Kapitel 3

STAAT

Mehr Daten, weniger Vertrauen in Statistik

–

Wie Zuhause so im Cyberspace? Internationale Perspektiven auf digitale Souveränität

–

Bildung als Voraussetzung digitaler Souveränität

V. Wittpahl (Hrsg.), *Digitale Souveränität*,
DOI 10.1007/978-3-662-55788-4_3, © Der/die Autor(en) 2017

Quellenangaben: Anhang, Quellenverzeichnisse der Zahlen und Fakten

__85 Prozent__ der Internetnutzer glauben, dass man nicht herausfinden kann, welche staatlichen Stellen oder Unternehmen persönliche Daten ihrer Kunden speichern. __70 Prozent__ möchten, dass die öffentliche Verwaltung ihre Dienste verstärkt auch online anbietet. Im Jahr 2009 hielten __44 Prozent__ der Bürger den Staat verantwortlich für den Datenschutz im Internet – 2014 waren es nur noch __15 Prozent__.

__55 Prozent__ können sich vorstellen, per Internet zu wählen. __80 Prozent__ der Befragten sind der Meinung, dass es neue Gesetze braucht, damit Fake News in den sozialen Medien schneller gelöscht werden. __74 Prozent__ meinen, dass man ohne die Nutzung digitaler Medien von vielen Bereichen des alltäglichen Lebens ausgeschlossen ist. __61 Prozent__ glauben, dass Fake News unsere Demokratie bedrohen. In Deutschland haben __31 Prozent__ der Internetnutzer keinen Schulabschluss oder einen Hauptschulabschluss.

3.1 Mehr Daten, weniger Vertrauen in Statistik

Thomas Gaens, Stefan Krabel

Welche Auswirkungen es hat, wenn Datenkompetenzen hinter den Anforderungen einer digital verwalteten Gesellschaft zurückbleiben, zeigt dieser Beitrag. Zudem wird diskutiert, welche Ansatzpunkte es gibt, um Big Data[1] sinnvoll zu nutzen, welche Voraussetzungen dazu nötig sind und wie die Gefahr von beliebiger Interpretation von Daten und Informationen abgewendet oder zumindest gemildert werden kann.

Wissen ist Macht. Im Sinne des englischen Philosophen Francis Bacon, auf den diese Redewendung zurückgeht, ist damit gemeint, dass Wissen um kausale Zusammenhänge Macht steigern kann. Denn diejenigen, die Ursache und Wirkung einander zuordnen können, ermächtigt dieses Wissen dazu, Wirkungen voraussehen und durch die Veränderung ihrer Ursachen beeinflussen zu können.

Jedem Bürger Zugang zu Wissen zu ermöglichen, um ihn dazu zu befähigen, seine Unmündigkeit abzulegen und an der Gestaltung des gesellschaftlichen Zusammenlebens teilhaben zu können – so lautet der über Bacons Schlussfolgerung hinausgehende bildungspolitische Appell, der seinen Weg in die Prinzipien der europäischen Aufklärung fand.

Zugang zu Wissen gilt als elementare Grundlage für eine demokratische Gesellschaft. Doch wie entsteht Wissen eigentlich? Ausgangspunkt sind Daten. Um daraus Erkenntnisse ableiten zu können, müssen Daten ausgewertet und interpretiert werden. Je besser Daten bereits Geschehenes abbilden, umso besser lassen sich mit ihrer Hilfe Prognosen für künftige Entwicklungen erstellen.

In modernen Wissensgesellschaften kommt der Verwendung von Daten deshalb eine zentrale Bedeutung zu. Kenntnis über verschiedene Methoden zu Auswertung von Daten ist nötig, um einschätzen zu können, wie Ergebnisse und Prognosen von Datenauswertungen zustande kommen, wie valide diese sind und wie stark respektive vorsichtig sie interpretiert werden sollten. Derartige Einschätzungen erfordern ihrerseits die Fähigkeit zur kritischen Bewertung der verwendeten Informationen: Welche Daten wurden ausgewertet? Wie wurden diese zusammengestellt und wel-

[1] *Big Data ist ein Komplex aus großen Datenmengen, der Kombination verschiedener Datenquellen und auf diese Eigenschaften angepassten Auswertungsmethoden.*

che wurden gegebenenfalls nicht betrachtet? Dies alles erfordert Kompetenzen bezüglich der Daten – sowohl von der Person, die diese auswertet als auch von der Person, die diese Ergebnisse dann verarbeitet. Insofern sind Transparenz und die Kommunikation der Grenzen von Analysemethoden und Prognosen von zentraler Bedeutung, um das Vertrauen in empirische Evidenz wieder zu stärken. Dadurch kann auch die Legitimation von politischen Prozessen auf der Grundlage empirischer Evidenz und den Dialog über diese Evidenz wieder an Bedeutung gewinnen.

Statistik in der Krise?

Die im allgemeinen Sprachgebrauch als westlich bezeichneten Gesellschaften haben den aufklärerischen Bildungsauftrag weitestgehend umgesetzt. Der Zugang zum gesellschaftlich geteilten Wissensfundus ist auch heute nicht für jeden gleichermaßen, wohl aber prinzipiell möglich. Verwaltet wird das bereits gewonnene Wissen von Wissenschaftlern, die auch für die Erweiterung des Wissensfundus und gegebenenfalls für Korrekturen zuständig sind. Sie erheben Daten und werten sie aus. Damit stellen sie in einer funktional differenzierten Gesellschaft das Wissen zur Verfügung, das als Grundlage für politische Entscheidungen dient. Politiker nutzen dieses Wissen, um Entscheidungen treffen zu können, die die Gesellschaft näher an ihre Vorstellungen eines optimalen Zustands bringen sollen. Die Bürger schließlich entscheiden per Wahl, welche politischen Ideen umgesetzt werden sollen. Da Bürger auch Zugang zu dem Wissen haben, das Grundlage der politischen Entscheidungen ist, sind sie im Prinzip auch dazu in der Lage, die darauf beruhenden politischen Ideen zu bewerten.

Datenkompetenzen müssen alle Beteiligten aufweisen: Für Wissenschaftler sind sie eine der Voraussetzungen ihres Berufs. Für sie sollte es selbstverständlich sein, sowohl bei der Datenerhebung und -auswertung als auch bei der kritischen Einordung von Forschungsergebnissen auf dem neuesten Stand zu bleiben. Doch auch Politiker und Bürger müssen dazu fähig sein, Forschungsergebnisse anhand ihrer Entstehung zu bewerten, um ihren Gebrauchswert beurteilen und sie nutzen zu können. Nur wenn die Bürger Wissen über gesellschaftliche Zusammenhänge besitzen, können sie überhaupt in mündiger Form an der politischen Gestaltung partizipieren.

Der Grad der Mündigkeit der Bürger bestimmt die konkrete Ausgestaltung der Dreiecksbeziehung zwischen ihnen, der Politik und der Wissenschaft in entscheidendem Maße: Wenn die Bürger nicht mehr beurteilen können, was wahr ist und was nicht, sind sie auch nicht mehr fähig, politische Entscheidungen rational zu bewerten. Diese Gefahr wächst, wenn in Massen falsche oder irreführende Nachrichten (Fake News) als sogenannte alternative Fakten verbreitet werden.

Mangelndes Vertrauen und seine Ursachen

Falschmeldungen in öffentlichen Berichterstattungen sind zwar kein exklusives Produkt des digitalen Zeitalters. Die Häufigkeit, mit der sie heutzutage auftreten, und ihre inzwischen enorme Reichweite, die sie zu einem relevanten Faktor der öffentlichen Meinungsbildung werden lassen, sind es jedoch schon.

Seine Bedeutung verdankt dieses neue Phänomen den interessengeleiteten Fake News vor allem sozialen Netzwerken wie Facebook oder Twitter, in denen die Verbreitung von Informationen in Abhängigkeit von ihrer potenziellen Reichweite erfolgt. Was zählt, sind Klicks und die mit ihnen verbundenen Werbeeinnahmen. Der regulierende Charakter einer medialen Sorgfaltspflicht, wie sie sich im traditionellen Pressewesen über einen langen Zeitraum hinweg herausbilden konnte, existiert hier nicht. Dort, wo sich nach unzähligen Reproduktionen durch verschiedenste Formen des Teilens unter den Mitgliedern in der sozialen Medienwelt sowieso nicht mehr ohne enormen Rechercheaufwand nachvollziehen lässt, aus welcher Quelle eine Nachricht stammt oder gar wie verlässlich diese Quelle ist, sind der Verbreitung sogenannter alternativer Fakten keine Hürden gesetzt.

In einer Welt, in der für den einzelnen Bürger immer undurchschaubarer wird, welche Aussagen der Wahrheit entsprechen und welche Fantasieprodukte sind, ließe sich annehmen, dass statistisch fundierte Aussagen eine willkommene Orientierungshilfe wären. Stattdessen lässt sich jedoch nationenübergreifend ein mangelndes Vertrauen in Statistik feststellen – sei es in Hinblick auf die deutsche Inflationsrate (Forsa-Umfrage im Auftrag des Stern-Magazins, Weber 2014), auf Angaben der britischen Regierung zur Zahl der im Land lebenden Immigranten (Umfrage von YouGov, Rogers 2015) oder auf die gesamte staatliche Wirtschaftsstatistik der USA (vgl. Marketplace-Edison Research Poll, Ryssdal 2016). Dieser Befund mag in Anbetracht eines steigenden Anteils ausgebildeter Akademiker, die durch ihr Studium in statistischen Methoden geschult sind (vgl. Buschle und Hähnel 2016), zunächst paradox wirken, ist bei genauerer Betrachtung jedoch nachvollziehbar.

Erstens können die Bürger auch in etablierten Medien zunehmende Ungenauigkeiten von Meinungsumfragen beobachten, die in der öffentlichen Wahrnehmung einen prominenten Platz der Außendarstellung statistischer Analysen einnehmen. Zwei prominente Beispiele aus dem Jahr 2016: Prognosen sahen bei der Abstimmung der britischen Bürger im Referendum zum sogenannten Brexit eine höhere Wahrscheinlichkeit für einen Verbleib Großbritanniens in der EU, und Hillary Clinton galt auch sehr spät im US-Wahlkampf noch als klare Favoritin. Beide Prognosen stimmten nicht.

Zweitens nutzen Politiker statistische Ergebnisse oft auf fahrlässige Art und Weise. Dass aus dem Kontext gerissene Zahlen als Beleg für nicht statistisch fundierte Mei-

nungen herhalten müssen, ist gerade im Wahlkampf keine Seltenheit, ebenso wenig wie die eigenmächtige Umdeutung von Analyseergebnissen. Donald Trump hat bewiesen, dass es möglich ist, sogar mit dem kontinuierlichen Gebrauch nachweislich frei erfundener Zahlen US-Präsident zu werden. Dieser „numerische Nihilismus", wie ihn die Journalistin Catherine Rampell (2016) nennt, führt dazu, dass in der Öffentlichkeit Zahlen kursieren, die widersprüchlich sind. Solche Widersprüche hinterlassen ratlose Wähler. In einer Studie von BritishFuture zum Thema Immigration gaben Befragte beispielsweise an, dass verschiedene Parteien für entgegengesetzte Positionen jeweils Fakten und Auswertungen präsentieren und die Wähler schlicht nicht einschätzen können, welche Seite die validierten und näher an der Wahrheit liegenden Auswertungen präsentiert.[2]

Statistische Berechnungen erhalten durch die genannten Fehleinschätzungen und bisweilen widersprüchlichen Forschungsergebnisse den Eindruck der Beliebigkeit. Hinzu kommt, dass auch Falschmeldungen häufig mit – erfundenen – statistischen Parametern versehen sind. Und wie soll ein Nutzer bei viral verbreiteten und von ihren Quellen entkoppelten Meldungen bewerten, ob die Daten, die ihm gerade präsentiert werden, um eine Aussage zu be- oder widerlegen, zuverlässig sind? In Anbetracht der Datenflut, die auf digitalem Weg entstehen kann, ist es verständlich, dass eine angemessene Skepsis gegenüber zahlenmäßigen Aussagen ohne Quelle zu einem allgemeinen Vertrauensverlust bis hin zu reflexartigem Misstrauen (vgl. Katwala et al. 2014) gegenüber empirischen Befunden mutiert.

Mangelndes Vertrauen und seine Folgen

Die – tatsächliche wie wahrgenommene – Krise der Statistik und der daraus entstehende Vertrauensverlust in empirische Befunde produzieren zwei sich komplementär zueinander verhaltende, folgenschwere Veränderungen im politischen Legitimationsprozess:

1. Wenn der digital unmündige Bürger nicht mehr fähig ist, politische Entscheidungen rational zu beurteilen, führt dies entweder dazu, dass er nicht mehr von seiner Wahlmöglichkeit Gebrauch macht, oder aber dazu, dass er seine Wahl auf andere Entscheidungshilfen stützt. Was noch bleibt, wenn sachliche Argumente wegfallen, sind emotionale Erwägungen. Oder anders formuliert: Verstehe ich nicht, wem ich folgen sollte, liegt es nahe, dem zu folgen, der mich zu verstehen scheint.

[2] *„Both sides fire a lot of facts and figures at you, which they bandy around. Facts and figures – in the end you believe what you want. They are both as convincing as each other. That's the problem. And you don't know quite – well, I can't make my mind up – which side is being honest with these figures." (Katwala et al. 2014, S. 27, herv. i. O.)*

2. Wenn der digital unmündige Bürger politische Entscheidungen nicht mehr rational beurteilt, müssen Politiker an die Emotionen der Wähler appellieren, um die Ermächtigung zu erhalten, ihre politischen Ideen umsetzen zu können.

Wissenschaftliche Erkenntnisse – unabhängig von ihrer Bedeutung für tatsächliche politische Entscheidungen – verlieren durch diese Entwicklung ihren Wert im politischen Legitimationsprozess. Die Menschen tendieren dazu, eher ihrem Bauchgefühl zu vertrauen als wissenschaftlicher Erkenntnis. So stimmen 38 Prozent der im Wissenschaftsbarometer 2016 Befragten der folgenden Aussage zu: „Die Menschen vertrauen zu sehr der Wissenschaft und nicht genug ihren Gefühlen und dem Glauben." Nur 32 Prozent stimmen nicht zu (Abbildung 3.1.1). Dies bedeutet jedoch nicht, dass Datenauswertungen in Zukunft keine Rolle mehr bei politischen Entscheidungen spielen können und werden. Es gibt aber andere – und mehr – Daten und Datensätze, die verschiedene Akteure nutzen und darstellen können.

„Letztlich geht es in der immer lebhafter werdenden Debatte [der digitalen Souveränität] um nichts weniger als die Neuverhandlung der Machtgrenzen zwischen Staaten, ihren Bürgern und einer globalisierten Wirtschaft." (Lepping und Palzkill 2016, S. 17) Die Staaten sind dabei, als Verlierer dieser Verhandlungen vom Tisch zu gehen, und die digitale Mündigkeit ihrer Bürger steht dabei auf dem Spiel.

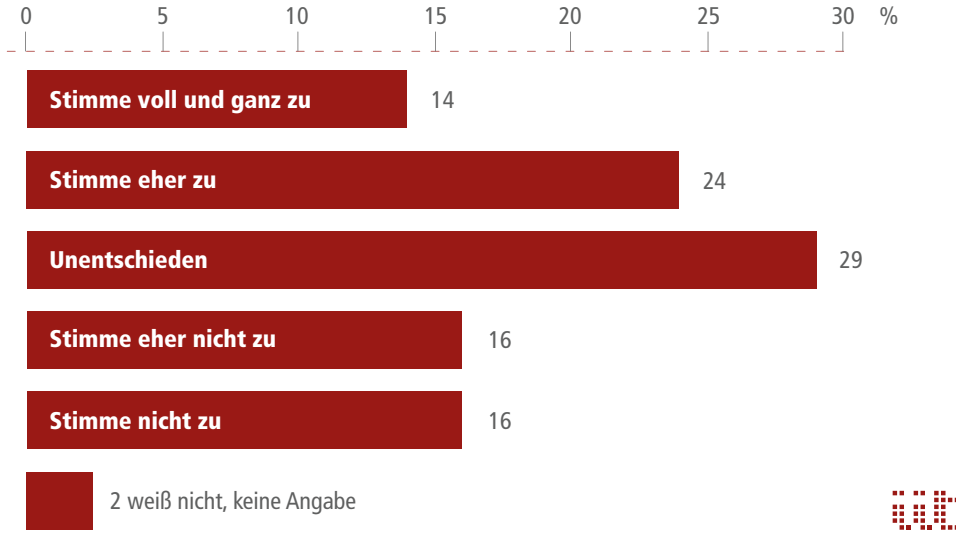

Abbildung 3.1.1: Vertrauen in die Wissenschaft (Zustimmung zur Aussage, dass die Menschen zu sehr der Wissenschaft und nicht genug ihren Gefühlen und dem Glauben vertrauen). Quelle: WiD und TNS emnid 2016

Big Data und ihre Gefahren

Die Erfassung und Verknüpfung riesiger Datenmengen ist inzwischen nicht nur technisch möglich, sondern bildet auch einen gewaltigen Markt. Erfasst wird längst nicht mehr nur das Surfverhalten am heimischen PC oder auf dem Smartphone, sondern jede Handlung, die digital abgebildet ist. Und mit der fortschreitenden Digitalisierung aller Lebensbereiche werden immer mehr personenbezogene Daten aus ehemaligen Offline-Bereichen gesammelt: Über die WLAN-fähige Zahnbürste und den Fitness Tracker sind das Vitaldaten, über das Payback-Konto die Einkäufe, über Fahrassistenzsysteme Routen und über das Smart Home jede Einstellung im eigenen Heim. Vollständige Datenverfügbarkeit ist keine Illusion mehr, sondern nur noch eine Frage der Vernetzung der einzelnen Elemente untereinander – sie vollzieht sich unter dem Stichwort Internet of Things (IoT). Heute sind mehr personenbezogene Daten erfasst als jemals zuvor – und es werden täglich mehr, solange bis jede Handlung digital abgebildet und gespeichert wird und alles mit allem vernetzt ist. Neben Daten, die das Handeln selbst abbilden, wird auch jede Äußerung in sozialen Netzwerken, Kommentarspalten und Foren, die die Einstellungen und die Emotionen der Nutzer ausdrückt, erfasst.

Für Statistiker klingt die vollständige Datenverfügbarkeit zunächst einmal wie ein paradiesischer Zustand. Der Omitted-Variable-Bias – verzerrte Schätzungen aufgrund nicht-berücksichtigter Variablen – wäre nur noch ein Problem unvollständiger theoretischer Modellierungen, eigene Erhebungen wären hinfällig. Doch so einfach ist es nicht, denn Big Data ist kein öffentliches Gut. Die Nutzer bezahlen alle Annehmlichkeiten der Digitalisierung mit den Rechten an ihren Daten. Die Kontrolle über Big Data liegt in kommerziellen Händen. Im Verborgenen wird hier „Data Mining" betrieben, also das – in der Regel theorielose – Aufspüren von Zusammenhängen zur Modellierung von Trends und anderen Mustern. Das tatsächliche Verhalten digital vernetzter Menschen zu erfassen bedarf keines großen Mehraufwands: Bewegungsprofile, Ernährungsgewohnheiten, Konsumvorlieben, präferierte Freizeitaktivitäten, sexuelle Orientierungen und vieles mehr werden bei der Nutzung von Apps bereitwillig eins zu eins an die Server privatwirtschaftlicher Unternehmen übermittelt – sofern die Nutzer, wie üblich, die Nutzungsbedingungen ignorieren.

Doch auch politische und persönliche Einstellungen lassen sich bei ausreichender Auskunftsfreudigkeit im Internet anhand digitaler Fußspuren und Fingerabdrücke nahezu perfekt rekonstruieren, unter anderem durch die Verwendung von Sentiment-Analysen. Und der dafür notwendige kritische Punkt an bereitgestellten Informationen ist immer leichter zu erreichen. Denn Big-Data-Auswertungen haben klassischen, statistischen Analysen begrenzter Datenmengen gegenüber einen Vorteil: Je größer die Fallzahl und die Zahl der miteinander vernetzten Variablen, umso unbedeutender wird der Vorhersagefehler von Schätzungen – oder anders formuliert: Je

mehr ich weiß, umso geringer ist die Wahrscheinlichkeit, dass ich aus meinem Wissen die falschen Schlussfolgerungen ziehe.

Wenn Politiker an die Emotionen der Wähler appellieren müssen, um von ihnen den Auftrag zu erhalten, ihre politischen Ideen umsetzen zu können, bietet Big Data den perfekten Ausgangspunkt. War es für das Agenda-Setting im klassischen Sinne noch notwendig, etwa über Umfragen selbst herauszufinden, welche Themen die Bürger bewegen, lassen sich inzwischen – von den Menschen größtenteils unbemerkt – unmittelbare Anknüpfungspunkte an emotionale Befindlichkeiten aus Big Data auslesen. Wenige stabile Muster über die Einstellungen einer ausreichend großen Personengruppe sind alles, was es für das Zusammenspinnen eines emotionalen Narrativs[3] bedarf.

Politischer Erfolg ist für denjenigen wahrscheinlicher, der seine Themen nach bereits im Vorhinein vorhandener Zustimmung definiert. Es spielt keine Rolle mehr, ob Aussagen, im Wahlkampf getroffen, vollends der Wahrheit entsprechen – solange sich mit ihnen genug Wähler mobilisieren lassen, die sich durch deren Inhalt in ihren Meinungen bestätigt sehen und sich wahrgenommen und ernst genommen fühlen. Dieser Effekt wird dadurch verstärkt, dass die politische Meinungsbildung im digitalen Raum vor allem innerhalb bereits gefestigter Filterblasen stattfindet, in denen selbst krude Thesen einen Anschein von Common Sense erlangen und sich den Mantel des sogenannten gesunden Menschenverstands umhängen können. Für Politiker, die ihre Arbeit bisher auf der Grundlage rationaler Argumentation verfolgt haben, steigt innerhalb ihres dem Code Macht/Ohnmacht verpflichteten gesellschaftlichen Teilsystems (vgl. Luhmann 1987) der Anreiz, es selbst auch nicht mehr allzu genau mit der Wahrheit zu nehmen, insbesondere wenn „alternative Fakten" mehr Aufmerksamkeit und Zustimmung einbringen. Wissen über emotionale Anknüpfungspunkte und Einstellungsmuster erlangt allerdings nur, wer Zugang zu den entsprechenden Daten besitzt. Diese Bedingung begünstigt die Verlagerung politischen Einflusses und politischer Gestaltungsmöglichkeiten von Berufspolitikern bis hin zu Managern, die Big Data kontrollieren (wie etwa im aktuellen US-Kabinett), sei es durch eigene Nutzung oder den Verkauf (oder die Bereitstellung) der Daten.

An wissenschaftsethische Standards bei der Datenerfassung und -auswertung fühlt sich dieser Personenkreis nicht immer zwingend gebunden. Es besteht die Gefahr einer spiralförmigen Selbstverstärkung der skizzierten Machtverschiebung, die die digital getriebene Entdemokratisierung beschleunigen wird, wenn keine Widerstände gegen diese Entwicklung auftreten sollten.

---

[3] *Als Narrativ wird hier eine emotional wirksame Geschichte verstanden, die ein Gefühl des „Verstanden-Werdens" vermittelt.*

Wissen ist Macht. Es scheint jedoch, als besäße das Wissen über die Emotionen von Menschen im digitalen Zeitalter mehr Machtpotenzial als das Wissen um gesellschaftliche Zusammenhänge. Intransparente Handhabung der Daten, die von einigen wenigen globalen Unternehmen verwaltet werden, lässt nicht nur den Schutz digital Unmündiger zunehmend unrealistisch erscheinen. Als Grundlage für den Erfolg der machtpolitischen Strategie emotionaler Narrative bedroht Big Data den gesamten Prozess rational begründeter Meinungsbildung.

Die Bedeutung von Daten in Gesellschaft und Demokratie

Die Verlagerung der Kontrolle über Bevölkerungsdaten aus dem öffentlichen Raum in die kommerzielle Handhabung ist ein Prozess, der sich in Europa historisch bis zu den ersten Hochrechnungen demografischer Daten im 17. Jahrhundert, noch vollständig unter nationalstaatlicher Kontrolle, zurückverfolgen lässt (vgl. Davies 2017). Nicht nur diese Pfadabhängigkeit lässt vermuten, dass die rechtliche Regulierung von Datenerfassung und -nutzung alleine eine wenig erfolgversprechende Strategie im Kampf um die Verteidigung demokratischer Prinzipien darstellt. Vielmehr gilt es, erneut dort zu beginnen, wo bereits Bacon und seine Mitstreiter ansetzten: an der Vernunft der Bürger. Es bedarf eines Zeitalters der digitalen Aufklärung.

