierte, pseudonymisierte Daten und zum Umgang mit Einwilligungen zur Datenverarbeitung in der Praxis zu erarbeiten.

Für Unternehmen wie für Mitarbeiter ist zudem Rechtssicherheit zu schaffen: Wo sind die Grenzen und wo die Leitplanken bezüglich des Einsatzes digitaler Technologien in der Arbeitswelt? Gerade bei den neuen, sich in der Digitalisierung herausbildenden Formen der Zusammenarbeit, wie etwa dem Crowd Working, sind diese Fragen noch unbeantwortet. Daraus ergibt sich die weiterführende Frage, welche Orientierungshilfen dem Einzelnen gegeben werden können. Um ein Bewusstsein über existierende und verbleibende Risiken herzustellen, sind die IT-Kompetenzen hinsichtlich Datenschutz und digitaler Souveränität daher auszubauen. In diesem Zusammenhang ist auch die betriebliche Mitbestimmung zu stärken, etwa durch neue intelligente IT-Unterstützung für Betriebsräte. Privatheit ist dabei auch als eine Grundbedingung zur freien, unbeeinflussten Meinungsäußerung zu sehen.

Ein im betrieblichen Umfeld geschaffenes Bewusstsein hinsichtlich informationeller Selbstbestimmung kann darüber hinaus auch eine Multiplikator-Funktion einnehmen: Ein verantwortungsvoller Umgang mit personenbezogenen Daten ist in allen Lebensbereichen wichtig, erfordert jedoch in vielen Fällen erst eine Sensibilisierung und einen Ausbau der Wissensgrundlage.

Die Intransparenz von Datenerhebung und -verarbeitung sowie der potenziellen Bildung von Mitarbeiterprofilen ist letztendlich ein Problem, das intern bei Belegschaft und Arbeitgebern das Vertrauensverhältnis schwächen und die Reputation nach außen leiden lassen kann. Durch Intransparenz wird die Chance vergeben, verantwortungsvolles Verhalten zu demonstrieren. Nur wenn die Privatheit Gewicht hat, kann gegenseitiges Vertrauen als Grundlage guter digitaler Arbeit entstehen. Dies ist ein Qualitätsmerkmal, das auch Vorteile bei der Anwerbung von neuen Mitarbeitern bringt und langfristig die Zufriedenheit aller Beschäftigten sicherstellen kann.

Literatur

Arntz, M.; Gregory, T.; Lehmer, F.; Matthes; B.; Zierahn, U. (2016). Arbeitswelt 4.0 – Stand der Digitalisierung in Deutschland. Dienstleister haben die Nase vorn. Institut für Arbeitsmarkt- und Berufsforschung (IAB) (Hrsg.). Nürnberg (22/2016).

Bundesministerium für Arbeit und Soziale (BMAS) (2016). Grünbuch Arbeiten 4.0 – Arbeit weiter denken. Verfügbar unter: www.bmas.de/SharedDocs/Downloads/DE/PDF-Publikationen-DinA4/gruenbuch-arbeiten-vier-null.pdf?__blob=publicationFile, zuletzt zugegriffen am 26.07.2017.

Bundesministerium für Wirtschaft und Energie (BMWi) (2015). Erschließen der Potenziale der Anwendung von „Industrie 4.0" im Mittelstand. Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi)., agiplan GmbH, Fraunhofer IML und ZENIT GmbH. Mülheim an der Ruhr.

Böhme, J. (2017). 10 Minuten für eine E-Mail, 30 für eine Rechnung. In: brand eins Wirtschaftsmagazin (3/2017).

Fischer-Hübner, S.; Hoofnagle, C. J.; Krontiris, I.; Rannenberg, K.; Waidner, M. (2011). Online Privacy: Towards Informational Self-Determination on the Internet (Dagstuhl Perspectives Workshop 11061). In: Dagstuhl Manifestos 1(1): 1–20 (2011).

Geisberger, E.; Broy, M. (Hrsg.) (2012). Integrierte Forschungsagenda Cyber-Physical Systems. agendaCPS. acatech – Deutsche Akademie der Technikwissenschaften e. V. (acatech). Berlin, München: acatech STUDIE.

Hansen, M.; Thiel, C. (2012). Cyber-Physical Systems und Privatsphärenschutz. In: Datenschutz und Datensicherheit – DuD Januar 2012, Volume 36, Issue 1, S. 26–30.

Hornung, G.; Hofmann, K. (2015). Datenschutz als Herausforderung der Arbeit in der Industrie 4.0. In: Hirsch-Kreinsen, H. et al. (Hrsg.). Digitalisierung industrieller Arbeit: Die Vision Industrie 4.0 und ihre sozialen Herausforderungen. Baden-Baden: Nomos Verlagsgesellschaft, S. 165–182.

Jerchel, K. (2015). Datenschutz und Persönlichkeitsrechte für Beschäftigte in der digitalisierten Welt. In: ver.di-Bereich Innovation und Gute Arbeit (Hrsg.). Gute Arbeit und Digitalisierung. Prozessanalysen und Gestaltungsperspektiven für eine humane digitale Arbeitswelt. Berlin.

Krause, R. (2017). Digitalisierung und Beschäftigtendatenschutz. Bundesministerium für Arbeit und Soziales (BMAS). Berlin (Forschungsbericht, 482).

Mansmann, U. (2017). Big Data im Arbeitsrecht: Rechte und Pflichten des Arbeitgebers bei der Datenverarbeitung. In: c't 2017, Heft 1, S. 78–79.

Morlok,T.; Matt, C., Hess, T. (2016). Führung und Privatheit in der digitalen Arbeitswelt – Auswirkungen einer erhöhten Transparenz. In: Datenschutz und Datensicherheit – DuD Mai 2016, Volume 40, Issue 5, S. 310–314.

Roßnagel, A.; Geminn, C. L.; Richter, P.; Jandt, S. (2016). Datenschutzrecht 2016 „Smart" genug für die Zukunft? Ubiquitous Computing und Big Data als Herausforderungen des Datenschutzrechts. Kassel: Kassel University Press.

Staab, P.; Nachtwey, O. (2016). Die Digitalisierung der Dienstleistungsarbeit. In: Aus Politik und Zeitgeschichte (APuZ), 66. Jahrgang (18-19), S. 24–31.

Statista (2016). Umfrage zum Vertrauen in Arbeitgeber bei der Nutzung privater Daten in Europa 2015. Verfügbar unter: http://de.statista.com/statistik/daten/studie/567392/umfrage/vertrauen-in-den-arbeitgeber-bezueglich-der-nutzung-privater-daten, zuletzt zugegriffen am 18.06.2017.

Wedde, P.; Spoo, S. (2015). Mitbestimmung in der digitalen Arbeitswelt. In: ver.di-Bereich Innovation und Gute Arbeit (Hrsg.). Gute Arbeit und Digitalisierung. Prozessanalysen und Gestaltungsperspektiven für eine humane digitale Arbeitswelt. Berlin, S. 30–39.