Der beschriebene Vertrauensverlust ist es, der korrigiert werden muss. Er ist fatal im Prozess der digital getriebenen Entdemokratisierung: Aus Big Data abgeleitete emotional wirksame Narrative verlieren auch im Angesicht valider, statistisch fundierter Befunde, die sie widerlegen, nicht an Überzeugungskraft, wenn niemand an deren Zuverlässigkeit glaubt. Wissenschaftliche Erkenntnis und die Möglichkeit, mit ihrer Hilfe zu argumentieren, können im politischen Prozess nur dann wieder an Bedeutung gewinnen, wenn die Wähler bereit und in der Lage sind, sogenannte alternative von echten Fakten zu unterscheiden. Eine notwendige, aber nicht hinreichende Bedingung dafür ist, die Verbreitung von Fake News einzudämmen. Darüber hinaus muss es aber auch gelingen, den Imageschaden statistischer Analysen in der öffentlichen Wahrnehmung zu reparieren und die Meinungsforschung aus ihrer Krise zu befreien. Es stellt sich demnach die Frage: Wie können das Vertrauen in empirische Evidenz wieder gestärkt und die Macht Big-Data-basierter Narrative beschränkt werden?

Die Grenzen klassischer statistischer Verfahren

Dazu gilt es zunächst einmal, sich der Ursachen der Fehlprognosen bewusst zu werden, die das Image statistischer Analyse in der Öffentlichkeit beschädigt haben: Warum lagen die Prognosen der Meinungsforscher sowohl bei der US-Wahl als auch bei der Abstimmung über den Verbleib Großbritanniens in der Europäischen Union so deutlich neben den tatsächlichen Ergebnissen? Mehrere Gründe sind hier zu nennen: Trump beispielsweise ist es gelungen, in bedeutendem Umfang Wählergruppen zu

mobilisieren, die in den Prognosemodellen nur gering gewichtet waren. Gleichzeitig haben die erfassten Wähler zu einem größeren Anteil als üblich eine falsche Wahlabsicht angegeben – hier dürfte das Phänomen der sozialen Erwünschtheit gewirkt haben: Auch Trumps Wählern wird nicht entgangen sein, dass seine Wahlkampfaussagen unverhohlen so ziemlich jede Minderheit diskriminierten, und nicht jeder von ihnen wird seine Zustimmung zu diesen Aussagen gegenüber Forschenden zugeben wollen. Darüber hinaus leidet die Zuverlässigkeit von Meinungsumfragen unter dem generellen Trend, dass viele nicht mehr bereit sind, an ihnen teilzunehmen, sowie unter dem speziellen Problem der geringeren Erreichbarkeit von potenziellen Teilnehmenden. Immer weniger Menschen nutzen einen Festnetzanschluss, der bislang als Standard galt, um telefonisch in Verbindung zu treten. Und schließlich ist es eine immer komplexer werdende Welt selbst, die sich nicht mehr so leicht erfassen lässt, wie es vielleicht einmal möglich war. Mit dem fortschreitendem Zerfall traditioneller Strukturen der Vergemeinschaftung, der stetigen Auflösung typischer Berufslaufbahnen und der zunehmenden Vervielfältigung gesellschaftlicher Zuschreibungsmuster, die die Individualisierung in modernen Gesellschaften produziert hat, geht ein Identifikationsverlust Einzelner einher. Für sie bleiben immer weniger gesellschaftliche Gruppen als Anker für eine Zugehörigkeit. Gemeinschaftsformen wie die Großfamilie schwinden, feste Berufslaufbahnen sind so stark flexibilisiert und kollektive Identität stiftende Schichtzugehörigkeiten haben sich nach so vielen Merkmalen ausdifferenziert, dass auch innerhalb der von Meinungsforschern definierten Gruppen inzwischen häufig mehr Unterschiede als Gemeinsamkeiten hinsichtlich Lebenslagen und Lebensstilen existieren. Die statistisch konstruierten Schubladen sind zu groß, um erfassen zu können, welche Vielfalt in ihnen herrscht (vgl. Davies 2017)[4].

Was die Meinungsumfragen hat ins Leere laufen lassen, ist also nichts anderes als das grundsätzliche und altbekannte Problem des statistischen Inferenzfehlers: „Zufallsstichproben bleiben im Kern eine Krücke. Ihnen fehlt die Detaildichte, um das zugrunde liegende Phänomen umfassend abzubilden" (Mayer-Schönberger 2015, S. 15). Je ungenauer die behandelte Stichprobe die Gesamtheit repräsentiert, umso unwahrscheinlicher ist es, dass die Verallgemeinerung der Analyseergebnisse den tatsächlichen Verhältnissen entspricht. Und je komplexer das zu erfassende Phänomen ist, desto schwieriger gestaltet sich eine zufriedenstellende Stichprobenauswahl.

Während Wissenschaftler sich weiterhin an ihre Krücke klammern, sind Big-Data-Analysten dabei, alleine laufen zu lernen. Für sie definiert vor allem die technische

[4] *„Traditional forms of statistical classification and definition are coming under strain from more fluid identities, attitudes and economic pathways. Efforts to represent demographic, social and economic changes in terms of simple, well-recognised indicators are losing legitimacy." (Davies 2017)*

Machbarkeit beim Handling immer schneller wachsender Datenmassen neue Herausforderungen bei der Auswertung unserer immer komplexer werdenden Welt. Das Problem des statistischen Inferenzschlusses wird für sie spätestens dann buchstäblich in der Datenflut untergehen, wenn die Vernetzung vollendet ist.

Big Data und ihre Möglichkeiten

Die empirische Forschung, die im öffentlichen Raum stattfindet und gesellschaftliche Entwicklungen fehlerhaft abbildet, leidet also an einer heilbaren Krankheit – an Datenmangel. Dass die Auswirkungen unvollständiger Daten auch im öffentlichen Raum abgemildert werden können, zeigt sich bereits an einigen wichtigen Beispielen; in den Gesundheitswissenschaften wird beziehungsweise wurde Big-Data-Nutzung bereits erfolgreich zur Vorhersage von Infektionen Neugeborener (vgl. McGregor 2013), bei der Prognose des Verlaufs von Grippewellen oder etwa der Ausbreitung von Malaria angewendet (vgl. Wesolowski et al. 2012).

Daten sind häufig prinzipiell verfügbar und erlauben die Kombination mehrerer Datensätze und die Integration sehr vieler verschiedener Merkmale. Wenn dabei die Analyseverfahren dieser komplexen Datenstruktur angemessen sind, ist ein Erkenntnisgewinn gegenüber klassischen Methoden der Datenerhebung und -auswertung absehbar. Das grundlegende Problem ist demnach keine Krise der Statistik im Allgemeinen, sondern ein Passungsproblem wissenschaftlicher Forschung: Denjenigen, die immer umfassenderes Datenwissen besitzen, lässt sich rein systemtheoretisch unterstellen, dass sie es nicht zum Wohle der Allgemeinheit nutzen, wenn dieses nicht zufällig ihrem Eigeninteresse entspricht. Diejenigen, die – zumindest in der Theorie – vor allem dem Wohle der Öffentlichkeit verpflichtet sind, besitzen häufig nicht genug Daten, um zuverlässig damit zu arbeiten.

Hinzu kommt eine allgemeine Skepsis gegenüber Big Data. Insbesondere Sozialwissenschaftler werden in ihrer Ausbildung stets darauf geschult, Korrelationen nicht mit kausalen Zusammenhängen gleichzusetzen. Eine in erster Linie mit Korrelationsanalysen, Trend- und Mustererkennungen konnotierte Form der Datenerfassung und -nutzung muss ihnen fast zwangsläufig zunächst einmal einen enormen Schrecken einjagen. Und tatsächlich wächst die Gefahr, auf Scheinkorrelationen hereinzufallen, mit steigendem Datenvolumen und steigender Variablenanzahl – schließlich steht alles irgendwie mit irgendetwas anderem in irgendeinem Zusammenhang. Das ist aber kein Grund, Big Data von vornherein zu verteufeln. Denn die Vorteile liegen auf der Hand:

- Big Data kann Verhalten direkt messen und nicht nur über zuvor zu operationalisierende Items Einstellungen abfragen.
- Big Data verzeiht Messfehler aufgrund der Kombination unterschiedlicher Datenquellen (vgl. Mayer-Schönberger 2015).

- Big Data erfasst Zusammenhänge, die sonst gar nicht registriert werden könnten, weil sie entweder in zu kleinen Fallzahlen versteckt sind oder sich aus bestehendem Wissen keine Hypothesen zu ihnen ableiten lassen.
- Mit Hilfe von Big Data kann nicht nur die Überprüfung von Hypothesen, sondern auch deren Generierung erfolgen (vgl. Anderson 2008).
- Im besten Fall erzwingt Big Data durch die Verknüpfung von Daten unterschiedlicher Forschungsbereiche sogar eine neue Form interdisziplinärer Theoriebildung, weil die Bedeutung vorgelagerter disziplinspezifischer Operationalisierungen abnimmt.

Nutzung von Daten in Politik, Gesellschaft und Demokratie

Unterm Strich bleiben zentrale Fragen: Wie soll die Politik, wie sollen Medien, wie soll die Gesellschaft Daten verwenden? Wie sollen statistische Ergebnisse interpretiert werden? Und was kann der Staat für einen Beitrag leisten? Zweifellos wäre es vermessen zu erwarten, dass breite Teile der Gesellschaft genügend tiefe Kenntnisse über Datengrundlagen und statistische Verfahren entwickeln, um statistische Ergebnisse stets sensibel einordnen zu können. Das bedeutet jedoch nicht, dass die Auswertung von Daten obsolet wird. Im Gegenteil: Das Vorbild der Gesundheitswissenschaften zeigt, dass mehr Daten und Kombinationen von Datenquellen einen Erkenntnisgewinn bedeuten können. Weitere Beispiele für den sinnvollen Einsatz von Big Data gibt es auch in internationalen Kontexten, etwa Analysen zu den Auswirkungen der Strenge rechtlicher Verpflichtungen in internationalen Verträgen auf die Ratifikationsgeschwindigkeit, zur Intensivität mit der nationale Parlamente EU-Themen debattieren (Tokhi und Rauh 2015) oder auch in Analysen der chinesischen Internetzensur (King et al. 2013).

Um einen Mehrwert aus Daten und empirischen Auswertungen zu erreichen, müssen zudem diejenigen, die Daten auswerten, ihre Erhebungen und Erhebungsinstrumente sorgfältig auswählen und die Grenzen der Interpretation transparent und verständlich kommunizieren. Letzteres ist umso bedeutender, je stärker eine empirische Information grundlegenden Einfluss auf Entscheidungen besitzt. Beispielsweise können empirische Aussagen in der Medizin, dass etwa Maßnahmen der Krebsvorsorge oder Impfungen die Wahrscheinlichkeit einer Krankheit verringern, die Entscheidungen von Patienten über eine Behandlung beeinflussen. Ausgesprochen wichtig ist hierbei, dass Mediziner deutlich und verständlich vermitteln, dass eine Behandlung die Wahrscheinlichkeit einer Erkrankung nur verringert, diese aber nicht ausschließt. Ebenfalls transparent kommunizieren müssen sie die Frage, wie stark die Wahrscheinlichkeit zu erkranken sinken kann.

Die verständliche und klare Bewertung von empirischer Evidenz ist daher auch eine zentrale Aufgabe und Herausforderung, wenn politische oder gesellschaftliche Ent-

scheidungen auf empirischer Evidenz basieren. Wenn den Menschen etwa bei Wahlprognosen klargemacht wird, dass diese auf Hochrechnungen mit Standardfehlern und Varianzen beruhen und dass letztgenannte statistische Maße den vorausgesagten Abstand zwischen Kandidaten übersteigen, gewinnen sie womöglich das Vertrauen in Hochrechnungen wieder zurück.

Um das Potenzial von Big Data ausschöpfen zu können, muss zudem die Methodenentwicklung und -ausbildung der Wissenschaftler mit der Digitalisierung Schritt halten. Neue Auswertungsmethoden müssen den Eigenschaften von Big Data gerecht werden: Der enorme Umfang an Daten, die nötige Geschwindigkeit bei der Auswertung und die Vielfalt der Datenstrukturen erschweren eine sinnvolle Anwendung klassischer statistischer Verfahren auf Big Data. Potenzielle Probleme sind Heterogenität bei Datenerhebungen, akkumulierte Stichprobenfehler und Scheinkorrelationen in der Auswertung sowie möglicherweise falsche Annahmen von Exogenität, die Auswertungen zugrunde gelegt werden. Demzufolge müssen weitere Big-Data-Verfahren in der Methodenlehre Aufnahme finden, um hohen wissenschaftlichen Ansprüchen in der Datenauswertung gerecht zu werden (vgl. Mahrt 2015).

Eine Hinwendung zu Big Data ist für die Wissenschaft über die Möglichkeit des Erkenntnisgewinns hinaus von zentraler Bedeutung. Sie ist außerdem eine notwendige Bedingung, um den gemeinschaftlichen Charakter wissenschaftlicher Forschung zu bewahren, denn die Alternative zu einer generellen Öffnung der Wissenschaft gegenüber Big Data ist eine Trennlinie zwischen wenigen Forschenden mit privilegiertem Zugang zu privaten Datensätzen und der digital abgehängten Masse („new kind of digital divide", Boyd und Crawford 2011, S. 13). Der Staat sollte eine solche Neuausrichtung in eigenem Interesse unterstützen.

Fazit und Ausblick

Momentan verfügen vor allem privatwirtschaftliche, gewinnorientierte Unternehmen über riesige Datensätze, aus denen sich Einstellungen von Nutzern auslesen lassen. Mit diesen Daten können emotionale Anknüpfungspunkte innerhalb von Bevölkerungsgruppen ermittelt werden. In emotional wirkende Erzählungen übersetzt, bieten diese Informationen die Möglichkeit, verunsicherte Wähler auch ohne Aussagen mit Wahrheitsgehalt zu mobilisieren, weil sie das Vertrauen in statistische Analyseergebnisse durch Fake News und fehlerhaften Meinungsprognosen zunehmend verlieren.

Die Datenkompetenzen der Menschen sind der Dreh- und Angelpunkt: Sind Bürger und Wähler nicht mehr in der Lage zu beurteilen, welche Daten valide und welche Analyseergebnisse wahr sind, sind Fakten auch nicht mehr relevant für ihre Beurteilung des politischen Legitimationsprozesses.

Dass Wähler allerdings selbst beurteilen könnten, welche der ihnen präsentierten Daten valide sind und welche Zahlen in welchem Maße reale Verhältnisse widerspiegeln, ist in funktional differenzierten Wissensgesellschaften nicht vorstellbar. Zu komplex sind die sozialen Zusammenhänge, die erfasst und ausgewertet werden, zu kompliziert die Erhebungs- und Auswertungsmethoden aussagekräftiger empirischer Studien. Es ist aber auch nicht notwendig, denn schließlich sind Wissenschaftler für diese Arbeit zuständig, auf die die übrigen Bürger ihre Datenkompetenzen im übertragenen Sinne auslagern können. Dafür ist jedoch Vertrauen nötig. Vertrauen in wissenschaftlich generierte Analyseergebnisse und Vertrauen, das momentan nicht vorhanden scheint.

Dieses Vertrauen wiederherzustellen ist außerordentlich wichtig, um den bereits entstandenen Schaden am politischen Legitimationsprozess zu reparieren und künftigen Schaden einzudämmen. Dazu muss aber offen gesagt werden, dass statistische Methoden bei bestimmten Fragestellungen an ihre Grenzen gelangt sind. Insbesondere Wissenschaftler, Meinungsforscher und Analysten sind hier in der Pflicht, zum einen die Ergebnisse von klassisch generierten Wahlprognosen als das darzustellen, was sie sind: Auf bestimmten Annahmen beruhende Verallgemeinerungen, die nur dann zutreffen, wenn diese Annahmen sich als korrekt erweisen. Diese Annahmen zusammen mit den Prognoseergebnissen transparent zu kommunizieren, wäre darüber hinaus hilfreich. Zum anderen müssen Wissenschaftler, Meinungsforscher und Analysten ihre Datenkompetenzen auch weiterentwickeln. Statistische Methoden müssen der Komplexität der Welt wieder gerecht werden und dabei gezielt die breite Streuung von Lebensverhältnissen und -stilen stärker in den Fokus nehmen, um eine zunehmende Abweichung von durchschnittlichen, leicht zu kategorisierenden Standards erfassen zu können.

Die zunehmende Verknüpfung immer mehr personenbezogener Daten lässt sich nicht aufhalten. Für welche Zwecke und auf welche Weise solche Daten unter privatwirtschaftlicher Kontrolle verwendet werden, wird sich alleine aufgrund ihrer schieren Masse künftig kaum noch wirksam kontrollieren und deshalb auch nicht sinnvoll reglementieren lassen. Statt aber einem intransparenten, häufig theorielosen Umgang mit solchen Daten das Feld zu überlassen und Big Data grundsätzlich abzulehnen, sollten insbesondere Wissenschaftler die Chance wahrnehmen, selbst Erkenntnisse aus Big Data zu gewinnen.[5]

[5] *Intuitiv mag sich an dieser Stelle die Problematik des Datenschutzes als potenzieller Hinderungsgrund aufdrängen. Es sollte jedoch bedacht werden, dass die Wissenschaft sowohl eher in der Lage sein wird, einen datenschutzwürdigen Umgang mit Big Data zu entwickeln (ggf. unter Weiterentwicklung der bisherigen Vorstellungen von Datenschutz, die einer digitalisierten Welt unter Umständen nicht mehr gerecht werden), als auch einen solchen Umgang gewissenhafter zu praktizieren als dies im privatwirtschaftlichen Rahmen zu erwarten ist.*

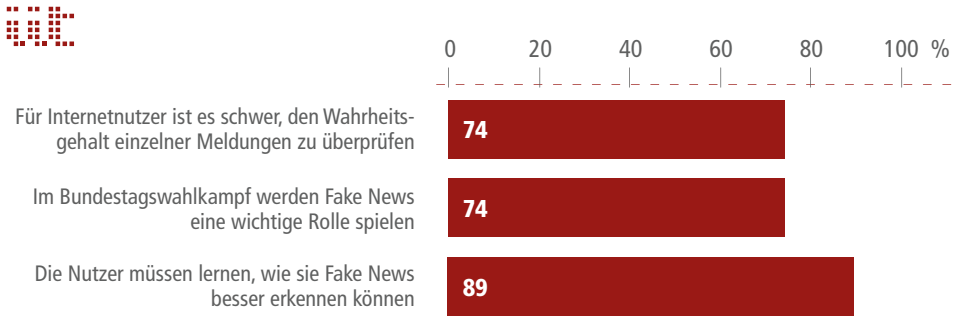

Abbildung 3.1.2: Die Bedeutung von Fake News in der Bevölkerung in Deutschland (Angabe: „stimme voll zu" und „stimme eher zu"). Quelle: bitkom research 2017

Wissenschaftler haben es also selbst in der Hand, ihre digitale Souveränität als „Fähigkeit zu selbstbestimmtem Handeln und Entscheiden im digitalen Raum" (Bitkom 2015, S. 7) durchzusetzen und damit auch die Mündigkeit der Bürger zu stärken. Die Menschen in diesem Land sind sich der grundlegenden Problematik ihrer digitalen Entmündigung durchaus bewusst und würden ihr gern etwas entgegensetzen (Abbildung 3.1.2) – es wird Zeit, sie dabei zu unterstützen. Der Wissenschaft und der Meinungsforschung kommt dabei die entscheidende Aufgabe zu, das Ansehen statistischer Analysen in der Öffentlichkeit wiederherzustellen und Transparenz im Datendschungel zu schaffen.

Literatur

Anderson, C. (2008). The end of theory: The data deluge makes the scientific method obsolete. In: Wired. Verfügbar unter: www.wired.com/2008/06/pb-theory, zuletzt zugegriffen am 21.07.2017.

Bitkom (Hrsg.) (2015). Digitale Souveränität. Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa. Bitkom. Berlin. Verfügbar unter: www.bitkom.org/Bitkom/Publikationen/Digitale-Souveraenitaet-Positionsbestimmung-und-erste-Handlungsempfehlungen-fuer-Deutschland-und-Europa.html, zuletzt zugegriffen am 21.07.2017.

bitkom research (Hrsg.) (2017). Zustimmung zu ausgewählten Aussagen zum Thema Fake News in Deutschland. Verfügbar unter: www.bitkom.org/Presse/Anhaenge-an-PIs/2017/02-Februar/Bitkom-Charts-PK-Fake-News-02-02-2017.pdf, zuletzt zugegriffen am 21.07.2017.

Boyd, D.; Crawford, K. (2011). Six Provocations for Big Data. Conference Paper, A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society. University of

Oxford. Oxford (Hrsg.). Verfügbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431, zuletzt zugegriffen am 21.07.2017.

Buschle, N.; Hähnel, S. (2016). Hochschulen auf einen Blick. Ausgabe 2016. Statistisches Bundesamt (Hrsg.). Wiesbaden. Verfügbar unter: www.destatis.de/DE/Publikationen/Thematisch/BildungForschungKultur/Hochschulen/BroschuereHochschulen-Blick0110010167004.pdf?__blob=publicationFile, zuletzt zugegriffen am 21.07.2017.

Davies, W. (2017). How statistics lost their power – and why we should fear what comes next. In: The Guardian, 19.01.2017. Verfügbar unter: www.theguardian.com/politics/2017/jan/19/crisis-of-statistics-big-data-democracy, zuletzt zugegriffen am 21.07.2017.

Katwala, S.; Ballinger, S.; Rhodes, M. (2014). How to talk about immigration. In: Ballinger, S. (Hrsg.). British Future. London. Verfügbar unter: www.britishfuture.org/wp-content/uploads/2014/11/How-To-Talk-About-Immigration-FINAL.pdf, zuletzt zugegriffen am 21.07.2017.

King, G.; Pan, J.; Roberts, M. E. (2013). How Censorship in China Allows Government Criticism but Silences Collective Expression. In: American Political Science Review, 107, S. 1–18.

Lepping, J.; Palzkill, M. (2016). Die Chance der digitalen Souveränität. In: Wittpahl, V. (Hrsg.). Digitalisierung. iit-Themenband. Institut für Innovation und Technik (iit). Springer: Berlin, S. 17–25. Verfügbar unter: www.iit-berlin.de/de/publikationen/digitalisierung, zuletzt zugegriffen am 21.07.2017.

Luhmann, N. (1987). Soziologische Aufklärung 4. Beiträge zur funktionalen Differenzierung der Gesellschaft. Opladen: Westdeutscher Verlag.

Mahrt, M. (2015). Mit Big Data gegen das „Ende der Theorie"? In: Maireder, A.; Ausserhofer, J.; Schumann, C.; Taddicken, M. (Hrsg.). Digitale Methoden in der Kommunikationswissenschaft. Berlin, S. 23–37.

Mayer-Schönberger, V. (2015). Was ist Big Data? Zur Beschleunigung des menschlichen Erkenntnisprozesses. In: Aus Politik und Zeitgeschichte (APuZ), (11–12/2015). Verfügbar unter: www.bpb.de/apuz/202242/zur-beschleunigung-menschlicher-erkenntnis?p=3, zuletzt zugegriffen am 21.07.2017.

McGregor, C. (2013). Big Data in Neonatal Intensive Care. In: Computer, 46 (6), S. 54–59.

Rampell, C. (2016). When the facts don't matter, how can democracy survive? In: Washington Post, 17.10.2016. Verfügbar unter: www.washingtonpost.com/opinions/when-the-facts-dont-matter-how-can-democracy-survive/2016/10/17/560ff302-94a5-11e6-9b7c-57290af48a49_story.html?utm_term=.0d5e5b880e93, zuletzt zugegriffen am 21.07.2017.

Rogers, J. F. (2015). Are conspiracy theories for (political) losers? YouGov UK. Verfügbar unter: https://yougov.co.uk/news/2015/02/13/are-conspiracy-theories-political-losers, zuletzt zugegriffen am 21.07.2017.

Ryssdal, K. (2016). Poll finds Americans' economic anxiety reaches new high. Marketplace – Edison Research. Verfügbar unter: www.marketplace.org/2016/10/13/economy/americans-economic-anxiety-has-reached-new-high, zuletzt zugegriffen am 21.07.2017.

Tokhi, A.; Rauh, C. (2015). Die schiere Menge sagt noch nichts. Big Data in den Sozialwissenschaften. In: WZB-Mitteilungen (150 der Gesamtfolge), S. 6–9.

Weber, M. (2014). Deutsche fühlen deutliche Inflation. In: stern-Magazin, 22.01.2014. Verfügbar unter: www.stern.de/wirtschaft/news/stern-umfrage-deutsche-fuehlen-deutliche-inflation-3130940.html, zuletzt zugegriffen am 21.07.2017.

Wesolowski, A.; Eagle, N.; Tatem, A. J.; Smith, D. L.; Noor, A. M.; Snow, R. W.; Buckee, C. O. (2012). Quantifying the impact of human mobility on malaria. In: Science, 338, S. 267–270.

Wissenschaft im Dialog (WiD); TNS emnid (Hrsg.) (2016). Wissenschaftsbarometer 2016. Verfügbar unter: www.wissenschaft-im-dialog.de/projekte/wissenschaftsbarometer/wissenschaftsbarometer-2016, zuletzt zugegriffen am 21.07.2017.

3.2 Wie Zuhause so im Cyberspace? Internationale Perspektiven auf digitale Souveränität

Stephanie Christmann-Budian, Johannes Geffers

Der Diskurs über die Digitalisierung – und die Zurückgewinnung einer zumindest relativen Souveränität – gewinnt zusätzlich an Komplexität, wenn man über die Grenzen hinaus auf andere globale oder regionale Akteure und deren Umgang mit digitaler Souveränität schaut. Im In- wie Ausland sind auf nationaler und regionaler Ebene unterschiedliche politische Strategien und Maßnahmen erkennbar, die geprägt sind von den jeweiligen politischen und soziokulturellen Systemen, in denen sie entstanden sind.

Der Begriff digitale Souveränität scheint sich als ein Kernbegriff im Digitalisierungsdiskurs zu etablieren, bleibt jedoch bereits auf deutschem Parkett nach wie vor reich an unterschiedlichen Interpretationen und Assoziationen. Seine Popularität vor allem im politischen Diskurs mag daher rühren, dass der Souveränitätsbegriff semantisch sehr gut den Wunsch nach einem Zustand auszudrücken vermag, den viele Menschen, Organisationen und auch Staaten angesichts einer sich scheinbar unbeherrschbar vollziehenden Digitalisierung der Gesellschaft schmerzlich vermissen. Die nur eingeschränkt sichtbaren Datenspuren, die wir auf digitalen Plattformen wie Facebook oder Twitter, eBay oder Alibaba, Google oder Baidu hinterlassen, oder die wiederholt erfolgreichen Angriffe auf die IT-Infrastruktur des Deutschen Bundestages, auf Kundendatenbanken großer Unternehmen und nicht zuletzt die Verwendung von speziellen Programmen von Sicherheitsdiensten durch Hackergruppen – all das hinterlässt leicht ein Gefühl der Ohnmacht.

In der rasanten Entwicklung zur digitalisierten Gesellschaft hat der Staat seine neue Rolle noch nicht gefunden. Er muss die Sorgen der Bürger ernst nehmen und selbst aus einer defensiven Haltung herausfinden, die nicht mehr nur auf den digitalen Fortschritt reagiert, sondern diesen aktiv mitgestaltet. In Deutschland sind die Debatten dazu wie gewohnt vielschichtig und mit Sorge erfüllt: Ist die digitale Souveränität Deutschlands bedroht? Wie sehen andere Gesellschaften die Entwicklung? Treiben die Menschen in anderen Ländern ähnliche Sorgen und Hoffnungen um, wie dies in Deutschland der Fall ist? Und wenn nicht, warum ist es um die Situation und die Sichtweisen auf die digitale Souveränität in anderen Staatssystemen und zugehörigen Gesellschaften so anders bestellt? Die Digitalisierung der Gesellschaft ist ein Prozess, der an nationalstaatlichen Grenzen mitunter gebrochen werden mag, aber er macht vor ihnen nicht halt. Ein Vergleich verschiedener internationaler Perspekti-

ven – aus China, Singapur, Estland, Dänemark sowie von internationalen Organisationen – kann helfen, gemeinsame Themen und Strategien zu identifizieren, Differenzen nachzuzeichnen, und die Situation in Deutschland vor diesem Hintergrund zu betrachten.

Status Quo

Digitale Souveränität wird in der Regel als ein Spannungsfeld zwischen Fremdbestimmung und Autarkie über die Erhebung, Übertragung, Verarbeitung sowie Speicherung von Daten beschrieben (vgl. Bitkom 2015). Es wird vorgeschlagen, verschiedene Ebenen der digitalen Souveränität wie etwa Gesellschaft, Organisationen und Individuen zu unterscheiden (vgl. Lepping und Palzkill 2016). Dies scheint hilfreich, um die bestehenden Hierarchien zwischen den Positionen von Individuen, Organisationen und Staaten fassen zu können, die wesentlich zu dem eingangs erwähnten Gefühl der Ohnmacht beitragen.

Einen anderen Zugang zur Beschreibung und Analyse benutzt Farid Gueham (2017, S. 11), der das Bild verschiedener, miteinander in Konflikt stehender Kreise digitaler Souveränität verwendet: Der erste Kreis betrifft die persönlichen Daten, die von Individuen zur Verfügung gestellt werden. Der zweite Kreis bezieht sich auf die digitale Souveränität von Unternehmen und anderen Organisationen, deren Daten zu ihren wesentlichen Ressourcen zählen. Der dritte und letzte Kreis ist bei Gueham schließlich für die Souveränität von Staaten reserviert, die auf die Debatten über den Datenschutz Einfluss nehmen können.

Zur Illustration von Konflikten zwischen den genannten Kreisen und Ebenen seien hier nur einige Schlaglichter auf vergangene und gegenwärtige Auseinandersetzungen und Kontroversen geworfen: Schon in den 1990er Jahren, als das Internet und andere Prozesse der Digitalisierung wie beispielsweise die der Finanzmärkte noch in den Kinderschuhen steckten, war die staatliche digitale Souveränität und ihre mögliche Bedrohung ein Thema westlicher Debatten. Frühe Analysen, die hier aus der Globalisierungsforschung stammen, kommen heutigen Fragestellungen bereits sehr nahe (vgl. Perrit 1998; Sassen 1998).

Ausgangspunkt des Austauschs zwischen Perrit und Sassen war die Vorstellung, dass die Bedrohung digitaler staatlicher Souveränität vor allem ein Problem autoritärer Staatssysteme sei, die einen Kontrollverlust durch eine vermehrte Möglichkeit zur Teilhabe an der gesellschaftlichen Öffentlichkeit befürchteten, wie sie das Internet versprach. Demgegenüber seien liberale Staaten mit gewollt liberalen bürgerlichen Freiheiten und Märkten durch diese neuen Möglichkeiten nicht bedroht, vielmehr würden bürgerliche Freiheiten – und damit zugleich der demokratische, liberale Staat – gestärkt.

Doch schon vor zwanzig Jahren zeichnete sich ab, dass der Fokus auf die Potenziale des Internets wirtschaftliche Akteure einschließen müsste – insbesondere transnationale Unternehmen –, deren Einfluss entweder durch die Produktion von Hardware, Software oder die Bereitstellung von Dienstleistungen nicht nur im Internet, sondern allgemein im Digitalisierungsprozess wuchs. Und nicht zuletzt fehlten diesen frühen Diskussionen über staatliche Souveränität und Digitalisierung die Erfahrungen, die man nach dem 11. September 2001 machte, nach der Finanzkrise der 2000er Jahre oder den Enthüllungen von Edward Snowden im Jahr 2013, die in dieser Frage wohl als einschneidendstes Ereignis gelten können. Dennoch deutete sich bereits damals an, dass Globalisierung und Digitalisierung herkömmliche Strukturen und zugehörige Denkformen herausfordern, die staatliche Souveränität im herkömmlichen Sinne grundsätzlich in Frage stellen:

> *„Neue transnationale Regime und Institutionen schaffen Systeme, die die Ansprüche bestimmter Akteure (Aktiengesellschaften und große multinationale Firmen) stärken und entsprechend die Position kleinerer Akteure und Staaten schwächen." (*Sassen 1998, S. 555)[6]

Erkennbar wird, dass nicht nur die Chiffre der digitalen Souveränität einer weiteren Differenzierung bedarf, sondern insbesondere in der Diskussion über nationale bzw. staatliche Souveränität ein genauerer Blick erforderlich ist. Anders formuliert: Die digitale Souveränität eines Individuums hat andere Voraussetzungen und ist anderen Bedrohungen ausgesetzt als etwa die digitale Souveränität eines Unternehmens oder eines Staates. Insbesondere mit Blick auf die digitale Souveränität liberaler Staaten ist es erforderlich, deren Verhältnis zu seinen Bürgern zu klären, die – als Gesamtheit – in Staaten dieses Typs der Souverän sind.

Vor diesem Hintergrund schlagen wir in diesem Beitrag eine Kombination einzelner Elemente und eine Ergänzung der oben skizzierten Modelle vor: Die Darstellung unterschiedlicher Sphären digitaler Souveränität als Kreise, im Sinne des Modells von Gueham, erscheint in besonderer Weise geeignet, um Konflikte in den entsprechenden Überschneidungsfeldern zu verorten, die Ausgangspunkt für Veränderungen sein können. Grundsätzlich erscheint auch der Aspekt einer Hierarchisierung wie bei Lepping und Palzkill geeignet, um ein asymmetrisches Machtverhältnis verschiedener Akteure abbilden zu können. Gegenüber dem Modell von Gueham erscheint es jedoch sinnvoll, einen eigenen Kreis für Akteure oberhalb der nationalen Ebene vorzusehen, wozu sowohl internationale Organisationen wie die Vereinten Nationen

[6] *Zitat im englischen Original: „New transnational regimes and institutions are creating systems that strengthen the claims of certain actors (corporations and large multinational legal firms) and correspondingly weaken the position of smaller players and states."*

(UN), die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) oder die Europäische Union (EU) als auch große, international agierende Unternehmen wie Google, Baidu, Facebook oder Alibaba zählen, die aufgrund ihrer faktischen Macht im Feld der Digitalisierung nur begrenzt mit normalen Unternehmen vergleichbar sind.

Trotz – oder gerade wegen – der prinzipiellen Grenzenlosigkeit der Digitalisierung ist der Staat in diesem von Macht durchsetzten Feld von Einflusssphären in besonderer Weise interessant. Durch Gesetzgebung, Fördermaßnahmen und als Akteur auf der internationalen Ebene kommt ihm eine zentrale, vielfach changierende Bedeutung

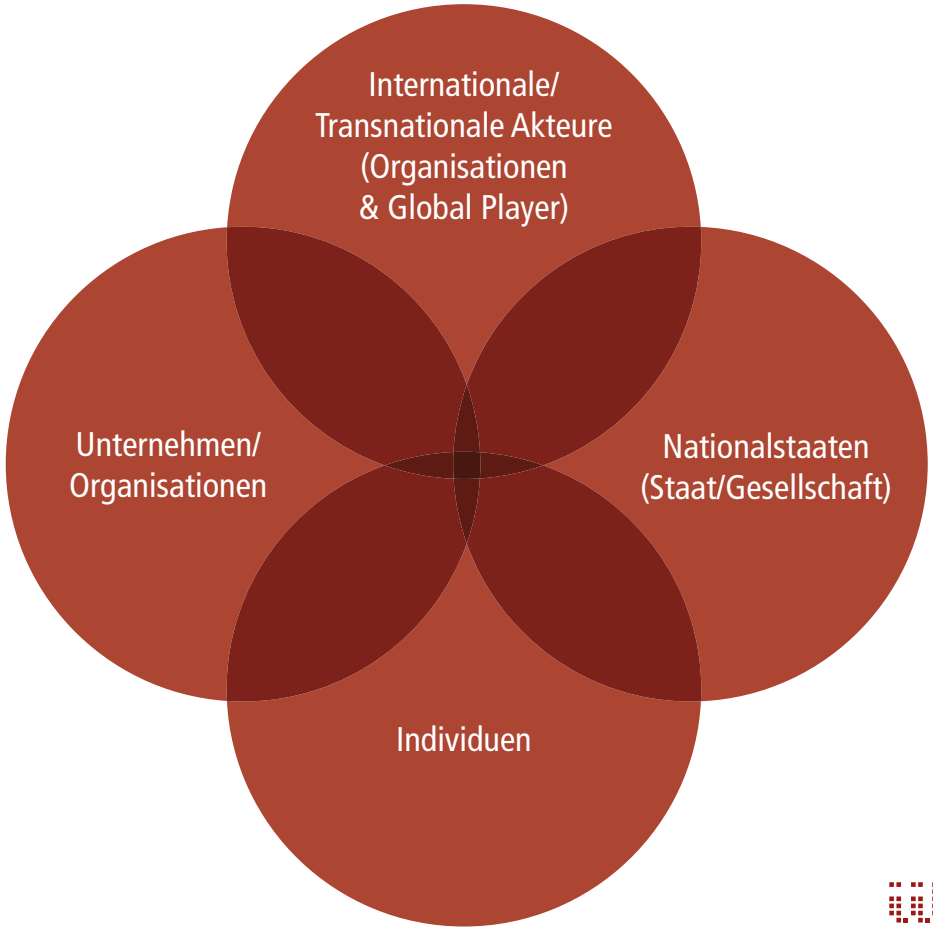

Abbildung 3.2.1: Sphären der digitalen Souveränität

zu: Seine Bürger, Unternehmen und andere Organisationen rufen ihn vielfach als Schutzmacht auf, er vertritt nationale Interessen gegenüber anderen Staaten, und seine Bürger können ihn zugleich als Bedrohung wahrnehmen. Stichworte sind hierzu die Abschaffung des Bargelds, ein verpflichtender elektronischer Pass oder etwa auch die Diskussion um den gläsernen Bürger.

Interessant sind daher in diesem Zusammenhang vor allem Aktivitäten, die sich auf die Sicherung einer staatlichen digitalen Souveränität richten, aber auch jene, aufgrund derer die digitale Souveränität der Bürger Beachtung bei staatlichen Maßnahmen findet. Viele dieser staatlichen Aktivitäten sind national ausgerichtet, aber die grundsätzlich grenzüberschreitende Digitalisierung erfordert auch internationales Engagement. Auf die rasanten technologischen Entwicklungen der letzten Jahre haben Staaten in der Mehrzahl der Fälle nur reagiert, nicht selten mit großer Verspätung. Die Frage ist, ob und wie sie wieder in eine aktivere und gestaltende Rolle finden können und dazu in der Lage sind, etwa Konflikte zwischen den verschiedenen digitalen Souveränitäten nachhaltig und zukunftsweisend zu moderieren.

Vor diesem Hintergrund führt die folgende Übersicht relevante Themen im Kontext staatlicher digitaler Souveränität auf (siehe Abbildung 3.2.2). Auch hier wird deutlich, dass die staatliche Perspektive auf digitale Souveränität keinesfalls isoliert ist, sondern enge Bezüge zu anderen gesellschaftlichen Bereichen wie etwa den Individuen, der Öffentlichkeit in ihrer Gesamtheit sowie der Wirtschaft hat.

Wie in der Übersicht deutlich wird, sind sowohl Chancen als auch Herausforderungen der Digitalisierung eng verbunden mit der Globalisierung, die wiederum ihrerseits durch die fortschreitende Digitalisierung stark vorangetrieben wurde.

Internationale Perspektiven auf digitale Souveränität

Der grenzüberschreitende Charakter des Internets und anderer digitaler Prozesse löst die Bedeutung nationalstaatlicher Grenzen zwar nicht auf, übersteigt in der Regel jedoch die Möglichkeiten einzelner Staaten, regulierend einzugreifen. Viele Konflikte um die digitale Souveränität von Staaten – die im internationalen Kontext stellvertretend für Bürger, Unternehmen und andere gesellschaftliche Akteure auftreten – sind nur auf internationaler Ebene zu verhandeln, denn dort sind auch die großen transnational agierenden Unternehmen aktiv. Internationale Organisationen wie beispielsweise die UN oder OECD bieten daher Foren, um Souveränitätskonflikte zu thematisieren und zu regulieren, die auf der Ebene der Nationalstaaten nicht oder nur eingeschränkt geregelt werden können.

Die Auseinandersetzungen der vergangenen Jahre in diesen Foren haben auch die unterschiedlichen Vorstellungen digitaler Souveränität der Länder sichtbar werden lassen, die in nationalen Traditionen begründet und mit politischen Agenden der

Chancen für staatliche digitale Souveränität

Chancen zur **Partizipation und Artikulation im Sinne der zu stützenden Meinungsfreiheit und Demokratisierung**: „Digitaler Space für alle"

Sicherheit: neue, digital gestützte Infrastrukturen für die (militärische) nationale und internationale Sicherheit (z. B. NATO)

Erweiterte Möglichkeiten der staatlichen **Einflussnahme** durch einen breiten (und kostengünstigen) medialen Zugang über digitale Medien (Internet/soziale Medien):
- vereinfachte Information der Bürger
- verbesserte Möglichkeiten für breite Bildung etc.

Pluralisierung politischer, transnationaler Akteure
- z. B. in Form finanzstarker IT-Unternehmen, Digitalisierung der Finanzmärkte (parallel zu allgemeinen Globalisierungstendenzen)
- Positiver Beitrag zur ökonomischen Entwicklung

Staatliche Regulierung der **Wirtschaft** zur Sicherung des **nationalen Wohlstands**:
- Chancen für Handel und Produktion durch Digitalisierung
- Innovationschancen, Serviceverbesserungen
- neue Märkte und Arbeitsplätze

Verbesserte **Kommunikationsmöglichkeiten**:
- Grenzenlosigkeit
- Vermehrte Transparenz und Artikulations- bzw. Partizipationsmöglichkeiten durch die Bevölkerung
- verbesserte Kooperationsmöglichkeiten (z. B. in Wissenschaft und Innovation, Bildung etc.)
- vermehrte Möglichkeiten für Bürgerinitiativen/Engagement (NGOs)
- Möglichkeiten der Selbstregulierung der transnationalen Cyber-Community (Stichwort: self-governance)

Recht:
- eine stärkere Rechtssicherheit und -sichtbarkeit auf nationalenr und internationaler Ebene (z. B. WTO)
- verbesserte Kenntnis der Gesetze und Regularien

Abbildung 3.2.2: Chancen und Herausforderungen für staatliche digitale Souveränität

Herausforderungen für staatliche digitale Souveränität

Gefahr des **Missbrauchs** und der zunehmenden Dominanz der **Kommerzialisierung**

Bedrohung staatlicher Souveränität durch digitale Technologien der staatlichen Sicherheit über das Internet:

- Eingriff in national relevante IT-Systeme, Missbrauch von Daten (Big Data) etc.

Bedrohung staatlicher Souveränität durch

- potenzielle Fragmentierung und Reorganisation in andere institutionelle/kulturelle Einheiten mit Akteuren, die mit dem staatlichen „Souverän" im Wettbewerb oder gar Konflikt stehen (z. B. human rights organisations in China/Russland)
- unkontrollierbare Meinungsbeeinflussung durch in- und ausländische politische Akteure (alternative Fakten; Social Bots)

- Beeinflussung nationaler und internationaler Politik in Bezug auf Gesetzgebungen zugunsten der digitalbasierten Wirtschaftsakteure (Lobbyismus)
- Risiken durch liberalisierte und digital gestützte Finanzgeschäfte (z. B. die internationale Finanzkrise nach 2008, Cole 2016)

- Bedrohung der nationalen Regulierbarkeit ökonomischer Aktivitäten (einhergehend mit Globalisierungstendenzen)
- Nationaler Wohlstand ist gefährdet, wenn in Fragen der Digitalisierung im globalen Wettbewerb der Anschluss verpasst wird und Marktchancen ungenutzt bleiben
- Verpasste Personalqualifizierung führt zu erhöhter Arbeitslosigkeit

- befürchteter Verlust der nationalen/kulturellen Identität
- Gefährdung bürgerlicher/moralischer oder auch ideologischer Werte im nicht-staatlichen Sinne durch offenen Internetzugang für antagonistische (politische, religiöse etc.) Akteure (z. B. rechte Äußerungen in Deutschland; Menschenrechtsbewegungen in China)
- rasante Entwicklungen dank beschleunigter Cyber-Information oft ohne Vorbereitung für nachhaltige Implementierung (Kontext: reaktiver statt agiler Staat, z. B. nach der Jasmin-Revolution keine nachhaltige Verbesserung für Akteure)
- Selbstorganisation kann aus Staatssicht auch subversive Formen annehmen

- transnationale Verbindungen in Kommunikation und Handel über das Internet bedürfen einer wirksamen internationalen Regulierung
- Probleme des grenzüberschreitenden Handels, insbesondere in Bezug auf Rechts- und Steuerfragen (bedarf (inter-)nationaler Regulierung)
- Kollision unterschiedlicher Gesetzgebungen z. B. in Fragen der Meinungsfreiheit, beim Datenschutz, bei Intellectual Property Rights

Nationalstaaten verknüpft sind. Die Initiativen der staatlichen Akteure sind hier oft geleitet von der Vorstellung, dass im Internet erlaubt sein soll, was auch sonst innerhalb des eigenen Territoriums zulässig ist. Eine solche Übertragung von Regeln aus territorial eingegrenzten Staaten in den Cyberspace[7] ist jedoch nicht oder nur eingeschränkt realisierbar, wie die hier vorgestellten Länderskizzen zeigen.

Internationale Organisationen

Der grenzüberschreitende Charakter des Internets und anderer digitaler Prozesse – wie zum Beispiel die alltägliche Nutzung von Dienstleistungen transnational agierender Unternehmen wie Facebook, Google, Baidu, Alibaba oder eBay – machen deutlich, dass Regulierungen und Vereinbarungen auf überstaatlicher Ebene zu treffen sind. Nachfolgend werden daher schlaglichtartig einige Themen skizziert, die zuletzt auf den Agenden der internationalen Organisationen beziehungsweise Staatenbünde und Staatenverbünde standen. Der Blick auf die Aktivitäten dieser internationalen Organisationen erscheint auch unter dem Gesichtspunkt relevant, dass ihre Handlungsfelder durch Initiativen von nationaler Ebene informiert werden und sie zugleich Stichwortgeber für Aktivitäten auf nationaler Ebene sein können.

Vereinte Nationen United Nations (UN)

Die internationale Staatengemeinschaft hat sich mit Blick auf das Thema der digitalen Souveränität zuletzt mit dem Recht auf Privatheit im Digitalzeitalter und dem Verbraucherschutz befasst (vgl. UN 2016a; UN 2016b). Adressiert werden damit Themen, die sich vor allem dem Schutz der digitalen Souveränität von Individuen widmen. Den von den UN hierzu gefassten Resolutionen beziehungsweise veröffentlichten Richtlinien gingen Beratungsgespräche mit anderen gesellschaftlichen Akteuren, wie beispielsweise Amnesty International, voraus. Diese Dokumente erkennen nicht nur die positiven Potenziale der technologischen Entwicklung, sondern verweisen auch darauf, dass Regierungen mit der Verbreitung von Informationstechnologien neue Möglichkeiten bekommen, Unternehmen und Einzelpersonen zu überwachen oder Daten über sie zu sammeln.

Insbesondere das Recht auf Privatheit im Digitalzeitalter hat die Organisation über mehrere Jahre hinweg intensiv beschäftigt, und sie hat die ursprüngliche Resolution mehrfach aktualisiert. War die erste Fassung aus dem Jahr 2013 zum Thema „Privacy in the Digital Age" noch primär eine Reaktion auf die Enthüllungen Edward Snowdens über staatliche Überwachungsmaßnahmen, so appelliert die Version aus dem

[7] *„Als Cyberspace wird jede nicht real existierende Welt bezeichnet, die nur mithilfe eines Computers virtuell betreten werden kann." (Lackes und Siepermann 2017)*

Jahr 2016 nicht nur an die Mitgliedstaaten, sondern auch an Unternehmen. Diese werden unter anderem aufgerufen, die Menschenrechte – insbesondere das Recht auf Privatheit – zu achten, Nutzer über das Erheben, die Verwendung und Aufbewahrung von Daten zu informieren und sich für die Entwicklung sicherer Kommunikation einzusetzen.

In den Richtlinien zum Verbraucherschutz (Guidelines for Consumer Protection) gehen die UN in einem kurzen Abschnitt separat auf den elektronischen Handel ein. An erster Stelle rufen sie die Mitgliedsstaaten dazu auf, das Vertrauen der Verbraucher in den elektronischen Handel zu verbessern, wofür unter anderem effektive und transparente Maßnahmen zum Verbraucherschutz für den Bereich E-Commerce zu entwickeln seien. Abschließend wird auf die Richtlinien der OECD für den Verbraucherschutz im elektronischen Handel verwiesen.

Zur Frage der digitalen Souveränität lassen sich die beiden Initiativen der UN – der Schutz der Privatheit gegenüber Ausspähung durch Staaten und der Schutz individueller Rechte in der Sphäre der Wirtschaft – als Parteinahme für die Individuen lesen, deren individuelle digitale Souveränität bedroht scheint. Dass die UN diese Frage thematisiert haben, ist jedoch zunächst wohl nur als ein Indikator dafür anzusehen, dass die internationale Bedeutung des Themas inzwischen erkannt wird.

Organisation für wirtschaftliche Zusammenarbeit und Entwicklung Organisation for Economic Co-operation and Development (OECD)

Auch die OECD hat sich in den vergangenen Jahren unter wirtschaftlichen Gesichtspunkten mit dem Thema Digitalisierung auseinandergesetzt. Die Ergebnisse skizziert der Bericht „Kernthemen der Digitalen Transformation in den G20" (engl. „Key Issues for Digital Transformation in the G20") (OECD 2017), der im Rahmen der deutschen Präsidentschaft für ein Treffen der G20 im Januar 2017 vorbereitet wurde. Die OECD konstatiert in diesem Bericht, dass mit der technologischen Entwicklung und den sinkenden Kosten für die IT-Infrastruktur soziale und ökonomische Aktivitäten zunehmend in das Internet verlagert werden. Ebenso wie die UN sieht die OECD neben positiven Entwicklungen auch Gefahren und weist unter anderem auf den nachhaltigen Einfluss auf Produktivität, Beschäftigung und Gesundheit hin, der von disruptiv wirkenden digitalen Technologien ausgehen kann, indem die bestehenden Produkte und Dienstleistungen vollständig verdrängt werden. Hervorgehoben wird auch, dass mit solchen technologischen Entwicklungen gesellschaftliche Verwerfungen einhergehen können, wie beispielsweise der Verlust von Arbeitsplätzen in spezifischen Wirtschaftssektoren oder die Vertiefung bestehender sozialer Ungleichheiten.

Neben einer Bestandsaufnahme des Standes der Digitalisierung in den G20-Staaten umreißt der Bericht eine Vielzahl an Themen. Hierzu zählen beispielsweise der

Zugang zu digitalen Diensten, digitale Infrastrukturen, die Finanzierung digitaler Infrastrukturen, die Entwicklung von Standards und die Regulation des IT-Sektors, die digitale Sicherheit, der Verbraucherschutz in der digitalen Ära sowie rechtliche Rahmenbedingungen. Viele dieser Aspekte lassen sich unter ihrer direkten oder mittelbaren Bedeutung für die digitale Souveränität betrachten. Im Fokus stehen an dieser Stelle allerdings nur zwei Bereiche: die digitale Sicherheit sowie der Verbraucherschutz.

Mit digitaler Sicherheit werden zuallererst Gefahren für Unternehmen und Individuen beschrieben (OECD 2017, S. 92ff). Während die digitale Sicherheit lange Zeit vor allem als ein technisches Problem behandelt wurde, sieht die OECD in den letzten Jahren einen Trend bei Regierungen und anderen Akteuren, diese als ein facettenreiches Handlungsfeld für die Nationalstaaten zu begreifen. Neben der technologischen Dimension zählen hierzu der soziale und ökonomische Wohlstand, das Thema Cyber-Kriminalität sowie die nationale und internationale Sicherheit. Als primäre Ziele für die nationale digitale Sicherheit werden unter anderem Maßnahmen aufgezählt, die dazu befähigen sollen, ihre digitalen Risiken managen zu können. Eine weitere Facette ist die Förderung von Beispielen guter Praxis im Bereich des Datenschutzes. Hingewiesen wird auch darauf, dass Organisationen, die mit dem Schutz der Daten von Individuen beauftragt sind, möglicherweise unterschiedliche Interessen haben. Die Risiken eines Datendiebstahls und die damit verbundenen Kosten auf der einen Seite sowie die Kosten für die Implementierung von Sicherheitsmaßnahmen zum Schutz personenbezogener Daten auf der anderen Seite abzuwägen, erscheint primär als ein ökonomisch relevanter Aspekt. Das Thema Datenschutz verhandelt der Bericht im Unterschied zu Stellungnahmen etwa der UN nicht als Realisierung des individuellen Rechts auf Selbstbestimmung über die eigenen Daten, sondern als einen (Kosten-)Faktor unter vielen, der das Verhältnis zwischen Unternehmen und Kunden beeinflusst.

Das Thema Verbraucherschutz im Kontext der Digitalisierung verknüpfen die Dokumente der OECD zentral mit dem Thema Vertrauen. Im Mittelpunkt steht hier vor allem die Rolle digitaler Plattformen – beispielsweise Netflix, Facebook, Twitter, Alibaba, eBay, Snapdeal und nicht zuletzt Google und Baidu. Sie erlauben den Zugang zur digitalen Welt, strukturieren die alltäglichen Aktivitäten der Individuen und werden deshalb auch als das Herz des digitalen Ökosystems beschrieben. Außerdem hätten sie eine intermediäre Funktion, seien Marktmacher und gewönnen durch ihr Potenzial zur Steuerung von Aufmerksamkeit und auch durch die Möglichkeit des Sammelns von Daten eine besondere Macht – zunächst über individuelle Nutzer, aber letztlich auch darüber hinaus.

Digitale Souveränität taucht in diesem Dokument der OECD als Begriff nicht auf. Und doch scheint das Thema an vielen Stellen durch. Insbesondere betont es die Gefahren

durch Cyberkriminalität sowohl für Unternehmen als auch für Personen. Die Sicherung von Daten – unter anderem personenbezogener Daten – sind jedoch primär unter dem Gesichtspunkt der Abwägung von Kosten ein Thema. Solange die Aufwendungen für erforderliche Sicherheitsmaßnahmen die finanziellen und sozialen Kosten im Schadensfall nicht übersteigen, ist die digitale Sicherheit ökonomisch nicht begründbar. Das Thema Vertrauen positioniert die Agenda unter der Überschrift des Verbraucherschutzes als zentralen Punkt, aber eher funktional mit Blick auf die Teilnahme am Markt, weniger im Sinne eines keiner weiteren Begründung bedürfenden Rechts.

Europäische Union European Union (EU)

Die Europäische Union als regionaler Staatenverbund erscheint mit Blick auf das Thema der digitalen Souveränität in den vergangenen Jahren eher in der Rolle einer Getriebenen, die in vielfacher Weise vor allem gegenüber den USA im Hintertreffen ist. Symbolisch für den Konflikt zwischen den unterschiedlichen Vorstellungen von digitaler Souveränität der EU und der USA stehen hier die Auseinandersetzung um die Snowden-Enthüllungen und die Asymmetrie beim Umgang mit den großen, transnational agierenden Unternehmen auf dem Feld der Digitalisierung.

Rechtlich und politisch erscheinen die Enthüllungen von Edward Snowden für die EU als eine Zäsur, die die Bedrohung ihrer digitalen Souveränität – stellvertretend für die ihrer Mitgliedsstaaten und nicht zuletzt auch ihrer Bürger – versinnbildlicht. In diese Zeit fiel auch die Entscheidung des Gerichtshofs der Europäischen Union (EuGH) von 2015, das unter dem Namen „Safe Harbor" bekannte Abkommen für unwirksam zu erklären. Diese Vereinbarung hatte die Übermittlung personenbezogener Daten von europäischen Ländern in die USA geregelt. Mit der Entscheidung des EuGH drohte tausenden Unternehmen, die mehr als 15 Jahre lang auf dieser Grundlage gearbeitet hatten, die Arbeitsgrundlage entzogen zu werden. Nur während einer Übergangsfrist war eine Fortführung der Aktivitäten erlaubt, und es bedurfte des unter viel Zeitdruck entwickelten Nachfolgeabkommens „Privacy Shield", um Unternehmen unter veränderten Bedingungen die Fortsetzung ihrer wirtschaftlichen Initiativen zu ermöglichen. Hier war es also der europäische Gerichtshof, der zum Schutz der fundamentalen Rechte der europäischen Bürger einschritt und eine Neuverhandlung des Status quo der digitalen Souveränität einforderte.

Stellvertretend für die wirtschaftliche Distanz zwischen der EU und den USA stehen die großen internationalen Player des Internets beziehungsweise der Digitalisierung wie Google, Apple, Facebook oder Amazon, die ihren Hauptsitz allesamt in den USA haben. Die Liste der für die Digitalisierung strukturell relevanten amerikanischen Firmen, die Hardware produzieren oder digitale Dienstleistungen bereitstellen, ließe sich fortsetzen. Die Verbindung der Snowden-Enthüllungen mit den Möglichkeiten der Hardware-Hersteller, sogenannte Hintertüren in Hardware einzubauen, die

Sicherheitsdienste, aber auch von anderen kriminellen Akteuren genutzt werden können – die damit ab dem Tag des Verkaufs des Geräts verwundbar für Angriffe sind – machte die Abhängigkeit der EU von den USA überdeutlich.

Die relative Rückständigkeit mit Blick auf die wirtschaftliche Dimension der Digitalisierung (vgl. FZI 2017) war schon länger ein Thema für die Europäische Union. Hervorzuheben sind hier insbesondere die Digitale Agenda für Europa von 2010 (Europäische Kommission 2010), die Cyber-Sicherheitsstrategie der Europäischen Union von 2013 (Europäische Kommission 2013) und die Strategie für einen digitalen Binnenmarkt in Europa („Digital Single Market Strategy") von 2015 (Europäische Kommission 2015). Im Vordergrund der Ziele und an erster Stelle der Aktionsbereiche der Digitalen Agenda stand von Anfang an die Schaffung eines neuen, digitalen Binnenmarktes. Insbesondere die Fragmentierung des europäischen Marktes und der übergroße Anteil an Käufen im außereuropäischen Ausland – insbesondere in den USA – wurde und wird als Problem und Herausforderung für die Wiedererlangung einer (wirtschaftlichen) digitalen Souveränität angesehen.

Zahlen von 2015 weisen einen Anteil US-basierter Online-Dienstleistungen von 54 Prozent aus, gefolgt von 42 Prozent nationaler Dienstleistungen und einem demgegenüber verschwindend geringen Anteil von 4 Prozent für EU-grenzüberschreitende Online-Services (Europäische Kommission 2015). Neben eher auf die formalen oder technischen Infrastrukturen gerichteten Maßnahmen, die als Voraussetzung für die Teilhabe am Digitalen gelten können, sieht sich die EU vor allem mit der Aufgabe konfrontiert, das Vertrauen in das Internet bzw. in digitale Dienstleistungen wiederherzustellen, das nicht zuletzt durch die Snowden-Enthüllungen, aber auch durch Berichte über Datenmissbrauch stark eingebüßt hat. Eine zwischen 2013 und 2014 von dem Telekommunikationsunternehmen Orange in fünf europäischen Ländern durchgeführte Studie zur Zukunft des digitalen Vertrauens kam zu dem Ergebnis, dass 78 Prozent der Befragten der Ansicht waren, dass es schwer sei, Unternehmen beim Umgang mit persönlichen Daten zu trauen (vgl. Orange 2014).

Ein wegweisender Schritt in Richtung der Wiedererlangung des Vertrauens der Bürger bzw. Kunden kann die 2016 verabschiedete Datenschutz-Grundverordnung (DSGVO) der EU sein. In ihr wird unter anderem die Einbeziehung von Technologielösungen für Datenschutz im Rahmen der Entwicklungsphase von IT-Anwendungen gefördert. Im Sinne des Art. 25 Abs. 1, 2 (EU) 2016/679 geregelten „Privacy by Design" und „Privacy by Default" sind IT-Systeme so zu gestalten, dass sie von Anbeginn Datenschutzgrundsätze effektiv realisieren (vgl. FZI 2017).

Zudem funktioniert die EU-Datenschutz-Grundverordnung nun auch bei Verstößen durch Akteure, die keine Niederlassung in der EU haben, jedoch innerhalb der EU Waren oder Dienstleistungen anbieten oder das Verhalten von Personen beobachten. Hier ist also auf EU-Ebene ein gemeinsamer Lösungsansatz für digitale Heraus-

forderungen auf den Weg gebracht worden, der auch die mächtigen auswärtigen Akteure der Digitalwirtschaft insbesondere in den USA aufhorchen lässt. Doch obwohl die DSGVO keiner weiteren Umsetzung auf nationaler Ebene bedarf, enthält sie doch in mehr als 60 Öffnungsklauseln einigen Spielraum für nationale Regelungen durch Mitgliedstaaten. Hier ist nur zu hoffen, dass die Grundidee der EU-Datenschutz-Grundverordnung durch ergänzende nationale Detailarbeit in der EU eher noch klarer konturiert wird.

Länderprofile

China

George Orwells fiktionaler Big Brother im Roman „1984" findet inzwischen im liberalen Westen wieder erhöhte Aufmerksamkeit. Die erneute Beachtung dieser klassischen Dystopie im Westen ist sicher eng verbunden mit Befürchtungen in der Bevölkerung bezüglich negativer Folgen einer digital gestützten allumfassenden staatlichen Kontrolle des Bürgers. Im nach wie vor offiziell sozialistischen China sind der omnipräsente Staat und die allwissende Partei seit fast 70 Jahren gewohnte Realität. Der chinesische Einparteienstaat hat die Mechanismen zur Kontrolle seiner Bürger und zum Schutz seiner Souveränität im Zuge der technologischen Entwicklung modernisiert und mit den der Digitalisierung innewohnenden gegenläufigen Tendenzen einer allumfassenden Kontrolle recht gut Schritt gehalten. Ein Großteil der chinesischen Bevölkerung akzeptiert dies jedoch oder hat sich zumindest daran gewöhnt. Regierung und Staatssystem legitimieren sich auch heute nicht zunächst aus den gebotenen Freiheiten, sondern aus dem Schutz seiner Einheit, seiner Grenzen und – im postmaoistischen Zeitalter – aus dem kontinuierlich steigenden Wohlstand. Wenn es um den Schutz persönlicher Daten geht, scheint man in China generell weniger sensibel eingestellt zu sein als in Deutschland (vgl. Huawei 2016).

China verfügt bis heute über ein erstaunlich gut funktionierendes Propagandasystem, das über die diversen staatlichen Medien das aktuell gültige Gedankengut an die Bevölkerung vermittelt und einen allzu umfassenden Widerstand mit einem effektiven Zensursystem bisher grundsätzlich in Zaum halten konnte. Das chinesische System einer eingeschränkten Meinungsfreiheit hat jedoch die Herausforderungen der Digitalisierung erkannt und versucht diese durch eine Expansion seines Kontrollapparates und mit Hilfe der Digitalisierungstechnologien abzuwehren. Im Jahr 2014 wurde Chinas sogenannte „Great Firewall" um die „Cyberspace Administration of China" (CAC) (guojia lianwang xinxi bangongshi) erweitert. Diese Institution der chinesischen Zentralregierung kümmert sich auch um Fragen der ideologischen Propaganda sowie die Zensur und Ermittlung unangepasster Internet-User. In dem in urbanen Zentren mittlerweile technologisch fortgeschrittenen Land ist es ein Katz- und

Mausspiel zwischen nach Nischen spähenden Nutzern des Internets und dem kontrollierenden Staat.

Chinas Beispiel macht also zunächst deutlich, dass der Schutz staatlicher digitaler Souveränität in manchen Staatsystemen auch nach innen gerichtet sein kann. Doch natürlich sind ausländische Einflüsse auf diese Weise ebenfalls reduzierbar oder zumindest besser kontrollierbar. Auch ausländische Internetseiten, auf denen Medien negative Berichterstattung über China liefern, wie etwa die New York Times zu Chinas Verwicklung in den Panama-Paper-Skandal (vgl. Forsythe und Ramzy 2016), werden zum Ziel von Attacken und je nach Anlass für kürzere oder längere Zeit gesperrt. Das harte Vorgehen wird in China vereinfacht durch die staatlicherseits leicht zugänglichen Suchmaschinen und sozialen Medien inländischer Bauart (Baidu, WeChat, Weibo etc.), nachdem man sich in der Volksrepublik schon vor Jahren der US-amerikanischen Originale (Google, Facebook, Twitter etc.) entledigt hat (z. B. Gracie 2014).

Dies leitet über zu der anderen, ebenfalls bemerkenswerten Seite der Situation in China: Die staatlich über Subventionen und Regularien intensiv geförderte IT-Branche des Landes ist nicht nur Mittel zur politisch-ideologischen Wahrung nationaler Integrität (vgl. Cai und Kwong 2016). China hat Informationstechnologien bereits um die Jahrtausendwende innerhalb der allgemeinen Wirtschaftsstrategien hoch auf die nationale Entwicklungsagenda gesetzt (vgl. Christmann-Budian 2012), denn diese Entwicklung passt zu vielen anderen nationalen Zielen: Sie unterstützt zunächst seine Überholstrategie („leap frog strategy") im Wettbewerb mit den etablierten Industrienationen. Die Digitalisierung ist auch bei der Umstellung auf eine nachhaltige, eigene Innovationen (zizhu chuangxin) fördernde Wirtschaftspolitik und Chinas Aufstieg von der verlängerten Werkbank der Industrieländer eine große Hilfe (Medium Long Term Plan 2005, 12th Five Year Plan for the Strategic Emerging Industries; vgl. Tagscherer und Christmann-Budian 2013). Die Digitalisierungstechnologien können in diesem Zusammenhang zu einer eigenständigen profitablen Ausnutzung des riesigen Binnenmarktes beitragen. Den inländischen Markt kennt man in China im Übrigen auch in Sachen IT besser als die ausländische Konkurrenz – deren Zutritt man mit staatlichen Hebeln zudem erschweren kann. Omnipräsentes Beispiel und mittlerweile einer der größten weltweiten Player ist das Unternehmen Alibaba. Alibaba betreibt de facto, entgegen weit verbreiteter Vorstellungen, nicht nur E-Commerce, sondern ist vielmehr ein komplexes Konglomerat, das von der ursprünglichen Handelsplattform in diversen Variationen über Online-Finanztransaktionen (Alipay) bis hin zu Logistik (cainiao.com) eine große Bandbreite von Produkten und Dienstleistungen abdeckt (vgl. Fritz 2017).

Um die skizzierte Doppelstrategie von Zensur und Protektion der lokalen Internetindustrie gegenüber der internationalen Kritik zu legitimieren, ruft Chinas Regierung unter Präsident Xi Jinping in der jüngeren Zeit, z. B. 2016 im Rahmen der großzügig

durch China gehosteten World Internet Conference, vermehrt zum Respekt nationaler digitaler Souveränität auf (vgl. Cai und Kwong 2016).

China ist mit dieser Linie staatlicher Kontrolle im Cyber-Space nicht allein: Andere, ähnlich ausgerichtete Staatssysteme wie Russland oder Saudi Arabien teilen derartige Vorstellungen der Souveränität über die eigene (nationale) Netzhoheit (vgl. Margolin 2016). Einmischung von außen lehnen sie konzertiert ab und postulieren Zensur als innere Angelegenheit, selbst wenn dies die ausländische Berichterstattung betrifft.

> *„[...] der Begriff ‚Internet-Souveränität' oder wangluo zhuquan (网络 主权) verkörpert die Behauptung der Kommunistischen Partei Chinas, dass der traditionelle Begriff der nationalen Souveränität auf den Cyberspace anwendbar sei, für den die Befürworter der ‚Netzneutralität' behaupten, dieser müsste ohne Grenzen und frei von staatlichen Eingriffen bleiben. Nach dem Prinzip der ‚Internet-Souveränität' behält sich China vor, den Informationsfluss im Internet innerhalb seiner Grenzen und über seine Grenzen hinaus zu kontrollieren, selbst mit Mitteln, die die Informationsrechte von Einzelpersonen außerhalb der physischen Grenzen Chinas verletzen könnten. Die Weiterentwicklung der ‚Internet-Souveränität' wird häufig mit dem verbunden, was man die Fragmentierung oder die Balkanisierung des Cyberspace nennt."* (CMP 2015)[8]

Ausländische Akteure haben sich in China an die dortigen Regeln zur Tabuisierung oder umgekehrt einer erzwungenen Offenlegung von Informationen zu halten. Gegen Kritik an dieser Haltung wappnet sich China, indem es mit anderen autoritären Regimen Allianzen schmiedet. Ausländische Unternehmen betrachten die Verschärfung entsprechender Kontrollen mit Sorge, denn sie könnten zur Offenlegung ihrer Geschäftsdaten und zu einem weiteren unfreiwilligen Know-how-Transfer gezwungen werden (vgl. Alsabah 2017). Als Grundlage baut China hierzu die nationale Gesetzgebung beispielsweise mit dem „Cyber Security Law" (zhonghua renmin gongheguo wangluo anquan fa NPC 2015) von 2015 aus (vgl. Fulbright 2015).

---

[8] *Zitat im englischen Original: „[…] the term ‚Internet sovereignty', or wangluo zhuquan (网络主权), encapsulates the Chinese Communist Party's assertion that the traditional notion of national sovereignty is applicable to cyberspace, which proponents of ‚net neutrality' would argue must be kept borderless and free of government interference. Under the principle of ‚Internet sovereignty', China reserves the right to control the flow of information on the Internet within its borders and across its borders, even if in ways that might infringe upon the information rights of individuals outside of China's physical borders. The advancement of ‚Internet sovereignty' is often associated with what some have called the fragmentation, or balkanisation, of cyberspace."*

Nachdem der Staat digitale Spuren und Profile im Netz bereits in der jüngeren Vergangenheit immer umfassender nachvollziehen konnte – zum Beispiel über einen ID-Card-Registrierungszwang in den sozialen Medien –, will er das Konzept des gläsernen Bürgers wie auch des gläsernen Unternehmens nunmehr „vervollkommnen". Alibaba beispielsweise häuft mit seinem „Sesame Credit" wertvolle Big-Data-Vorräte zum privaten Finanz- und Konsumverhalten, aber auch über andere soziale Verhaltensweisen im weitesten Sinne an, mit denen künftig auch, aber nicht nur über Kreditanträge von Bürgern entschieden werden kann (vgl. Hatton 2015). Es gibt Pilotprojekte wie das der Stadt Rongcheng in der Shandong-Provinz, wo für ein Bürger-Rating jegliche Aktivitäten seiner Einwohner erfasst werden. Hier fließen auch etwa kritische Äußerungen in den sozialen Medien mit ein. Diese Ratings sind schließlich die Grundlage für ein Auf- oder Abstufen des Bürger-Status und damit verbundener Privilegien oder Sanktionen. Strafen bestehen beispielsweise darin, keine Flugtickets zu bekommen oder nicht ausreisen zu dürfen (vgl. Strittmatter 2017).

Auch für in- und ausländische Unternehmen vergrößert sich der Grund zur Sorge: alles wird registriert und gespeichert. Bei negativen Informationen können Unternehmen von staatlichen Ausschreibungen ausgeschlossen bleiben, oder dringend notwendige Kredite sowie Zulassungen werden abgelehnt. Was jeweils positiv oder negativ ist, entscheiden die Autoritäten in den zuständigen Institutionen – nachvollziehbar muss das nicht sein.

China will bei dieser pragmatischen Nutzung von Big Data zur gesamtgesellschaftlichen Kontrolle weltweit Nummer eins sein. Sowohl als technisches Vorbild wie auch als Vorbild für Geschäftsmodelle. „Die Ersten. Das wäre eine Warnung für alle Demokratien, in denen Konzerne und Behörden ihre eigenen Big-Data-Träume träumen. Und könnte anderen gerade deshalb verlockend erscheinen (…)." (Strittmatter 2017, S. 13)[9]

Dass trotz all dieser Entwicklungen die internationalen Vorwürfe der Cyber-Spionage gegenüber China anhalten, ist nur auf den ersten Blick ein Widerspruch: Denn Chinas Position ist keineswegs im Sinne von „gleiches Recht für alle" zu verstehen, sondern eher als sehr nationalistisch-protektionistische Haltung ausschließlich im Interesse des eigenen Landes.

In Chinas Adaption des deutschen Industrie-4.0-Konzeptes in der Staatsstrategie „Made in China 2025" (2015) offenbaren sich auch die Herausforderungen für seine digitale Souveränität (wangluo zhuquan). Denn trotz aller technologischen Fortschritte basiert Chinas durchaus effektives Innovationssystem weiterhin stark auf Adaption, Anpassung und absorbierender Weiterentwicklung von (Informations-

[9] *Im Original steht fehlerhaft „erschienen".*

und Kommunikations-)Technologien ausländischer Innovationen, eigener erfolgreicher frugaler Innovation beziehungsweise auf einem Technologie-Transfer von und Innovationskooperation mit ausländischen Partnern (vgl. Bound et al. 2013; Wübbeke et al. 2016). Es fehlt bis heute der große Wurf im Sinne eines Innovators wie etwa Apple sowie die Unabhängigkeit von ausländischen Partnern und Konkurrenten. Dies führt jedoch zu der allgemeinen Frage, ob diese angestrebte, weitestgehende Unabhängigkeit von Partnern auch im Rahmen von Digitalisierungsstrategien und zugehörigem Souveränitätsstreben unrealistisch ist, wenn man zugleich auf einem wissenschaftlich-technologisch höchstem Niveau bleiben möchte.

Singapur

Singapur, ein weiterer hochdigitalisierter nationaler Akteur in Asien, geht offenbar andere Wege als die Volksrepublik China. Dabei ist der kleine Stadtstaat trotz der ungleich anderen Größenordnung in vielerlei Hinsicht durchaus vergleichbar mit dem Reich der Mitte. Das betrifft zum Beispiel die bis heute aktive staatliche Zensur. Auch das Internet wird kontrolliert, die hierfür zuständige Behörde in Singapur heißt „Infocommunications Media Development Authority" (IMDA)[10]. Der Vergleich mit China bietet sich auch deshalb an, weil Singapur für das wirtschaftlich und technologisch ambitionierte Reform-China in den zurückliegenden Jahrzehnten ein bedeutendes Vorbild war (vgl. Christmann-Budian 2012). Die konfuzianistisch geprägte Kultur Singapurs sowie seine autoritative Regierungsweise haben in Kombination mit seinem ökonomischen Aufstieg unter Präsident Lee Kuan Yew (1959 bis 1990) in vielerlei Hinsicht die Blaupause für das nach einem Entwicklungsvorbild suchende postmaoistische China abgegeben.

Trotz der weiterhin hohen staatlichen Kontrolle hat jedoch zumindest die Wirtschaft Singapurs den Ruf, weltweit eine der am wenigsten regulierten zu sein. Diese ökonomische Offenheit geht einher mit der umfassenden Integration digitaler Technologien in Wirtschaft und Gesellschaft, die durch den „Network-readiness-Indikator" des World Economic Forums bestätigt wird (vgl. Graham 2016).

Die daraus erwachsende Notwendigkeit, sich auf Informationstechnologien verlassen zu müssen, mache das Land jedoch zugleich in hohem Maße verletzbar, heißt es in der Ende 2016 veröffentlichten Cybersecurity-Strategie des Landes (vgl. CSA 2016). Angeführt von der „Cybersecurity Agency" (CSA) sollen gemeinsam mit der

[10] *Die IMDA ist eine Fusion der früheren „Media Development Authority" (MDA), der zentralen Medienzensurbehörde Singapurs, sowie der „Infocomm Development Authority" (IDA), die für die Planung und Entwicklung des Informations- und Kommunikationstechnologie-Sektors auf staatlicher Ebene verantwortlich war.*

Industrie und der Bevölkerung Maßnahmen zum Schutz der digitalen Souveränität von Singapur realisiert werden.

Die dabei verfolgte Strategie basiert vor allem auf vier zentralen Säulen: Aufbau einer belastbaren Infrastruktur, Schaffung eines sicheren Cyberspace, Entwicklung eines dynamischen Ökosystems für digitale Sicherheit und Stärkung von Partnerschaften.

Gerade die vierte Säule, die Relevanz von internationalen Partnerschaften bei der Stärkung der nationalen Cybersecurity, meint nicht wie im Falle China die Übereinkunft, man möge sich jeweils nicht in die Angelegenheiten des anderen nationalen Partners einmischen. Vielmehr scheint man in Singapur davon überzeugt zu sein, dass man nur gemeinsam, also in internationaler Kooperation der globalen Herausforderung bedrohter digitaler Sicherheit begegnen kann. Lücken in der (internationalen) Gesetzgebung gelte es gemeinsam zu schließen. Nicht Abschottung und Konzentration auf die innerstaatlichen Interessen und Regularien strebt Singapur an, sondern konsensorientierte Zusammenarbeit auf globaler Ebene, um das Ziel nachhaltiger Cyber-Sicherheit zu erreichen:

> *„Singapur engagiert sich für eine starke globale Zusammenarbeit für unsere gemeinsame globale Sicherheit. Singapur wird aktiv mit der internationalen Gemeinschaft zusammenarbeiten, insbesondere mit der ASEAN, um sich mit Fragen der transnationalen Cybersecurity und dem Thema Cybercrime zu befassen. Wir werden uns für Initiativen zum Aufbau der Cyber-Kapazitäten einsetzen und den Austausch über Cyber-Normen und -Rechtsvorschriften erleichtern. Durch internationalen Konsens, Vereinbarungen und Kooperationen können wir den Cyberspace zu einem sichereren und verlässlicheren Platz für alle machen."* (CSA 2016)[11]

Durch seine Erfahrung, dass Singapur seit 2013 mehrfach Opfer von Cyber-Spionage großen Ausmaßes wurde, fasst der Stadtstaat solche Attacken als globale Herausforderung auf – wenngleich er parallel zu kooperativen internationalen Aktivitäten auch im Inland zahlreiche eigenständige Gegenmaßnahmen getroffen hat: So hat Singapur seit 2013 einen „National Cybersecurity Master Plan" und das Programm „National Cybersecurity R&D" (NCR) zur Förderung der zugehörigen Forschung aufgelegt,

[11] *Zitat im englischen Original: „Singapore is committed to strong global collaboration for our collective global security. Singapore will actively cooperate with the international community, particularly with the ASEAN, to address transnational cybersecurity and cybercrime issues. We will champion cyber capacity building initiatives, and facilitate exchanges on cyber norms and legislation. Through international consensus, agreement and cooperation, we can make cyberspace a safer and more secure place for all."*

mit dem „National Cyber Security Centre" (NCSC) und der CSA zwei spezialisierte staatliche Institutionen geschaffen und diverse strategische und regulative Maßnahmen gestartet (Cybercrime Command 2015; National Cybercrime Action Plan 2016) (vgl. CSA 2016).

Auf Gesetzesebene überarbeitete Singapur im Nachhall der Cyber-Attacken von 2013 den „Computer Misuse Act" (CMA) im selben Jahr sowie erneut im Jahr 2017, um die Umsetzung der Cybersecurity-Strategie der Regierung und den Aufbau robuster Cybersecurity-Fähigkeiten zu unterstützen.

Der Gesetzentwurf versucht in seiner letzten Fassung, seine Reichweite zu erweitern, indem er Handlungen kriminalisiert, die durch Cyber-Angriffe ermöglicht werden. In Bezug auf die exterritoriale Anwendung stuft der CMA nunmehr auch Taten als strafbar ein, die vom Ausland gegen einen Computer in Singapur verübt werden. Allerdings reicht der Arm des CMA nicht so weit, dass er Handlungen ahnden könnte, die vom Ausland gegen einen Computer im Ausland begangen werden, auch wenn dadurch der Schaden in Singapur entsteht. Hier stößt er also an seine (transnationalen) Grenzen. Doch greift der CMA in seinem Wirkungskreis härter durch, weil mehrfach verübte Straftaten nun beispielsweise höher bestraft werden können (vgl. Leck und Lim 2017a).

Auf politischer Seite sorgt man sich in Singapur vor allem um die lokalen Unternehmen, deren Bewusstsein in Fragen der Datensicherheit unzureichend erscheint. Als Gegenmaßnahme bietet beispielsweise der staatliche Dienstleister „Singapore Computer Emergency Response Team" (SingCERT) Sicherheitshinweise für Unternehmen an, um sie auf Bedrohungen aufmerksam zu machen. Ferner soll die „Infocomm Media Development Authority" (IMDA) einen neuen Technologie-Hub etablieren, der unter anderem kleine und mittlere Unternehmen zum Thema Cybersecurity beraten kann (vgl. Leck und Lim 2017b).

Estland

Das kleine Land im europäischen Norden will in Sachen Digitalisierung ganz nach vorn und hat dafür unter anderem im staatlichen Sektor eine Vielzahl innovativer Maßnahmen realisiert. De facto hat sich Estland nach dem Einschnitt in Folge des Kalten Krieges, als sich das gesamte System zwangsläufig reorganisieren musste, mit dem Programm „e-Estonia" neu erfunden. Wie auf der Website e-Estonia.com nachzulesen ist, stand am Anfang dieses langen Prozesses die bewusste Entscheidung der estnischen Regierung nach dem Ende des Ostblocks, auf Digitalisierung als neue Entwicklungsbasis des Landes zu setzen. Seit mehr als zwanzig Jahren treibt die estnische Staatsführung diesen Plan nunmehr zielstrebig voran und hat damit ein einzigartiges staatliches Geschäftsmodell geschaffen.

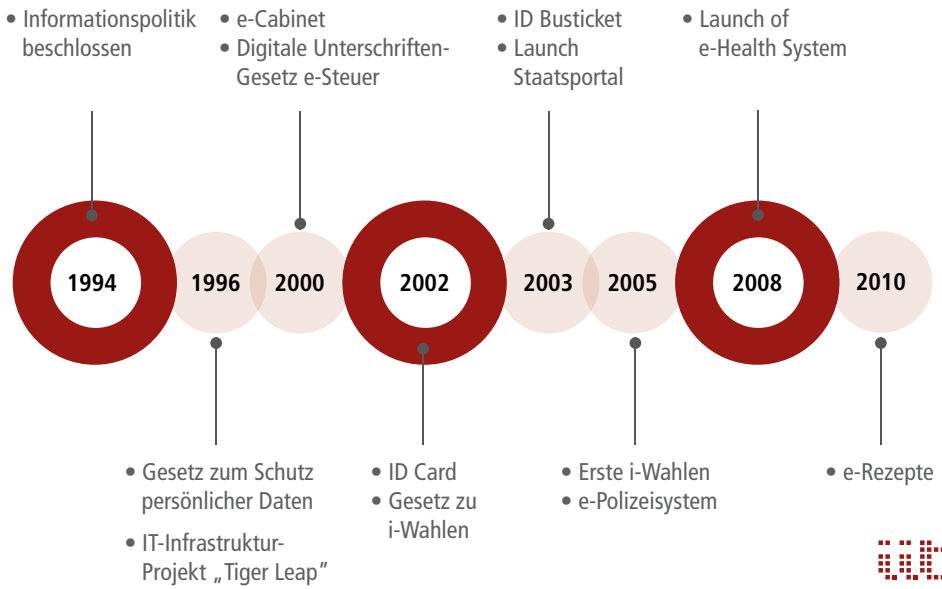

Abbildung 3.2.3: Estlands Weg zur E-Society

Besondere Aufmerksamkeit im Kontext digitaler (öffentlicher) Verwaltungsinnovationen hatte die „e-Residency" Estlands erregt. Diese wird seit 2014 angeboten und soll insbesondere Unternehmer virtuell und finanziell ins Land ziehen. Für 50 Euro erhält der Erwerber der e-Residency-Chipkarte zwar keine volle estnische Staatsbürgerschaft, aber er kann mithilfe der Identifikationsfunktionen zahlreiche Behördengänge in Estland via Internet absolvieren. Dies reicht bis hin zu Unternehmensgründungen, die in wenigen Minuten komplett über das Internet erfolgen können. „Über 40 Länder weltweit nutzen estonische IT-Lösungen"[12] heißt es dazu auf e-Estonia.com.

Die deutsche Bundesregierung holte für den digitalen Wandel hierzulande bereits Rat von estnischer Seite in Person des Premierministers Taavi Roivas ein, und Bundesinnenminister Thomas de Maizière bezeichnete Estland als europäischen Vorreiter, von dem Deutschland viel lernen könne (vgl. BR 2016).

Eine derartige gesamtgesellschaftliche Konzentration auf die Digitalisierung macht ein Land jedoch angreifbar für Cyber-Angriffe und folglich auch stark davon abhän-

[12] *Zitat im englischen Original: „Over 40 countries around the world are using Estonian e-solutions". Siehe hierzu: e-Estonia.com: How we got there. Verfügbar unter: https://e-estonia.com/the-story/how-wegot- there, zuletzt zugegriffen am 29.04.2017.*

gig, diesen wirksam begegnen zu können. Diese Verletzlichkeit wurde den Esten im Frühjahr 2007 sehr deutlich bewusst, als umfangreiche Attacken maßgebliche estnische Institutionen trafen. Das öffentliche Leben in Estland war durch die Ereignisse stark beeinflusst, denn die Angriffe richteten sich zwar primär auf politische Institutionen, aber auch auf Banken, Medien und Kommunikationsnetze (vgl. BBC News 2008).

Estlands Regierung bemüht sich seitdem umso mehr um höchste Sicherheitsstandards. Gleichzeitig wurden aber auch internationale Partner endgültig wachgerüttelt. Passend dazu betreibt beispielsweise die NATO seit 2008 in Tallinn ein Cyber-Abwehrzentrum und nutzt so zugleich die hervorragende digitale Infrastruktur Estlands. Auch gemeinsame Manöver zur Cyber-Abwehr werden von NATO-Staaten regelmäßig in Estland abgehalten.

Jüngst ging Estlands Regierung noch einen Schritt weiter: Ganz im Sinne seiner grundsätzlich dezentralen IT-Infrastruktur werden nun außerhalb des Landes sogenannte Daten-Botschaften gegründet, an denen der estnische Datenbestand im Falle eines Falles als Back-Up verfügbar ist. Offenbar wird es nicht nur bei einem Standort bleiben: Die erste estnische Daten-Botschaft wird in Luxembourg eröffnet, nachdem Großbritannien wegen des Brexits ausschied (vgl. Security Week 2016).

Dänemark

Dänemark nahm im EU-Index für Digitalisierung (Digital Economy and Society Index – DESI) im Jahr 2017 erneut Platz eins ein. Seit Jahren ist Dänemark innerhalb der EU einer der digitalen Spitzenreiter. Doch für 2017 bescheinigt die DESI-Analyse Dänemark noch einmal besonders große Fortschritte (vgl. Europäische Kommission 2017). Auch der dänische Staat macht keinen Hehl daraus, dass das Land ambitionierte Zielsetzungen in Sachen Digitalisierung hegt (Dänemark – Das digitalisierteste Land der Welt)[13]: Diese Ambitionen schließen eine Höchststufe digitaler Sicherheit ein.

Das dänische „Centre for Cyber Security" konstatiert in einer Studie aus dem Jahr 2016 eine insgesamt sehr hohe Bedrohung der Cyber-Sicherheit sowohl für staatliche Stellen als auch für die Privatwirtschaft (vgl. CFCS 2016). Im April 2017 gab es erneut Meldungen, das dänische Verteidigungsministerium leide seit Jahren unter

[13] *Zitat im englischen Original: „Denmark – The most digitised country in the world". Siehe hierzu: Denmark – The most digitised country in the world. Visions for the Danish Government (2015). Verfügbar unter: www.finansraadet.dk/en/News/Documents/2015/193-2015%20Danmark%20Digitalisering%202015%20UK.PDF, zuletzt zugegriffen am 29.04.2017.*

Hacker-Attacken aus dem Ausland (vgl. MacFarquhar 2017), bei denen sich immer neue Herangehensweisen abzeichneten:

> *„Die staatlich finanzierten Hacker-Gruppen nutzen zunehmend Organisationen, zu denen sie bereits Zugriff erlangt haben, als Plattform, um mehr Ziele mit größerem Sicherheitsbewusstsein anzugreifen. Öffentliche Einrichtungen und private Unternehmen können so zum Sprungbrett für echte Ziele werden – dies ist ein Element, das in ihrem Risikomanagement berücksichtigt werden sollte."* (CFCS 2016)[14]

In technischer Hinsicht soll die Entwicklung neuer IT-Systeme im Sinne von „Privacy by Design" und „Security by Design" bereits im Entstehungsprozess auf ihre Konformität hin geprüft werden. So sieht es, wie oben erwähnt, auch die EU-Datenschutz-Grundverordnung vor. Vorschläge in den dänischen Strategien für Entwicklungsbereiche beziehen sich beispielsweise auf Lösungen für Daten-Anonymisierungs- und De-Anonymisierungsprozesse (Denmark – The most digitised country in the world 2015).

Auch die dänische Cyber Strategie 2016–2020 beschäftigt sich umfassend mit Sicherheitsfragen (The Government; Local Government; Danish Regions 2016). Für den dänischen IT-Governance-Bereich wird gefordert, Nutzer, die mit dem Entwicklungstempo nicht Schritt zu halten vermögen, umfassend zu unterstützen. So soll in der sehr auf sozialen Ausgleich orientierten Gesellschaft Dänemarks niemand den Anschluss an die digitale Entwicklung verlieren.

Sozialer Ausgleich und gleichberechtigte Teilhabe an der Digitalisierung sind auch im Kontext digitaler Sicherheit in Dänemark ein politisch relevanter Faktor, wozu auch der Schutz der Privatheit dänischer Bürger gehört. Deutlich wird im dänischen Diskurs – explizit und implizit –, dass der digitalen Souveränität aller Bürger analog zu dem allgemeinen gesellschaftlichen Zusammenhalt ein hoher Stellenwert eingeräumt wird.

In dem Strategiepapier zu den staatlichen Visionen von 2015, das unter umfangreicher Mitwirkung von zahlreichen dänischen Institutionen und Unternehmen entstand, zielt der Begriff der digitalen Sicherheit ebenfalls nicht nur auf den allgemeinen Schutz von individuellen und institutionellen Anwendern bei der Nutzung digi-

---

[14] *Zitat im englischen Original: „The state-sponsored hacker groups are increasingly using organizations whose networks they have already gained access to as platforms for attacking more targets with greater security awareness. Public authorities and private companies could thus become a stepping stone towards the real targets – an element that should be included in their risk management."*

taler Lösungen ab. Digitale Sicherheit umfasst auch hier die Einbeziehung herausgeforderter Gruppen der dänischen Gesellschaft, die nicht im Stich gelassen werden dürften. Dies steht in einem auffälligen Kontrast zu den genannten asiatischen Strategien, in denen Bürgerinteressen, Partizipation und Zugang auf der individuellen Ebene eine untergeordnete Rolle spielen. Passend hierzu heißt es auch zur dänischen „Agency for Digitisation", dass deren Gründung 2011 insbesondere mit der Zielsetzung erfolgte, den dänischen Wohlfahrtsstaat zu modernisieren (vgl. Danish Ministry of Defence 2016).

> *„Dänemark hat eine Tradition, eine integrative Gesellschaft zu sein, und wir müssen dies in Bezug auf die Digitalisierung beibehalten. Wir werden deshalb zusammen mit dem öffentlichen Sektor dazu beitragen, dass die Digitalisierung für alle in Dänemark verfügbar ist."* (Europäische Kommission 2017)[15]

Die deutsche Situation im Kontext

Die Aufregung in den sozialen Medien war groß, als die deutsche Bundeskanzlerin Angela Merkel 2013 im Rahmen einer Pressekonferenz mit Barack Obama das Internet als Neuland bezeichnete (vgl. BR 2013b). Was die „Digital Natives" in den Foren des Internets zu größter Aktivität anspornte, entbehrte zu dem Zeitpunkt jedoch für einen Großteil der deutschen Bevölkerung nicht jeder Grundlage: die Selbstverständlichkeit, mit der in Deutschland das Internet und digitale Dienstleistungen genutzt wurden und werden, ist mitunter längst nicht so groß wie von weiten Teilen der digitalisierungsaffinen jüngeren Generation und Vertretern der Medien durch ihre Entrüstung suggeriert wird. Im „The Digital Economy and Society Index" (DESI) der Europäischen Kommission nimmt Deutschland aktuell (2017) im europäischen Vergleich nur einen der mittleren Plätze ein, weit abgeschlagen hinter den Spitzenreitern Dänemark, Finnland, Schweden und den Niederlanden. Dass Deutschland in diesem bedeutsamen Feld von einer Spitzenposition recht weit entfernt ist, ist allen relevanten Akteuren bekannt und findet auch im Handeln des Staates – hier insbesondere des Bundes – seinen Ausdruck (Europäische Kommission 2017).

Der Begriff der digitalen Souveränität findet sich nicht im Koalitionsvertrag von CDU, CSU und der SPD für die 18. Legislaturperiode (BR 2013a), wohl aber vergleichbare Termini wie technologische Souveränität und Schlagworte wie Cyber-Kriminalität und digitaler Datenschutz. Mit der Digitalen Agenda 2014–2017 formulierte die Bundes-

[15] *Zitat im englischen Original: „Denmark has a tradition of being an inclusive society and we need to maintain this in terms of digitisation. We would therefore, together with the public sector, like to contribute to making digitisation available for everyone in Denmark."*

regierung 2014 die Grundsätze ihrer Digitalpolitik (BR 2014). Verantwortlich sind gleich drei Ministerien: das Bundesministerium für Wirtschaft und Energie, das Bundesministerium des Innern und das Bundesministerium für Verkehr und digitale Infrastruktur.

Das Dokument skizzierte die Absichten der Regierungsarbeit unter anderem für die Entwicklung digitaler Infrastrukturen, digitale Wirtschaft, Bildung und Forschung, Sicherheit sowie die Einbettung der deutschen Digitalen Agenda in den europäischen und internationalen Kontext. Die Digitale Agenda wurde bereits im Zuge ihrer Vorstellung mehrfach kritisiert. Beanstandet wurde unter anderem, dass sie kaum über eine Beschreibung der Problemlage hinaus käme (vgl. Steiner 2014). Und auch die Verteilung der Verantwortung auf gleich drei „Internetminister" (vgl. Matzat 2014) vermochte nicht zu überzeugen.

Ende April 2017 stellten nun die drei Ministerien den Legislaturbericht „Digitale Agenda 2014–2017" (vgl. BMI et al. 2017) vor und verwiesen auf die Fortschritte in den jeweiligen Handlungsfeldern. Entstanden sind demnach in den letzten Jahren unter anderem Weißbücher zu Themen wie Arbeiten 4.0 (BMAS 2017) und Digitale Plattformen (BMWi 2017).

Wie schon bei der Vorstellung der Digitalen Agenda zum Beginn der Legislaturperiode war auch die Resonanz auf den Legislaturbericht eher zurückhaltend. Die Kommentare machen unter anderem auf die großen Schwierigkeiten bei der Digitalisierung der öffentlichen Verwaltung und die Umsetzung von Open Data (vgl. tagesschau.de 2017) aufmerksam. Sowohl die eingangs erwähnte aktuelle Bewertung durch den DESI wie auch andere Indikatoren weisen darauf hin, dass Deutschland mit der Digitalen Agenda einer Spitzenposition in Europa bislang nicht nähergekommen ist und weitere Anstrengungen erforderlich sein werden. Dazu gehört unter anderem auch die Fortführung der Forschung über den Prozess der Digitalisierung und damit verbundener Implikationen. Ein Ort dafür wird künftig das Deutsche-Internet-Institut in Berlin sein, wie Ende Mai auf einer Pressekonferenz des Bundesministeriums für Bildung und Forschung bekanntgegeben wurde (vgl. BMBF 2017).

Dass in Bezug auf die technische Infrastruktur bei Weitem nicht alle Möglichkeiten ausgeschöpft wurden, attestiert auch eine Studie der Bertelsmann-Stiftung, die das Fraunhofer-Institut für System- und Innovationsforschung ISI durchgeführt hat. Fazit: Deutschland konnte bisher beim Ausbau seiner Breitbandnetze nicht aufholen. Gerade in Hinblick auf die Entwicklung der als zukunftsträchtig angesehenen Glasfaserinfrastruktur gibt Deutschland im Vergleich zu anderen – auch europäischen Staaten – ein schwaches Bild ab. Dies betrifft insbesondere ländliche Regionen, wo Deutschland nicht nur hinter kleinen, hier schon thematisierten Ländern wie Estland, sondern zum Beispiel auch hinter Spanien zurückbleibt (vgl. Beckert 2017).

Nach wie vor ist die Situation in Deutschland von dem Bestreben geprägt, Abhängigkeiten gegenüber dem Ausland – insbesondere bei Software, Hardware und digitalen Infrastrukturen – zu reduzieren. Hier liegt der Fokus auf wirtschaftlichen Interessen: Digitale Souveränität entwickelt sich hierzulande gerade im Kontext von Industrie 4.0 und der Hightech-Strategie der Bundesregierung zu einer entscheidenden ökonomischen Standortfrage. Mit der Fraunhofer-Gesellschaft an der Spitze der staatlich geförderten Forschung will der Staat aktuell die Wettbewerbsfähigkeit der deutschen Wirtschaft – besonders der Automobilindustrie – sicherstellen.

Entscheidend für das Gelingen der industriellen Automatisierungspläne Deutschlands ist unter anderem die Gewährleistung sicherer Datenräume, wie sie derzeit beispielsweise im Konzept „Industrial Data Space" avisiert wird (vgl. FhG 2016). Mit solchen Datenräumen, die in industrie-partnerschaftlich zugänglichen Clouds vor Cyber-Spionage durch ausländische Konkurrenz bewahrt werden, will man noch zögerliche, insbesondere auch mittelständische Unternehmen für ein Engagement im Zuge der datenbasierten vierten industriellen Revolution gewinnen (vgl. Ronzheimer 2017).

Die Abhängigkeit vom Betriebssystem Windows der Firma Microsoft hat sich zuletzt wiederholt als problematisch herausgestellt – beispielsweise im Rahmen des „WannaCry"-Hackerangriffs oder durch Meldungen über Computerprogramme wie Athena im Arsenal der CIA, mit dem sich die Organisation Zugang zu jedem Windows-Rechner verschaffen können soll (vgl. ntv 2017b). Hier konnten auch trotz entsprechender Beschlüsse des Europäischen Parlaments auf Kommissions- und Regierungsebene in Europa noch keine effektiven Maßnahmen durchgesetzt werden, die Abhängigkeiten von ausländischen Unternehmen wie Microsoft reduzieren würden (vgl. ntv 2017a).

Es liegt auf der Hand, dass hier komplexe wirtschaftspolitische Interessen und Machtstrukturen wirksame politische Schritte erschweren können. Derzeit geht es in der deutschen Ökonomie nicht mehr nur darum, ein Microsoft oder Google made in Germany beziehungsweise ein IT-Flaggschiff für eine noch unbesetzte Nische zu erschaffen (vgl. Bitkom 2015). Vielmehr sorgt man sich in Deutschland – etwa mit Blick auf das autonome Fahren –, dass die hiesigen Kernindustrien auf die hinteren Bänke der Hardware-Zulieferer für die digitalen Riesen degradiert werden, die künftig in allen möglichen Sparten den Ton angeben könnten (vgl. Canzler 2016).

Die digitale Souveränität auf staatlicher Ebene zu erweitern, heißt in Deutschland sowohl die Interessen der Wirtschaft zu wahren und Schutz zu gewährleisten als auch die Interessen der breiten Bevölkerung im Auge zu behalten. Dass das Vertrauen in die Kompetenz der Politik und die Neutralität im Sinne ihrer Bürger erschüttert ist, hängt sicherlich auch eng mit den Aufdeckungen von Edward Snowden zusammen, die sich bis zu den jüngsten Enthüllungen von Wikileaks fortsetzen und

den Bürger die Abgründe mehr als erahnen lassen. Vorstöße in jüngerer Zeit – wie jene zur Abschaffung des Bargelds oder zur verpflichtenden Durchsetzung des elektronischen Passes – haben in der deutschen Öffentlichkeit zum Teil vehemente Widerstände hervorgerufen und dürften eher das Gefühl der Bürger bestärkt haben, dass ihre digitale Souveränität gegenüber jener des Staates oder der Wirtschaft als nachranging angesehen wird. Das auf internationaler Ebene so vielfältig thematisierte schwindende Vertrauen in den Prozess der Digitalisierung allgemein und die Nutzung einzelner Dienstleistungen wird so nur schwerlich zurückzugewinnen sein.

Ausblick

Was bedeutet nun digitale Souveränität aus der Sicht von internationalen Organisationen, Staatengemeinschaften und einzelnen Ländern? Es gibt viele Gemeinsamkeiten: Die Potenziale der Digitalisierung – nicht nur des Internets – für die wirtschaftliche und soziale Entwicklung sind unbestritten. Doch zusammen mit dem rasanten technologischen Fortschritt, dem zunehmenden Zwang, auf Technologie und digitale Dienstleistungen vertrauen zu müssen, wächst zugleich das Bewusstsein der Abhängigkeit und Verletzbarkeit. Und es gibt noch eine Gemeinsamkeit aller Akteure, die sie zugleich verbindet und gegeneinander positioniert – die Vorstellung, dass die gleichen Normen, Prinzipien und Werte, die in den jeweiligen Ländern offline gelten, auch online angewendet werden sollten. Während die EU in ihrer Cybersecurity Strategie Offenheit und Freiheit im Netz als zentrale Prinzipien hervorhebt, die sie auch online zur Geltung bringen will (vgl. Europäische Kommission 2013), realisiert China einen nationalen Cyberspace, der den Normen und eher hermetischen Prinzipien folgt, die das Land auch offline zur Geltung bringt.

Der Kontrast zwischen der EU und China ist nur ein Beispiel für die zunehmende Fragmentierung eines ohnehin nicht einheitlichen Internets. Und die Auseinandersetzung um Sicherheitsrisiken und spezifische, nationale Interessen ist längst im Gange: Auch innerhalb des westlichen Blocks herrscht nicht uneingeschränkte Einigkeit. Beispielhaft ist bei uns der fortdauernde Konflikt mit Facebook über den Umgang mit in Deutschland strafrechtlich relevanten Beiträgen, etwa rechter Propaganda oder auch der Darstellung von Nacktheit.

Im E-Commerce und insbesondere im E-Service kollidieren oft anhand der Aktivitäten transnational agierender Unternehmen auch unterschiedliche Rechtssysteme. Und schließlich besteht auch in vielen europäischen Ländern ein gewisses Misstrauen gegenüber anderen westlichen Ländern, in denen etwa die zentralen Knotenpunkte des Internets verwaltet werden, an denen potenziell Daten abgegriffen werden können. Auch liberale Staaten oder Staatengemeinschaften haben vor diesem Hintergrund den Bedarf der Ausweitung ihrer Schutzfunktionen erkannt und stoßen im Zuge des Umdenkens an die Grenzen der Grenzenlosigkeit des digitalen Raums. Die

Folgen dieses auch als Balkanisierung des Internets beschriebenen Prozesses sind zum gegenwärtigen Zeitpunkt nur schwer vorherzusagen.

Bei dieser Untersuchung mit internationalen Perspektiven auf digitale Souveränität nahmen jedoch auch einige zentrale Lösungsansätze deutlichere Konturen an: Wie zu sehen war, strebt Singapur über die regionale Interessengemeinschaft ASEAN und darüber hinaus internationale Allianzen an, um den digitalen Herausforderungen zu begegnen. Es verfolgt damit offenbar eine andere Strategie als der asiatische Nachbar China und ist näher am Vorgehen der EU, die auf regionale Partnerschaften aufbaut. Regionale Staatenverbünde wie ASEAN und die EU können als Motoren für gemeinsame, grenzüberschreitende Initiativen von Partnerländern aktiv werden. Wie die beteiligten europäischen Staaten vereinbarte Maßnahmen unterstützen und mittragen müssen, um als regionale Macht ihre digitale Souveränität zu sichern – etwa bei der konsequenten Umsetzung der EU-Datenschutz-Grundverordnung –, so wird auch Singapur zu Kompromissen bereit sein müssen, wenn es mit Hilfe von Partnerschaften gemeinsame Strategien zur Wahrung von Cyber-Sicherheit und -Souveränität entwickeln und umsetzen will.

Internationale Zusammenarbeit stellt die eigenen, die Souveränität umgebenden Grenzen nicht in Frage, sondern ist vielmehr ihre langfristige Garantie – ebenso wie internationale Kooperation in Europa einen grundlegenden Zweck der Staatengemeinschaft darstellt. Denn nur durch die Kooperation der EU-Staaten können globale Herausforderungen nachhaltig adressiert werden.

Insbesondere für exportorientierte Länder wie Deutschland sind Abschottung und politische Alleingänge keine realistische Option. Angesichts globaler Wirtschaftsstrukturen ist eine ökonomische Autarkie ebenso wenig erstrebenswert wie realistisch. Die Analyse der Strategien der kleineren Staaten – insbesondere von Estland und Singapur – hat gezeigt, dass sie den Herausforderungen durch Offenheit und internationale Kooperation zu begegnen suchen. Eine Orientierung auf die Binnenwirtschaft mag heutzutage selbst für das bevölkerungsreiche China eine große Herausforderung darstellen, für kleinere Länder – und dazu muss in diesem Rahmen auch Deutschland gezählt werden – ist dies keine realistische Alternative.

Andererseits entwickeln sich, wie an den Beispielen Singapur, Estland und Dänemark zu sehen war, gerade kleinere Staaten recht gut, was die Digitalisierung und auch zumindest das Schaffen von Souveränitätsstrategien in diesem Kontext betrifft. Liegt das wiederum nur an den kleineren Ausmaßen dieser Systeme und ihrer Gesellschaften, die zum Beispiel die Mitnahme der ganzen Bevölkerung und Wirtschaft in Richtung Digitalisierung erleichtern? Gerade die europäischen Nachbarn, und hier insbesondere die skandinavischen Länder, Estland und die Niederlande sind aufgrund ähnlicher Wertesysteme nicht nur räumlich die vermutlich naheliegenderen Vorbilder. Doch auch hier ist eine genauere Untersuchung erforderlich, welche im Ausland

erprobten Entwicklungen für Deutschland geeignet sind und welche nicht. Wenn die gläserne Existenz der Bürger in Estland offenbar weitgehend akzeptiert wird beziehungsweise ohne weitere Alternativen durchgesetzt werden kann (Laaf und Schlieter 2016), dies hierzulande jedoch aufgrund einer anderen historischen Erfahrung und Rechtsprechung – etwa der im Rahmen der Volkszählung entstandenen Rechtsprechung zur informationellen Selbstbestimmung – mit Vorbehalten und Skepsis betrachtet wird, dann ist die Durchsetzung entsprechender Regelungen nur unter großen Kosten des Vertrauens in die Politik zu realisieren. Der Ansatz Dänemarks zeichnet sich hier durch seinen inklusiven und unterstützenden Ansatz bei der Begleitung des Prozesses der Digitalisierung aus, weil es die Einbindung der breiten Bevölkerung als aktives Aufgabenfeld der beteiligten Akteure aus Politik und Wirtschaft definiert.

Für Deutschland bedeutet dies, weiterhin eine sowohl die eigenen historischen und kulturellen Voraussetzungen respektierende Strategie zu entwickeln und zu verfolgen als auch dabei zugleich die Vielfältigkeit der internationalen Interessen und Entwicklungen anzuerkennen. Diese gilt es zu beobachten, wobei vor allem der Blick auf erfolgreiche europäische Partnerländer vielversprechend erscheint, um im internationalen Kontext gegenüber dem nach wie vor dominanten digitalen Hegemon USA sowie aufstrebenden Akteuren wie China bestehen zu können. Die europäische Kooperation erscheint hier dringlicher denn je. Maßnahmen wie die EU-Datenschutzrichtlinie können hilfreich sein, neuen nationalen Initiativen eine Orientierung zu geben und verlorenes Vertrauen sowohl in die politische Gestaltbarkeit der Digitalisierung der Gesellschaft als auch in die Europäische Union wiederherzustellen.

Literatur

Alsabah, N. (2017). Peking will gläserne Unternehmen. In: ZEIT ONLINE, 31.03.2017. Verfügbar unter: www.zeit.de/politik/ausland/2017-03/netzpolitik-china-cybersicherheit-zensur-internet, zuletzt zugegriffen am 29.04.2017.

BBC News (2008). Estonia fines man for ‘cyber war’. In: BBC News, 25.01.2008. Verfügbar unter: http://news.bbc.co.uk/2/hi/technology/7208511.stm, zuletzt zugegriffen am 29.04.2017.

Beckert, B. (2017). Ausbaustrategien für Breitbandnetze in Europa. Was kann Deutschland vom Ausland lernen? In: Bertelsmann-Stiftung. Verfügbar unter: www.bertelsmann-stiftung.de/fileadmin/files/Projekte/Smart_Country/Breitband_2017_final.pdf, zuletzt zugegriffen am 29.05.2017.

Bitkom (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 29.05.2017.

Bound, K.; Saunders, T.; Wilsdon, J.; Adams, J. (2013). China's absorptive state. Research, innovation and the prospects for China-UK collaboration. Verfügbar unter: www.nesta.org.uk/sites/default/files/chinas_absorptive_state_0.pdf, zuletzt zugegriffen am 21.07.2017.

Bundesministerium des Innern (BMI); Bundesministerium für Wirtschaft und Energie (BMWi); Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) (2017). Legislaturbericht Digitale Agenda 2014–2017. Verfügbar unter: www.digitale-agenda.de/Content/DE/_Anlagen/2017/04/2017-04-26-digitale-agenda.pdf?__blob=publicationFile&v=3, zuletzt zugegriffen am 29.05.2017.

Bundesministerium für Arbeit und Soziales (BMAS) (2017). Weissbuch Arbeiten 4.0. Verfügbar unter: www.bmas.de/SharedDocs/Downloads/DE/PDF-Publikationen/a883-weissbuch.pdf;jsessionid=CFBEED1F3D55F84F4C53BD3547034EBB?__blob=publicationFile&v=8, zuletzt zugegriffen am 29.05.2017.

Bundesministerium für Bildung und Forschung (BMBF) (2017). Das Deutsche Internet-Institut entsteht in Berlin – BMBF. Verfügbar unter: www.bmbf.de/de/das-deutsche-internet-institut-entsteht-in-berlin-4227.html (zuletzt aktualisiert am 23.05.2017), zuletzt zugegriffen am 29.05.2017.

Bundesministerium für Wirtschaft und Energie (BMWi) (2017). WEISSBUCH – DIGITALE PLATTFORMEN 2017. Verfügbar unter: www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/weissbuch-digitale-plattformen.pdf?__blob=publicationFile&v=22, zuletzt zugegriffen am 29.05.2017.

Bundesregierung (BR) (2013a). Deutschlands Zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD 18. Legislaturperiode. Verfügbar unter: www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf?__blob=publicationFile, zuletzt zugegriffen am 29.05.2017.

Bundesregierung (BR) (2013b). Pressekonferenz von Bundeskanzlerin Merkel und US-Präsident Obama. Verfügbar unter: www.bundesregierung.de/ContentArchiv/DE/Archiv17/Mitschrift/Pressekonferenzen/2013/06/2013-06-19-pk-merkel-obama.html, zuletzt zugegriffen am 29.05.2017.

Bundesregierung (BR) (2014). Digitale Agenda 2014–2017. Verfügbar unter: www.bmwi.de/Redaktion/Migration/DE/Downloads/Publikationen/digitale-agenda-2014-2017.pdf?__blob=publicationFile&v=1, zuletzt zugegriffen am 29.05.2017.

Bundesregierung (BR) (2016). Kabinettsklausur in Meseberg. Digitalisierung gemeinsam vorantreiben, 25.05.2016. Verfügbar unter: www.bundesregierung.de/Content/DE/Artikel/2016/05/2016-05-24-digitalisierung-meseberg.html, zuletzt zugegriffen am 29.04.2017.

Cai, J.; Kwong, P. (2016). Communist Party leadership calls for fairer global governance of internet. Developing nations should take on a greater role in managing the web, president tells opening of conference in Wuzhen. In: South China Moning Post, 16.11.2016. Verfügbar unter: www.scmp.com/news/china/policies-politics/article/2046645/communist-party-leadership-calls-fairer-global, zuletzt zugegriffen am 20.07.2017.

Canzler, W. (2016). Autonomes Fahren in Deutschland. Die deutsche Politik und die deutsche Automobilindustrie denken nicht weit genug. In: Tagesspiegel, 19.08.2016. Verfügbar unter: https://causa.tagesspiegel.de/gesellschaft/autonomes-fahren-sind-wir-bereit-fuer-selbstfahrende-autos/die-deutsche-politik-und-die-deutsche-automobilindustrie-denken-nicht-weit-genug.html, zuletzt zugegriffen am 29.05.2017.

Centre for Cyber Security (CFCS) (2016). Threat Assessment. The cyber threat against Denmark. Verfügbar unter: https://fe-ddis.dk/cfcs/CFCSDocuments/Threat%20Assessment%20-%20The%20cyber%20threat%20against%20Denmark.pdf, zuletzt zugegriffen am 27.04.2017.

China Media Project (CMP) (2015). Internet Sovereignty. China Media Project. Verfügbar unter: http://cmp.hku.hk/2015/09/30/internet-sovereignty, zuletzt zugegriffen am 24.04.2017.

Christmann-Budian, S. (2012). Chinesische Wissenschaftspolitik seit den 1990er Jahren. Eine empirische Analyse zur praxispolitischen und ideologischen Funktionalisierung von Wissenschaft in einer transformativen Gesellschaft der Globalisierungsära. Verfügbar unter: www.diss.fu-berlin.de/diss/servlets/MCRFileNodeServlet/FUDISS_derivate_000000012882/Dissertation_Christmann.pdf;jsessionid=A373022019E9F6C35A99712116B94F8A?hosts=, zuletzt zugegriffen am 20.07.2017.

Cole, T. (2016). Finanzkrise: Das Internet ist schuld – und die Lösung. In: IT Finanzmagazin. Verfügbar unter: www.it-finanzmagazin.de/finanzkrise-das-internet-ist-schuld-und-die-loesung-26620, zuletzt zugegriffen am 26.04.2017.

Cyber Security Agency of Singapore (CSA) (2016). Singapore's Cybersecurity Strategy. SCS 2016. Verfügbar unter: www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf?la=en, zuletzt zugegriffen am 28.04.2017.

Danish Ministry of Defence (2016). Danish Cyber Fact Sheet. Verfügbar unter: www.fmn.dk/temaer/nato/Documents/2016-NATO-faktaark-Danish-Cyber.pdf, zuletzt zugegriffen am 20.07.2017.

Denmark – The most digitised country in the world. Visions for the Danish Government (2015). Verfügbar unter: www.finansraadet.dk/en/News/Documents/2015/193-2015%20Danmark%20Digitalisering%202015%20UK.PDF, zuletzt zugegriffen am 29.04.2017.

Europäische Kommission (2010). Digitale Agenda für Europa. Verfügbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=URISERV%3Asi0016 (zuletzt aktualisiert am 25.06.2010), zuletzt zugegriffen am 24.04.2017.

Europäische Kommission (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brüssel. Verfügbar unter: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf, zuletzt zugegriffen am 24.04.2017.

Europäische Kommission (2015). Digital Single Market. Verfügbar unter: https://ec.europa.eu/digital-single-market/en/digital-single-market (zuletzt aktualisiert am 12.01.2017), zuletzt zugegriffen am 28.04.2017.

Europäische Kommission (2017): The Digital Economy and Society Index (DESI). Verfügbar unter: https://ec.europa.eu/digital-single-market/en/desi, zuletzt zugegriffen am 28.04.2017.

Forsythe, M.; Ramzy, A. (2016). China Censors Mentions of 'Panama Papers' Leaks. In: New York Times, 05.04.2016. Verfügbar unter: www.nytimes.com/2016/04/06/world/asia/china-panama-papers.html?_r=2, zuletzt zugegriffen am 20.07.2017.

Fraunhofer-Gesellschaft (FhG) (2016). Industrial Data Space – Digitale Souveränität über Daten (White Paper). Verfügbar unter: www.fraunhofer.de/content/dam/zv/de/Forschungsfelder/industrial-data-space/Industrial-Data-Space_whitepaper.pdf, zuletzt zugegriffen am 29.05.2017.

Fritz, S. (2017). Alibaba – Digitalisierung made in China. Verfügbar unter: https://stefanfritz.de/alibaba-digitalisierung-made-in-china, zuletzt zugegriffen am 28.04.2017.

Fulbright, N. R. (2015). Cyber security in China. Draft law strengthens regulation of internet and data privacy Juli 2015. Verfügbar unter: www.nortonrosefulbright.com/files/cyber-security-in-china-130661.PDF, zuletzt zugegriffen am 28.04.2017.

FZI Forschungszentrum Informatik (FZI) (Hrsg.) (2017): Sicheres Identitätsmanagement im Internet. Eine Analyse des ISÆN-Konzepts (Individual perSonal data Auditable addrEss) durch die Smart-Data-Begleitforschung im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi). Verfügbar unter: www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smartdata_studie_isaen.pdf;jsessionid=DF7A43747DDA38740F490671C8CE78C3?__blob=publicationFile&v=4, zuletzt zugegriffen am 28.04.2017.

Gracie, C. (2014). Alibaba IPO: Chairman Ma's China. In: BBC News, 08.09.2014. Verfügbar unter: www.bbc.com/news/world-asia-china-29119121, zuletzt zugegriffen am 20.07.2017.

Graham, L. (2016). Singapore is leading the way for the digital economy: Study. In: CNBC, 06.07.2016. Verfügbar unter: www.cnbc.com/2016/07/06/singapore-is-leading-the-way-for-the-digital-economy-study.html, zuletzt zugegriffen am 20.07.2017.

Gueham, F. (2017). Digital Sovereignty – Steps Towards a New System Of Internet Governance. Fondation pour L'Innovation Politique (Hrsg.). Verfügbar unter: www.fondapol.org/wp-content/uploads/2017/02/097-F.GUEHAM_Vang_2017-02-01_1.pdf, zuletzt zugegriffen am 24.04.2017.

Hatton, C. (2015). China 'social credit': Beijing sets up huge system. In: BBC News, 26.10.2015. Verfügbar unter: www.bbc.com/news/world-asia-china-34592186, zuletzt zugegriffen am 29.05.2017.

Huawei (2016). Deutschland und China – Wahrnehmung und Realität. Huawei-Studie 2016. Fokus: Digitalisierung und digitale Innovation. Verfügbar unter: www.huawei-studie.de/downloads/Huawei-Studie-2016-DE.pdf, zuletzt zugegriffen am 26.04.2017.

Laaf, M.; Schlieter, K. (2016). Digitalisierung von Politik. Vom Start-up zum Staat-up. In: taz.de, 09.12.2016. Verfügbar unter: www.taz.de/!5359317, zuletzt zugegriffen am 20.07.2017.

Lackes, R.; Siepermann, M. (2017). Gabler Wirtschaftslexikon, Stichwort: Cyberspace. Springer Gabler Verlag (Hrsg.). Verfügbar unter: http://wirtschaftslexikon.gabler.de/Archiv/75127/cyberspace-v9.html, zuletzt zugegriffen am 20.07.2017.

Leck, A.; Lim, R. J. (2017a). Proposed Changes to Computer Misuse and Cybersecurity Act. Verfügbar unter: www.bakermckenzie.com/en/insight/publications/2017/03/proposed-changes-to-computer-misuse, zuletzt zugegriffen am 29.04.2017.

Leck, A.; Lim, R. J. (2017b). Singapore Parliament Passes Amendments to Computer Misuse and Cybersecurity Act. Verfügbar unter: www.bakermckenzie.com/en/insight/publications/2017/04/singapore-parliament-passes-amendments, zuletzt zugegriffen am 29.04.2017.

Lepping, J.; Palzkill, M. (2016). Die Chance der digitalen Souveränität. In: Wittpahl, V. (Hrsg.). Digitalisierung. Bildung / Technik / Innovation. iit-Themenband, S. 17–25. Verfügbar unter: www.iit-berlin.de/de/publikationen/digitalisierung, zuletzt zugegriffen am 20.07.2017.

MacFarquhar, N. (2017). Denmark Says 'Key Elements' of Russian Government Hacked Defense Ministry. In: New York Times, 24.04.2017. Verfügbar unter: www.nytimes.com/2017/04/24/world/europe/russia-denmark-hacking-cyberattack-defense-ministry.html?_r=0, zuletzt zugegriffen am 20.07.2017.

Margolin, J. (2016). Russia, China, and the Push for "Digital Sovereignty". IPI Global Observatory (Hrsg.). Verfügbar unter: https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization, zuletzt zugegriffen am 12.09.2017.

Matzat, L. (2014). Kommentar: Zur Zukunft der Arbeit hat die Digitale Agenda nichts zu sagen. In: Netzpolitik.org, 25.08.2014. Verfügbar unter: https://netzpolitik.org/2014/kommentar-zur-zukunft-der-arbeit-hat-die-digitale-agenda-nichts-zu-sagen, zuletzt zugegriffen am 29.05.2017.

NPC – The National People's Congress of the People's Republic of China (NPC) (2015). wangluo anquan fa (cao an). Verfügbar unter: www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm, zuletzt zugegriffen am 12.09.2017.

ntv (2017a). Digitale Souveränität in Gefahr? IT-Profis warnen vor Microsoft. Verfügbar unter: www.n-tv.de/politik/IT-Profis-warnen-vor-Microsoft-article19786680.html, zuletzt zugegriffen am 29.04.2017.

ntv (2017b). Wikileaks enttarnt CIA-Programm – „Athena" spioniert jedes Windows aus. Verfügbar unter: www.n-tv.de/technik/Athena-spioniert-jedes-Windows-aus-article19853436.html, zuletzt zugegriffen am 29.05.2017.

Orange (2014). the future of digital trust. A European study on the nature of consumer trust and personal data. Verfügbar unter: www.orange.com/en/content/download/21358/412063/version/5/file/Orange+Future+of+Digital+Trust+Report.pdf, zuletzt zugegriffen am 28.04.2017.

Organisation for Economic Co-Operation and Development (OECD) (Hrsg.) (2017). Key Issues For Digital Transformation In the G20. Report prepared for a joint G20 German Presidency

/ OECD conference. Verfügbar unter: www.oecd.org/g20/key-issues-for-digital-transformation-in-the-g20.pdf, zuletzt zugegriffen am 24.04.2017.

Perrit, H. H., JR. (1998). The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance. In: Indiana Journal of Global Legal Studies, Vol. 5: Iss. 2, Article 4., S. 422–442. Verfügbar unter: www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1128&context=ijgls, zuletzt zugegriffen am 05.04.2017.

Ronzheimer, M. (2017). Datenschutz in der Industrie: Digitale Souveränität. In: taz.de, 11.11.2016. Verfügbar unter: www.taz.de/!5353390 (zuletzt aktualisiert am 21.05.2017), zuletzt zugegriffen am 29.05.2017.

Sassen, S. (1998). On the Internet and Sovereignty. In: Indiana Journal of Global Legal Studies, Vol. 5: Iss. 2, Article 9, S. 544–559.

Security Week (2016). Estonia's ‚Data Embassy' Could be UK's First Brexit Cyber Casualty, 10.08.2016. Verfügbar unter: www.securityweek.com/estonias-data-embassy-could-be-uks-first-brexit-cyber-casualty, zuletzt zugegriffen am 29.04.2017.

Steiner, F. (2014). Kommentar zur Digitalen Agenda: Leere Phrasen statt politischer Entscheidungen. In: heise.de, 20.08.2014. Verfügbar unter: www.heise.de/newsticker/meldung/Kommentar-zur-Digitalen-Agenda-Leere-Phrasen-statt-politischer-Entscheidungen-2297601.html, zuletzt zugegriffen am 29.05.2017.

Strittmatter, K. (2017). Schuld und Sühne. In: Süddeutsche.de, 19.05.2017. Verfügbar unter: www.sueddeutsche.de/politik/punkteregime-schuld-und-suehne-1.3514310?reduced=true, zuletzt zugegriffen am 29.05.2017.

tagesschau.de (2017). Digitale Agenda: Schulterklopfen – und weitermachen. Unter Mitarbeit von Ulla Fiebig. In: tagesschau.de. Verfügbar unter: www.tagesschau.de/inland/digitale-agenda-bilanz-101.html (zuletzt aktualisiert am 27.04.2017), zuletzt zugegriffen am 29.05.2017.

Tagscherer, U.; Christmann-Budian, S. (2013). Country report China. mKETsPL working document, Bd. 2013. Verfügbar unter: http://www.mkpl.eu/uploads/media/mKPL-_country_report_China.pdf, zuletzt zugegriffen am 28.04.2017.

The Government; Local Government Denmark; Danish Regions (2016). A Stronger and More Secure Digital Denmark – Digital Strategy 2016–2020. Verfügbar unter: www.digst.dk/~/media/Files/English/Ny-strategi-2016-2020/DS_Singlepage_UK_web.pdf, zuletzt zugegriffen am 29.04.2017.

United Nations (UN) (2016a). The right to privacy in the digital age. General Assembly, 16 November 2016. Verfügbar unter: https://documents-dds-ny.un.org/doc/UNDOC/LTD/N16/388/46/PDF/N1638846.pdf?OpenElement, zuletzt zugegriffen am 12.09.2017.

United Nations (UN) (2016b). Guidelines for Consumer Protection. Verfügbar unter: http://unctad.org/en/PublicationsLibrary/ditccplpmisc2016d1_en.pdf, zuletzt zugegriffen am 25.04.2017.

Wübbeke, J.; Meissner, M.; Zenglein, M. J.; Ives, J.; Conrad, B. (2016). Made in China 2025. The making of a high-tech superpower and consequences for the industrial countries. In: MERICS Papers on China 2016 (2). Verfügbar unter: www.merics.org/fileadmin/user_upload/downloads/China_Flash/161121_Handout_IndustrialInternet_Web.pdf, zuletzt zugegriffen am 29.04.2017.

3.3 Bildung als Voraussetzung digitaler Souveränität

Claudia Loroff, Ina Lindow, Michael Schubert

Soziodigitale Souveränität setzt Kompetenzen auf individueller Ebene voraus. Der vorliegende Beitrag zeigt auf, dass die drei aktivierenden Lehr-Lernformen des problem- und projektbasierten Lernens, des forschungs- sowie des arbeitsbasierten Lernens den Erwerb dieser Kompetenzen unterstützen können – vor allem dann, wenn digitale Medien einbezogen werden.

Für die unterschiedlichen Bildungsbereiche – die schulische und berufliche Bildung, die Hochschulbildung sowie die Weiterbildung – setzt die umfängliche und konsequente Umsetzung der drei Lehr-Lernformen unter Nutzung digitaler Medien verschiedene Neujustierungen voraus. Dabei steht das Bildungssystem insgesamt vor der Herausforderung, individuelle Lernwege zuzulassen und gleichzeitig Brüche auf Kompetenzebene und medialer Ebene zu vermeiden. Besonders wichtig sind dabei Lernarrangements, die die Kompetenzentwicklung durch unmittelbare Erfahrung erlauben.

Neue Anforderungen an Kompetenzen erfordern weitreichende Veränderungen unseres Bildungssystems

Soziodigitale Souveränität basiert auf vier Elementen (Stubbe 2017):

1. Kompetent durch Erfahrungen
2. Das große Ganze mitgestalten
3. Selbstbestimmung in der Datenwelt
4. Identität verantwortungsbewusst entfalten

Das erste Element betrifft besonders das Bildungssystem. Statt der Vermittlung von Faktenwissen wird im Kontext soziodigitaler Souveränität vor allem das erfahrungsbasierte Lernen in den Vordergrund gestellt.

Gleichzeitig führen stetig neue Möglichkeiten digitalen Wirkens im Zeitalter von Industrie 4.0 und Arbeit 4.0 zu einem fundamentalen und massiven Wandel in vielen Branchen: Die Märkte sind global, die Produktion wird passgenau auf die Kundenbedürfnisse ausgerichtet, Angebot und Nachfrage werden per Internet ausgehandelt, autarke Produktionseinheiten kommunizieren in der Fabrikhalle untereinander und

Produktionsprozesse werden ad hoc neugestaltet. Und in der Wissenschaft bieten immer umfangreicher zur Verfügung stehende Daten – kreativ kombiniert und ausgewertet – gänzlich neue Wege der Wissensgenerierung. Neue Forschungsfragen entstehen und verändern ganze Wissenschaftsbereiche. Zudem wird zunehmend in weltweiten Forschungsverbünden kooperiert, ohne dass sich die Beteiligten überhaupt je einmal persönlich getroffen haben müssten, und die Forschungsergebnisse werden online publiziert.

Um in dieser neuen digitalen Welt der Souverän zu sein, müssen dazu nötige Handlungskompetenzen auf der individuellen Ebene entwickelt, gefördert und deren Herausbildung in den Institutionen der Bildung unterstützt werden. Was ist also zu tun? Wirtschaft und Wissenschaft fordern eine stärkere Ausrichtung der Bildung auf Kompetenzen der Problemlösung, der Planung und Ordnung, wissenschaftliches Denken und Kreativität, die Fähigkeit zur Analyse und Kommunikation, starkes Verständnis von Medien und Technologien sowie die Kompetenz, in interdisziplinären Teams strukturiert und effizient zu arbeiten. Erkennbar wird, dass die digitale Souveränität in dieser neuen Welt maßgeblich auf dem folgenden Element beruht: zuvorderst auf Erfahrungen. Nur auf dieser Basis kann das Individuum am großen Ganzen mitgestalten, Selbstbestimmung in der Datenwelt erreichen und seine Identität verantwortungsbewusst entfalten. Das macht eine Neuausrichtung des Bildungssystems erforderlich.

An dem neuen Spektrum dieser Anforderungen hat die Abrufbarkeit klassischen Faktenwissens nur einen untergeordneten Anteil. Aneignen lassen sich die postulierten neuen Kompetenzprofile denn auch weniger auf althergebrachte Weise, sondern maßgeblich durch Lehr- und Lernmethoden, welche die Lernenden aktiv auffordern, sich in unterschiedliche Probleme und Forschungsbereiche hineinzudenken. Zu ihnen gehören vermehrt Lernformen, die auf Erfahrungen beruhen, wie das problem- und projektbasierte Lernen sowie ein forschungs- und arbeitsbasiertes Lernen in der Praxis.

Problembasiertes Lernen kann Lernende befähigen, deklaratives Faktenwissen und prozedurales Handlungswissen auf Alltagsprobleme anzuwenden. Prozesse der Problemlösung werden entsprechend in authentische Problemstellungen eingebettet (Merriënboer und Sweller 2005). Dabei werden Lernende wahlweise mit Schwierigkeiten konfrontiert, die entweder eine klare Lösung erfordern, oder mit solchen, die verschiedene Lösungsansätze und Perspektiven beinhalten (Jonassen 1997). In beiden Fällen erwerben Schüler oder Studierende an den Hochschulen ausgesprochene Problemlösefähigkeiten: analytische Fertigkeiten, Kompetenzen in der Planung und Steuerung von Prozessen, kreatives Geschick sowie Fähigkeiten der Lösungsimplementierung. Im Lernfeld zu lösende Probleme können dabei auch im Digitalen angesiedelt sein – dem Internet, in virtuellen Räumen oder in einer von digitalen Informa-

tionsangeboten überlagerten Realität (Augmented Reality). Lernende werden hierbei aufgefordert, Kompetenzen der Informationsrecherche und -validierung sowie digitale, mediale und technologische Lösungsansätze zu formulieren, zu programmieren oder zu entwerfen. Darüber hinaus müssen Lernende beim problembasierten Lernen häufig in Teams zusammenarbeiten und entwickeln dabei weitere kommunikative und soziale Fähigkeiten anhand von Kooperations-, Diskussions- und Aushandlungsprozessen unterschiedlicher Rollen oder Meinungen.

Der Fokus des *forschungsbasierten Lernens* liegt demgegenüber auf der Verschränkung theoretischer und praktischer Aspekte des Erkenntnisprozesses. „Forschendes Lernen zeichnet sich dadurch aus, dass Lernende den Prozess eines Forschungsvorhabens […] von der Entwicklung der Fragen und Hypothesen über die Wahl und Ausführung der Methoden bis zur Prüfung und Darstellung der Ergebnisse in selbstständiger Arbeit oder in aktiver Mitarbeit […] gestalten, erfahren und reflektieren." (Huber 2009, S. 11) Viele Forschungsfragen, insbesondere in den MINT-Fächern (Mathematik, Informatik, Naturwissenschaft und Technik), fordern die Lernenden auf, sich technologische und programmiertechnische Kenntnisse zu erarbeiten, auch etwa hinsichtlich eines auszugestaltenden Versuchsaufbaus und dessen Durchführung sowie der Datenerhebung und -auswertung. Dabei gewinnen die Lernenden nicht nur wissenschaftlich-technologische Handlungskompetenzen im Medienbereich, sondern entwickeln während der Bearbeitung von Forschungsfragen auch, ähnlich wie beim problembasierten Lernen, eine starke Eigenständigkeit sowie emotionale und soziale Kompetenzen im Team.

Im Rahmen des *arbeitsbasierten Lernens* sollen Arbeitsprozesse als Lernchancen wahrgenommen und genutzt werden. Lernende identifizieren, behandeln und reflektieren hierbei also symptomatische Problemstellungen in der Arbeitswelt. Erworbenes theoretisches Faktenwissen wird dabei direkt in die Praxis übertragen und am Arbeitsplatz angewendet. In der Ausbildung ebenso wie auch in der Weiterbildung bearbeiten Lernende dabei häufig ein relevantes lernhaltiges Projekt im realen betrieblichen Kontext. Ein solches Projekt bereiten die Lernenden in der Regel selbst vor, planen es, führen es durch bzw. implementieren es und werten es aus. Hierdurch sollen sie alltägliche Arbeitsprozesse, explizites Wissen in implizites Anwendungswissen überführen. Methodische Kompetenzen in Hinblick auf die Konzipierung, Durchführung und Auswertung realer Projekte aus dem Arbeitskontext stehen dabei im Fokus. Da digitale Medien, Werkzeuge und Systeme in der heutigen Arbeitswelt kaum noch wegzudenken sind, werden sie im arbeitsbasierten Lernen automatisch zum festen Lerngegenstand und fordern Lernende heraus, sich aktiv mit ihnen auseinanderzusetzen. Somit werden vor allem praktische Kompetenzen im Umgang mit digitalen Arbeitsumgebungen systematisch gestärkt. Ausbildende und auch Mentoren begleiten und unterstützen solche arbeitsbasierten Lernprozesse.

Die umfängliche und konsequente Umsetzung dieser drei Lehr- und Lernformen setzt über alle Bildungsbereiche hinweg weitreichende Modifikationen institutionellen Lehrens und Lernens voraus. Diese Modifikationen lassen sich wie folgt zusammenfassen:

1. Ein Verständnis der Lehrenden von ihrer Rolle und Funktion, das weniger auf die Vermittlung von klar definierten und fixierten Wissensbeständen setzt, denn diese können leicht im digitalen Raum vorgehalten werden. Stattdessen steht künftig die Begleitung und Unterstützung der Lernenden in der Auseinandersetzung mit lebensnahen, authentischen Frage- und Problemstellungen im Vordergrund. Dieses Rollenverständnis umfasst auch die Bereitschaft zur stetigen professionellen, interdisziplinären Weiterentwicklung in Lehr- und Lerngemeinschaften sowie die kooperative Planung und Gestaltung von Lerneinheiten unter Einbezug verschiedener Akteure innerhalb und außerhalb der jeweiligen Bildungsinstitution. Als Ergebnis dieses Orientierungsprozesses wird sich eine neue Lehrkultur in den Bildungsinstitutionen etablieren.

2. Eine Haltung der Lernenden, die das passive Rezipieren von Wissensinhalten und die bedenkenlose Übernahme scheinbar gesicherter und einfacher Wahrheiten ablehnt und stattdessen die Bereitschaft zu einem selbstbestimmten, planvollen und kritisch-hinterfragenden Lernen umfasst. Die Entwicklung dieser Haltung ist frühzeitig anzuregen, über die Bildungsbiografie aufrechtzuerhalten und zu stärken. Die Verantwortung für den eigenen Lernprozess nimmt hierbei stetig zu. Analog zum modifizierten Lehrverständnis steht diese veränderte Haltung und Rolle von Lernenden für eine neue Lernkultur.

3. Ein Bekenntnis zur Organisationsentwicklung, das – analog zu den veränderten Anforderungen an Lehrende und Lernende – zu planvollem und strategischem Handeln herausfordert, kooperativ ausgerichtet ist und Synergien zwischen verschiedenen Akteuren herstellen und nutzen kann sowie auf einem Selbstverständnis gründet, das die Institution als lernende Organisation anerkennt und somit Ausdruck einer institutionellen Lernkultur ist. Gegenwärtig erscheint vor allem eine Erweiterung traditioneller Rollen und Funktionen in den einzelnen Bildungseinrichtungen notwendig: Hardware und Software beispielsweise müssen zu bestimmten Zeitpunkten und in einer bestimmten Form Lernangebote in einem bestimmten Umfang, in definierter Größe und Qualität bereitstellen. Dabei muss auch geregelt sein, welche Lernangebote wann im Prozess benötigt werden, wer Zugriff auf diese Angebote hat, Veränderungen vornehmen darf oder soll und wer im Störungsfall Hilfe leisten kann.

4. Die Öffnung von Bildungsbereichen und das Zulassen individueller Bildungsbiografien. Den einzelnen Bildungsinstitutionen muss hierzu mehr Offenheit und Autonomie bei der Einbindung von Lernenden, aber auch bei der Gestaltung und

Bescheinigung von Lerninhalten gewährt werden. In Abhängigkeit vom Bildungsbereich kann diese Modifikation dazu führen, dass erst im Nachhinein festgestellt und bescheinigt wird, was gelernt wurde.

5. Die konsequente Einbindung des Digitalen in die vorhandenen Bildungsumwelten. Digitale Lernwerkzeuge und Lernkonzepte müssen überall dort eingesetzt werden, wo sie den Lernenden einen qualitativen Mehrwert bieten, Bildungschancen öffnen und eine Teilhabe ermöglichen. Medien und Technologien müssen aber auch selbst Gegenstand von Lerninhalten werden, um Lernende zu befähigen, als mündige Bürger innerhalb ihres digitalen Raums heranzuwachsen.

Wie die Lehr-Lernformen des problem- und projektbasierten Lernens sowie des forschungs- und arbeitsbasierten Lernens in den einzelnen Bildungsbereichen funktionieren und wie sich ihre Potenziale durch die Nutzung von digitalisierten Lernangeboten noch besser heben lassen, wird im Folgenden dargelegt und diskutiert. Die einzelnen Kapitel gehen hierbei auf die unterschiedlichen Entwicklungsstände der einzelnen Bildungsbereiche in Hinblick auf die Implementation der Lehr-Lernformen und die Nutzung digitaler Technik ein.

Schulische Bildung

Begründung für eine neue Lehr-Lernkultur

Für den Erwerb von Kompetenzen, die nicht ausschließlich dem Duktus traditionell definierter Unterrichtsfächer unterliegen und die Mündigkeit der Lernenden zur Prämisse haben, erscheint im schulischen Kontext vor allem das forschungsbasierte Lernen bedeutsam. Die Deutsche Kinder- und Jugendstiftung stellt für das forschungsbasierte Lernen in der Schule fünf Gründe heraus (DKJS):

- Erstens: Die Schülerinnen und Schüler können das Lernen lernen; sie werden so dazu befähigt, ihr Wissen lebenslang selbstständig zu erweitern.
- Zweitens: Forschungsbasiertes Lernen ist individualisiertes Lernen, das Kindern und Jugendlichen Verantwortung und Gestaltungsraum für ihre Lernprozesse ermöglicht.
- Drittens: Indem die eigenen Ideen und Lösungswege in den Mittelpunkt rücken, erfahren die Lernenden, dass sie etwas können; sie erleben Selbstwirksamkeit.
- Viertens: Forschungsbasiertes Lernen fördert die Kommunikations- und Teamfähigkeit; gemeinsames gegenstands- und zielorientiertes Überlegen und Diskutieren in der Gruppe wird zu einer Gelingensbedingung von Lernhandeln.
- Fünftens: Forschungsbasiertes Lernen verbindet Schule mit der Lebenswelt der Schülerinnen und Schüler; die Lerninhalte werden spannend und erfahrbar und

ermöglichen vielfältige Bezüge zu anderen Fächern, zu anderen Themenbereichen und nicht zuletzt zur Berufswelt.

Von anderen Bildungsbereichen unterscheidet sich das forschungsbasierte Lernen in der Schule insbesondere dadurch, dass die gewonnen Erkenntnisse in der Regel objektiv schon bekannt sind. Das macht die Lehr-Lernform für den Kompetenzerwerb der Kinder und Jugendlichen nicht weniger bedeutsam. Ganz im Gegenteil. Forschungsbasiertes Lernen fordert die Schüler heraus und ermöglicht es ihnen zugleich, eigene Fragen zu stellen und zielgerichtet sowie eigenständig nach Lösungen zu suchen. Die Lernenden sind angehalten, Dinge und Sachverhalte zu hinterfragen, den Willen zu entwickeln, durch Untersuchen und Nachforschen eigenständig und planmäßig nach Antworten zu suchen und schließlich ihre Erkenntnisse zu überprüfen sowie für andere nachvollziehbar zu machen (Messner 2009, S. 22). Die Wissenschaftsorientierung nimmt dabei mit steigendem Alter der Schülerinnen und Schüler stetig zu; sie gipfelt im wissenschaftspropädeutischen Unterricht der Sekundarstufe II.

Die Kompetenzen, die Schüler hierbei entwickeln, stimmen mit den Anforderungen überein, die für digitale Souveränität entscheidend sind: Probleme erkennen und (kreativ) lösen, Eigeninitiative entwickeln und aufrecht erhalten, sich in offenen, unüberschaubaren, komplexen und dynamischen Situationen selbstorganisiert zurechtfinden. Damit bedingt und fördert forschungsbasiertes Lernen in der Schule die Etablierung einer Lehr-Lernkultur, die Kinder und Jugendliche früh an wissenschaftliche Fragen und Methoden heranführt und der Ausbildung von fachlichen wie überfachlichen Methodenkompetenzen und dem Erwerb von Sozial- und Selbstkompetenz einen größeren Wert beimisst als die ausschließliche Anhäufung tradierter Wissensbestände. Digitale Medien wie Blogs, Chat-Tools, Sharing-Plattformen und Online-Literaturdatenbanken können die Entwicklung einer derartigen Lehr-Lernkultur unterstützen: Sie bieten die Möglichkeit, Lehr-Lernräume weiter auszudehnen und Lehr-Lernprozesse räumlich wie zeitlich zu flexibilisieren und zu dezentralisieren (vgl. Kergel und Heidkamp 2015, S. 73).

Der konsequente Einbezug digitaler Medien wirkt darüber hinaus auch auf einer zweiten Ebene: Er ermöglicht es den Lernenden, sich einen souveränen und mündigen Umgang mit digitaler Technik anzueignen. Damit schafft er für Schüler eine wichtige Grundlage, sich in einer zunehmend digitalisierten Welt – sei es im beruflichen wie im privaten Kontext – künftig zurechtfinden zu können.

Institution Schule neu gedacht

Erfolgt forschungsbasiertes Lernen unter Einsatz digitaler Medien wie Lernplattformen und den dazugehörigen Werkzeugen, den Lerntools, öffnen sich neue Räume. Das klassische Bild einer dozierenden Lehrperson und passiv rezipierender Schüler

verschwindet. Gleichzeitig machen Lern- und Forschungsszenarien, zu denen sich Gruppen von Lernenden zusammenfinden, Räume notwendig, die einen Rückzug gestatten, kreative Denk- und Austauschprozesse zulassen und dann wieder eine Präsentation der Erkenntnisse und Ergebnisse und ihre Würdigung ermöglichen. Diese Räume arrangieren ein Verschmelzen der virtuellen und realen Welt, wodurch die Bearbeitung von Fragestellungen durch Schüler nicht an die physischen Grenzen des Schulgebäudes stößt, sondern sich weit über diese hinaus erstrecken kann. Die Formulierung komplexer und lebensnaher Fragestellungen führt außerdem dazu, dass sich Fachgrenzen auflösen oder zumindest eine Reorganisation erfahren. Lehrende wie Lernende erhalten in diesen Räumen ein hohes Maß an Gestaltungsspielraum.

Diese Änderungen auf der Ebene der Einzelschulen setzen eine Schule voraus, die durch ein hohes Maß an Autonomie flexibel und bedarfsgerecht auf die Anforderungen und Auswirkungen des digitalen Wandels in der Gestaltung von Lehr-Lernprozessen reagieren kann. Bedenkt man, dass bisherige Reformen im Schulbereich vor allem Top Down – also von oben nach unten – initiiert und aus Sicht vieler Betroffener sehr schlagartig und unvermittelt umgesetzt werden mussten und deshalb teilweise nur unter großen Reibungsverlusten Eingang in den schulischen Alltag fanden, erscheint ein umfassendes Change Management notwendig. Für derart tiefgreifende Veränderungen, wie sie digital gestütztes, forschendes Lernen mit sich bringt, sind alle Betroffenen einzubeziehen. Sie müssen bei ihrer Arbeit begleitet, qualifiziert und unterstützt werden. Den Schulen muss Schritt für Schritt mehr Autonomie und Gestaltungsraum, auch finanzieller Art, eingeräumt werden. Und bei allen Akteuren muss nachhaltig ein Bewusstsein dafür geschaffen werden, dass Schule eine lernende Organisation sein muss.

Neue Rollen für Lernende und Lehrende

Die Lehrenden stellt digital gestütztes, forschendes Lernen vor didaktische und methodische Herausforderungen. Neu ist das Agieren in professionellen Lehr- und Lerngemeinschaften zur gemeinsamen und arbeitsteiligen Planung und Gestaltung von Lehr-Lernprozessen sowie zum Austausch und zur gemeinsamen Reflexion etwa über die individuellen Lernfortschritte der Schüler und Fragen der Leistungsbeurteilung. Da die Bearbeitung lebensnaher und offener Fragestellungen, die forschungsbasiertes Lernen kennzeichnet, in der Regel über die Grenzen eines Faches hinausgeht, sind auch die Lehrenden angehalten, über traditionelle Fächergrenzen hinweg zusammenzuarbeiten und zugleich einen Bezug zwischen Lerninhalten einzelner Fächer durch die Schüler nicht nur zu ermöglichen, sondern auch zu initiieren.

Nicht weniger komplex sind die Auswirkungen des digital gestützten, forschungsbasierten Lernens auf die einzelnen Kinder und Jugendlichen – in ihrer Rolle als Lernende werden sie gestärkt und gefordert zugleich:

- Gestärkt, weil sie freier agieren können; gefordert, weil mit dieser Freiheit auch ein höheres Maß an Selbstregulation und Verantwortung für den eigenen Lernprozess einhergeht.
- Gestärkt, weil sie bei der Bearbeitung von Frage- und Problemstellungen eigenständig Zusammenhänge herstellen und Problemlösungen finden dürfen; gefordert, weil eben dies auch anstrengend ist und die Erweiterung von Möglichkeiten immer auch die Herausforderung einschließt, mit Widersprüchen und Unsicherheiten umgehen zu müssen.

Hierbei ändert sich auch die Rolle der Lehrenden. Anerkennend, dass Lernen eine soziale Konstruktionsleistung und Wissen veränderbar bzw. kontextabhängig ist, wird die Lehrperson vielfach zum Impulsgeber, Berater und Begleiter.

Allerdings kommen Lehrende auch weiterhin nicht umhin zu bewerten. Spätestens in diesem Punkt stößt die emanzipative Selbstbestimmung der Schüler an Grenzen. Das heißt jedoch nicht, dass nicht auch die schulische Leistungsbewertung eine Veränderung erfahren kann. Leistungen forschenden Lernens ließen sich, insbesondere wenn sie digital erbracht wurden, beispielsweise mithilfe von E-Portfolios auch formativ erfassen (Kergel und Heidkamp 2015, S. 73). Lernfortschritte könnten auf diese Weise für die Lehrenden wie für die Lernenden selbst sichtbar gemacht und zugleich gewürdigt werden. Darüber hinaus wären Hinweise und Impulse für die weitere Lehr-Lernprozessgestaltung transparent und nachvollziehbar generiert. Der Schule inhärente Widerspruch, Lernende zu Selbstständigkeit und Unabhängigkeit zu erziehen, obgleich sie sich in Abhängigkeit von der unterrichtenden und bewertenden Lehrperson befinden, lässt sich durch digital gestütztes forschendes Lernen demnach nicht vollständig auflösen, wohl aber erheblich relativieren.

Berufliche Bildung

Mit der Digitalisierung werden technologische Neuerungen, neue Geschäftsideen, digitale Wertschöpfungsketten, Globalisierung und Internationalisierung verbunden. Digitalisierung ist dabei „Enabler" und „Disruptor" zugleich: Nicht nur Prozesse, sondern ganze Systeme verändern sich oder entstehen neu. Entsprechend muss in Hinblick auf digitale Souveränität allem voran die Vermittlung von planungs- und prozessorientiertem, systemischem und domänenübergreifendem Denken im Mittelpunkt stehen. Das geht aber nur, wenn Problemlösekompetenzen, Planungs- und Organisationskompetenzen, Kreativität, Analysekompetenzen, Kommunikationskompetenzen, Teamfähigkeit und Medienkompetenz konsequent in der Berufsbildung gefördert werden.

So beschreibt das Bundesinstitut für Berufsbildung (BIBB) in seinem Beitrag „Industrie 4.0 und ihre Auswirkung auf die Arbeitswelt", dass Arbeit von dem Einzelnen flexi-

bel, eigenständig und vor allem zunehmend projektorientiert zu leisten sei. Neben fachlichen Kompetenzen gehe es um grundlegende „21st-Century-Skills" wie die Fähigkeit zu virtueller Zusammenarbeit in Teams, die sich aus unterschiedlichen Verantwortlichkeiten und Experten zusammensetzen. Deshalb müssen heutige Mitarbeitende dazu in der Lage sein, ihr Wissen selbstständig und bedarfsorientiert – auch am Ort des Handelns – zu erwerben. Digitale Medien spielen hierbei eine wichtige Rolle. In der Erstausbildung sieht das BIBB für die Qualität und Attraktivität der Lehr- und Lernprozesse in den Betrieben in erster Linie das Ausbildungspersonal verantwortlich. Von seiner berufs- und medienpädagogischen Kompetenz hänge es ab, inwiefern dann die Anforderungen der Digitalisierung zeitgemäß in handlungsorientierte Bildungskonzepte übertragen werden können. Zugleich müssen auch die Bildungspläne der Berufsschulen mit Blick auf die neuen Herausforderungen rund um die Themenfelder Internet der Dinge, Wissensmanagement, smarte Produkte und E-Commerce – lernortübergreifend verzahnt – mit den Ausbildungsbetrieben überarbeitet werden (siehe hierzu BIBB).

Ausbildung steht traditionell dem arbeits- und problembasierten Lernen nah

In der beruflichen Bildung wurde und wird traditionell schon immer die Arbeit als Lernfeld systematisch genutzt. Modernisierte Ausbildungsordnungen[16] und neue Ausbildungsberufe orientieren sich an einem sich ständig verändernden Bedarf am Ausbildungsort und versuchen, diesen flexibel in die Curricula einzubinden. Jedoch gibt es noch immer eine starke Differenz zwischen dem, was in den Ausbildungsbetrieben stattfindet, und dem, was im Unterricht der Berufsschule vermittelt wird. So setzt die Berufsschule beispielsweise noch immer stark auf das Aneinanderreihen von Grundlagen und Lehrgängen, die dann in einer Prüfungsvorbereitung münden. Auszubildende müssen jedoch frühzeitig eine Einbindung in die systemischen Prozesse einer digitalisierten Arbeitswelt erfahren, damit sie die sehr komplexen, oft systemübergreifenden Arbeitsprozesse verstehen und in ihnen agieren können (vgl. Odendahl 2017).

Integration der Systemkomponente in die Ausbildung bringt neue Qualität

Die Forderung nach lernortübergreifenden und mit Ausbildungsbetrieben verzahnten Bildungsplänen muss um die oben beschriebene Systemkomponente erweitert

[16] *Das Bundesinstitut für Berufsbildung (BIBB) hat seit 2003 insgesamt 243 Ausbildungsordnungen überarbeitet und an die aktuellen wirtschaftlichen, technologischen und gesellschaftlichen Anforderungen angepasst. Hier wurden 206 Ausbildungsordnungen modernisiert und 37 Ausbildungsberufe neu geschaffen, weitere Überarbeitungen laufen (Verfügbar unter: www.bibb.de/de/pressemitteilung_50710.php, zuletzt zugegriffen am 26.07.2017).*

werden. Welche Auswirkungen die Berücksichtigung der Systemkomponente für Berufsbilder hat, ob hier der Trend zu höherer Spezialisierung oder eher zu Generalisten geht, ist derzeit noch nicht absehbar. Didaktisch lässt sich die zu integrierenden Systemkomponente in der Ausbildung begegnen, indem der Arbeitskontext selbst als Lerngegenstand genutzt wird. Genau hier setzen problem- und arbeitsbasiertes Lernen an: Die Auszubildenden begeben sich in die Systeme, definieren, planen und bearbeiten Projekte und reflektieren lernend ihre Arbeit. Ausbildenden und Lehrenden an Berufsschulen obliegt es hierbei, die Auszubildenden in diesen Prozessen zu begleiten, zu unterstützen und mit ihnen gemeinsam das Gelernte zu reflektieren. Freiräume hierfür lassen sich dadurch gewinnen, dass die reine Wissensvermittlung auf das Nötigste reduziert und durch digital bereitgestellte und individuell abrufbare Lernmodule oder durch Recherchen im Internet begleitet wird. Die reine Wissensvermittlung wird aufgrund der Verfügbarkeit von Informationen und ihrer oftmals geringeren Halbwertszeit künftig ohnehin eine immer kleinere Rolle einnehmen.

Die Integration der Systemkomponente in die Ausbildung unterstützt auf diese Weise maßgeblich die Vermittlung eines system- und domänenübergreifenden Denkens. Das bereits traditionell verankerte Lernen am Ausbildungsort erfährt so über die verschiedenen Bildungsorte hinweg eine neue Qualität.

Digitalisierung bietet vielfältige Möglichkeiten, die Prozesse zu unterstützen, wie etwa

- durch Konzepte des „Flipped Classroom“[17] oder durch virtuelle Labore zum Ausprobieren,
- durch die Verbindung von Auszubildenden und Ausbildenden zur fortwährenden Aktualisierung der Anforderungen der realen Arbeitskontexte und zur Abstimmung der Projektarbeiten sowie der Online-Unterstützung von Gruppenarbeit. Hierbei können auch voneinander weit entfernte Auszubildende gemeinsam ein Thema bearbeiten und dabei betreut werden. Und schließlich
- dadurch, dass auf Ressourcen örtlich entfernter Ausbildungsstätten digital zugegriffen werden kann – sei es auf Inhalte, auf einen 3D-Drucker oder CNC-Fräsmaschinen.

[17] *Der Begriff „Flipped Classroom“ bezeichnet eine Unterrichtsmethode, in der die Lerninhalte durch die Schülerinnen und Schüler zu Hause erarbeitet werden und die Anwendung des Gelernten in der Schule stattfindet.*

Durch Digitalisierung lässt sich Ausbildung völlig neu denken

Wie Digitalisierung es ermöglicht, Ausbildung neu zu denken, wird im Folgenden am Beispiel von Ausbildungsverbünden sowie überbetrieblichen Bildungsstätten[18] exemplarisch vorgestellt.

Ausbildungskooperationen erfolgen meist dann, wenn ein Ausbildungsort nicht alle für eine Ausbildung nötigen Kompetenzen vermitteln kann. Bisher mussten Ausbildungsstätten hierfür nah beieinander liegen. Durch Digitalisierung kann nun eine Ausbildung im Verbund auch solche Ausbildungsstätten zusammenführen, die weit voneinander entfernt sind. Dabei verändert sich der Fokus der Ausbildungskooperation. Ging es bisher vor allem darum, die Partner so zusammenzustellen, dass alle Ausbildungsinhalte vermittelt werden konnten (Defizitdenken), kann eine Ausbildungskooperation mittels Digitalisierung und mobilem Arbeiten nun so gestaltet werden, dass nur Akteure beteiligt sind, die am besten zur Bearbeitung eines Ausbildungsprojekts – im Sinne des problembasierten Lernens – geeignet sind. Das bedeutet, einen qualitativen Sprung nach oben vollziehen zu können.

Es wäre auch denkbar, dass Auszubildende im Rahmen einer Problemlösung auf eine Ausbildungsstätte in einem Netzwerk zugreifen, die eigentlich gar nicht vorgesehen war, aber optimal bei der Problemlösung unterstützen kann, sofern relevante Informationen zum Beispiel über eine Plattform digital verfügbar sind und hinsichtlich Zugang, Qualität, Anerkennung oder auch Anrechnung definierte Kooperationsbeziehungen bestehen. Ähnliches kann für Berufsschulen und überbetriebliche Berufsbildungsstätten gelten. Zudem ist es denkbar, dass Ausbildungsverbünde sich künftig durch die Integration etwa von Zulieferern oder kooperierenden Forschungseinrichtungen in die Ausbildung an bestehenden Systemen orientieren, um das Systemverständnis und domänenübergreifendes Denken zu fördern.

[18] *Überbetriebliche Berufsbildungsstätten (ÜBS) ergänzen die betriebliche Ausbildung in vielen Branchen durch praxisnahe Lehrgänge, insbesondere wenn KMU nicht alle notwendigen Ausbildungsinhalte selbst vermitteln können. ÜBS sollen zu Kompetenzzentren weiterentwickelt werden. Hier ordnet sich auch das Sonderprogramm „ÜBS-Digitalisierung" ein: Das Bundesinstitut für Berufsbildung (BIBB) unterstützt die ÜBS dabei, ihre Qualifizierungsangebote so anzupassen, dass KMU den größtmöglichen Nutzen aus der Digitalisierung ziehen können (Verfügbar unter: www.bibb.de/uebs-digitalisierung, zuletzt zugegriffen am 26.07.2017).*

Akademische Bildung

Forschungsbasiertes wie auch problembasiertes Lernen erfährt in den vergangenen Jahren eine zunehmende Bedeutung im tertiären Bildungssektor. In Hinblick auf die im Kontext digitaler Souveränität bedeutsamen Kompetenzanforderungen bedarf es bereits in den ersten Studienjahren an Fachhochschulen und Universitäten stetig größer werdender Experimentier- und Problemlöseräume, in denen Studierende die Chance erhalten, Verantwortung für ihr wissenschaftliches, problemlösendes und kreatives Denken und Handeln zu übernehmen. Hochschulleitende wie Hochschullehrende sind hierbei aufgefordert, durch entsprechende organisatorische und strukturelle Veränderungen, diesen Anforderungen gerecht zu werden, eine engere Verzahnung von Lehre, Forschung, Wissenstransfer und Praxis zu ermöglichen sowie passende Lehr- und Prüfungsszenarien zu entwickeln. Um Qualitäts- und Effizienzziele in der Lehre zu erreichen sowie die akademischen Medienkompetenzen der Studierenden zu stärken, sind digitale forschungs- und problembasierte Lehr- und Lernmethoden mit technologisch-medialen Inhalten ein vielversprechender Ansatz.

Aufbauend auf den bereits erworbenen schulischen Kompetenzen hat forschungsbasiertes Lernen an Hochschulen zum Ziel, Studierende an aktuelle Forschungsthemen und wissenschaftliches Arbeiten im Kontext fachlich prägender Theorien heranzuführen. Aktuelle wissenschaftliche Themen und praktische Forschung können so miteinander verbunden werden. Problembasiertes Lernen an Hochschulen soll Studierende an aktuelle, vor allem technische Entwicklungen heranführen und dabei neueste Innovationen und Erkenntnisse mit praktischen Fragestellungen verbinden. Beiden Lehr- und Lernformen ist gemein, dass sie, im Gegensatz zu Anwendungsszenarien in Schule und Berufsschule, einen starken Fokus auf neue Forschungsfragen und Probleme mit hohen Innovationspotenzialen setzen. Sind zu erforschende Erkenntnisse und zu erreichende Lösungen in Schulen und Berufsschulen oftmals objektiv im Vorfeld bekannt, sollen sich Studierende mit ansteigender Semesterzahl zunehmend mit genuin neuen Forschungs- und Problemgegenständen beschäftigen. Dadurch erwerben Studierende eine grundlegende, im akademischen Kontext wichtige Kompetenz: das Aushalten und Aushandeln von multiplen Perspektiven, von Unsicherheit und Komplexität. Auf der Ebene der Kommunikationskompetenzen werden Studierendengruppen dadurch in komplexe Situationen gebracht, die ein hohes Maß an argumentativen sowie objektiven Entscheidungsfähigkeiten in ihrer Kooperation und Arbeitsteilung erfordern.

Sind Forschungs- und Problemgegenstände mit Unsicherheit und multiplen Perspektiven behaftet, bedeutet dies auch, dass technologische Umgebungen und mediale Werkzeuge unbekannt sind, mitunter aber überhaupt noch nicht entwickelt wurden. Studierende sind hierbei aufgefordert, proaktiv nach neuen Technologien und Werk-

zeugen zu suchen, diese sinnvoll zu evaluieren und einzusetzen, sodass sie ihre Forschungsvorhaben und Problemstellungen bewältigen können.

Das Heben von Wissenspotenzialen auf allen Hochschulebenen

Forschungs- und problembasierte Lehr- und Lernformen sind an den Hochschulen nicht gänzlich unbekannt. Besonders an Fachhochschulen, die traditionell stärker anwendungsorientierte und berufsbildende Studiengänge anbieten und enger mit der Wirtschaft verknüpft sind, sind problem- und projektbasierte Lehrformen kein Neuland. Aber auch an Universitäten wird das forschungs- und problembasierte Lernen bereits eingesetzt, allerdings nur zu geringen Anteilen. Widerstände aus den etablierten Fakultäten sind hier allerorts spürbar. Es bedarf deswegen großer Anstrengungen, die einzelnen Akteure – die Hochschulleitungen, Fakultätsleitungen, Lehrenden und Lernenden – von den Vorteilen dieser Lehr- und Lernformen zu überzeugen. Die Umsetzung forschungs- und problembasierten Lehrens bedeutet im Kern die Chance für Hochschulen, theoretisch geleitete Lehre, Forschung, Wissenstransfer und Praxis stärker miteinander zu verzahnen. Ist eine Hochschule gewillt, diese vier Handlungsfelder systematisch miteinander zu kombinieren, ließen sich größere Innovationspozentiale schöpfen und auf gesellschaftliche Forderungen besser eingehen. Dafür bedarf es eines Umdenkens auf höchster Hochschulebene: Hochschulleitungen müssen geeignete Strategien und ein Change Management implementieren, das ein ganzheitliches, wissenschaftliches und lösungsorientiertes Denken in den Fokus rückt. Hier kann es, auch ganz unabhängig von Digitalisierungsaspekten, zu einer starken Profilbildung für die Hochschulen kommen.

Lernbegleiter und Studierende – eine gute Forschergemeinschaft

Für die Lehrenden bedeutet die Umstellung der Lehr- und Lernmethoden eine Umstellung ihrer Tätigkeiten. Anstatt sich auf die Vermittlung der reinen Theorie zu konzentrieren, sind die Lehrenden aufgefordert, sinnhafte realitätsnahe Probleme zu erfinden, Projekte aus der Wirtschaft zu akquirieren oder studentische Forschungsräume zu schaffen, in denen Studierende die erlernte Theorie wissenschaftlich bzw. lösungsorientiert durchdringen können. Entsprechend werden Lehrende zu Lernbegleitern und müssen dadurch didaktisch einen anderen Ansatz verfolgen, denn Lehre und Forschung erfahren dabei eine zunehmende Verschmelzung (vgl. „Inquiry Learning“ bei Hickman 2004). Auch wenn dies zunächst einen Mehraufwand bedeutet, können Dozenten erheblich von den Lehr-und Lernmethoden profitieren, beispielweise indem sie Frage- oder Problemstellungen aus ihrem eigenen Lehrstuhl und von eigenen Kooperationen mit in die Lehre bringen. Anstatt lediglich mit einer kleinen wissenschaftlichen Mitarbeitergruppe an den eigenen wissenschaftlichen Problemstellungen zu arbeiten, können Studien- und Lösungsansätze durch die große Anzahl an Studierenden potenziert werden. Kombinationen mit anderen Studienfächern

und Kollegen bieten die Chance einer ersten interdisziplinären, wissenschaftlichen Zusammenarbeit, möglicher vertiefter Kooperationen, sinnvoller Arbeitsteilung und eines höheren wissenschaftlichen Outputs. Auch wenn es bereits in vielen Studiengängen erste Ansätze gibt, praktische Kurse wissenschaftlichen Arbeitens zu implementieren, ist eine prinzipielle fächer- und semesterübergreifende Umstellung der Lehr- und Lernmethoden oder gar eine interdisziplinäre Zusammenarbeit über Fachspezialisierungen hinweg noch zu selten.

Studierende übernehmen im Rahmen dieser Lehr- und Lernformen stärker Verantwortung für ihren eigenen Lernprozess und erfahren dadurch ein hohes Maß an Selbstbestimmtheit insbesondere in Bezug auf die Fähigkeit, eigene Interessensgebiete, Fragestellungen und Ziele aufgrund von Selbsterfahrungen bestimmen zu können. Hinzu kommt Selbstregulation, also die Fähigkeit, den selbstgesteckten Zielen planvoll, reflektierend und korrigierend zu folgen sowie eine hohe Selbstwirksamkeitserwartung (Bandura 1977). Damit wird das Lehren zunehmend individualisiert und lerner- bzw. lerngruppenzentriert. Dies bedeutet auch, dass die Prüfungsverfahren stärker individualisiert und sich an den thematischen Kenntnissen der Lernenden orientieren müssen. Hochschulen sollte es deshalb ermöglicht werden, ihre Prüfungsverfahren adaptiv an die Studierenden und Studentengruppen anpassen zu können. Dabei sind Prüfungsszenarien zu entwerfen, die den individuellen, gruppenspezifischen und situativen Umständen Rechnung tragen.

Durch die neuen Lehr- und Lernformen entsteht zwischen Lehrenden und Lernenden eine neue Rollenkonstruktion: Studierende unterstützen ihre Dozierenden in der Lehre bei ihren Forschungsaktivitäten; Dozierende helfen ihren Studierenden bei der Entwicklung und Beantwortung ihrer Problemstellungen und Forschungsfragen. Somit entstehen schon frühzeitig Forschergemeinschaften zwischen studentischen Forscherteams und ihren sie anleitenden Lehrenden, die auch semesterübergreifend Bestand haben können. Über die Verbindung von Lehre und Forschung hinaus könnten auch Wissenstransfer und Praxis eine ganz neue, zentralere Rolle in den Forschergemeinschaften einnehmen. Sind Studierende beispielsweise stärker in Forscherteams des Lehrstuhls integriert und tragen aktiv zum neuen Erkenntnisgewinn bei, könnten sie auch stärker in Publikations- oder Präsentationstätigkeiten eingebunden werden. Studierende könnten so schneller mit der Wissenschaftswelt in Berührung kommen und auch in den entsprechenden Wissenschaftsforen ihre Kommunikationsfähigkeiten stärken. Anderweitige Prüfungsformen würden für die Forscherteams damit obsolet.

Lehrende haben umgekehrt die Chance, intensiver mit ihren Studierenden zusammenzuarbeiten. Sie betreuen studentische Forscherteams und steuern dabei in einer größeren Breite ihre eigene Forschung sowie den Wissenstransfer ihrer Forschung. Eine individuelle Betreuung wird auch bei einer Umstellung zu forschungs- und pro-

blembasierten Lernmethoden eine Herausforderung bleiben. Deswegen sollten Dozenten dazu befähigt werden, forschungs- und problembasierte Lehr- und Lernräume zu gestalten, effizient mit ihren Studierenden zu kommunizieren und deren Lern- und Arbeitsfortschritte so zu analysieren, dass sie gezielt Hilfestellungen anbieten können.

Selbstbestimmtes proaktives Lernen und Forschen im digitalen Raum

Innovationen in der Digitalisierung können die Umstellung hin zu forschungs- und problembasierten Lehr- und Lernmethoden sowie die skizzierten Implikationen fördern oder gar erst ermöglichen. So kann beispielsweise durch das Sammeln und Auswerten von gespeicherten Lernerdaten auf einer Lernplattform mittels „Learning Analytics" (Siemens 2012, S. 4ff) und „Educational Data Mining" (Baker und Inventado 2014) eine individuelle Anpassung von Lernaufgaben an den Wissensstand der Lernenden vorgenommen werden. Die Anpassungen erfolgen entweder automatisch oder durch die Lehrenden. Besonders Fächer und Vorlesungen mit hohen Studierendenzahlen können von diesen technischen Entwicklungen profitieren. Zusammen mit sogenannten „Massive Open Online Courses" (MOOCs), also aufgenommenen Vorlesungen, Vorträgen oder speziellen Erklärvideos, können diese Technologien im Konzept eines „Inverted Classroom" besonders an Hochschulen gewinnbringend eingesetzt werden. Beim forschungs- und problembasierten Lernen spielen außerdem digitale Assistenten, die sich an die Gruppenbedürfnisse, Gruppenkonstellationen sowie Forschungs- bzw. Lernphasen anpassen können, eine wichtige Rolle. Hierbei werden insbesondere Anweisungen an die Gruppensituation und Kollaborationsphase angepasst (vgl. „Adaptives Scripting" bei Demetriadis und Karakostas 2008). Nichtsdestoweniger müssen digitale Lernumgebungen an Hochschulen in einem höheren Maße offen, erweiterbar und für die Studierenden frei konfigurierbar sein. Studierende müssen in der Lage sein, kreative Lösungen und neue Forschungsdesigns digital umzusetzen. Mit der Vision von Forscherteams und einer vollständig digitalen wissenschaftlichen Arbeitsweise müssen künftige Kommunikations- und Kooperationsplattformen helfen, die Kommunikation zwischen Forscherteams und Dozierenden zu erleichtern, ein Forschungsdatenmanagement und digital unterstützte Datenanalyse zu integrieren sowie eine direkte Verknüpfung zwischen Forschungsdaten und -publikationen zu ermöglichen. Werden forschungs- und problembasiertes Lernen stärker und flächendeckender in Hochschulen angewandt, ist bereits absehbar, dass bestehende digitale Plattformen wie Ilias[19] oder Moodle[20] und andere digitalisierte Infrastrukturen wie „Open Educational Resources", Bibliotheksbestände und Forschungsdatenzentren Schnittstellen entwickeln

[19] *Siehe hierzu: www.ilias.de*

[20] *Siehe hierzu: https://moodle.de*

müssen, die ein reibungsloses wissenschaftliches Lernen und Forschen im digitalen Raum ermöglichen.

Hochschulen werden zunehmend damit konfrontiert sein, ein einheitliches digitales Studieren und Forschen zu ermöglichen. So formulierte die Kultusministerkonferenz (KMK) in ihrem Strategiepapier zur Bildung in der digitalen Welt, dass die […] Hochschulen in ihrem Bemühen zu unterstützen [seien], die Digitalisierung in der Lehre als Aspekt der Profilbildung und Bestandteil übergreifender Forschungs- und Lehrstrategien voranzutreiben." (KMK 2016, S. 50) Das Bundesministerium für Bildung und Forschung (BMBF) ergänzte in seiner Bildungsoffensive für die digitale Wissensgesellschaft, dass alle Bildungseinrichtungen „[…] über eine Strategie und die notwendigen Ressourcen zur Umsetzung digitaler Bildung […] [und über die] notwendigen organisatorischen, technischen und Management-Kompetenzen […]" (BMBF 2016, S. 27) verfügen sollten, diese umzusetzen.

Zentral bei der digitalen Umstellung von Forschung, Lehre und Wissenstransfer ist die Prämisse, dass Technologien immer unter dem Gesichtspunkt messbarer Lern- und Arbeitseffekte, eines qualitativen Mehrwerts von Ergebnissen sowie eines effizienteren, reibungsloseren Arbeitens beurteilt werden sollten. Aus diesem Grund bedarf es weiterer großer Forschungs- und Entwicklungsanstrengungen, die Effektivität und Qualität digitalen wissenschaftlichen Arbeitens zu erforschen, sowie einer massiven Investition in gebrauchstaugliche, digitale Infrastrukturen, um ein Lehren, Studieren und gemeinschaftliches Forschen von Lehrenden und Studierenden im digitalen Raum zu etablieren.

Weiterbildung

Die Entwicklung der Kompetenzen, auf denen digitale Souveränität fußt, müssen Eingang in das lebenslange Lernen finden, um auch diejenigen Bürger zu erreichen, die ihre initiale Bildungs- und Lernphase bereits – möglicherweise seit längerer Zeit – abgeschlossen haben. Sowohl Arbeitsprozesse als auch Forschungsprojekte können Ausgangspunkt einer qualitativ hochwertigen Weiterbildung sein. Wenn die Arbeit selbst oder Forschungsprojekte zum Lerngegenstand gemacht werden, orientieren sich die Weiterbildungsinhalte per se an aktuellen Themen und Herausforderungen. Durch systematische Reflexionsprozesse bei der Bearbeitung der Forschungs- oder Arbeitsprojekte wird das Lernen erfahrbar. Gleichzeitig bieten sich Chancen für neue Kooperationsbeziehungen entlang der Wertschöpfungskette, zwischen Bildungssystemen sowie zwischen Unternehmen und Weiterbildungsanbietern.

Weiterbildung in der Arbeit und mit der Wissenschaft

Reine Wissensvermittlung ist in der Weiterbildung heute nicht mehr zielführend, zumal Wissen schnell veraltet und für die oft sehr speziellen Belange der Unterneh-

men nicht spezifisch genug ist. Weiterbildung muss deshalb auf die konkrete Anforderung einer Person im jeweiligen Arbeitskontext zugeschnitten sein – inhaltlich, zeitlich und organisatorisch. Deshalb bietet sich Weiterbildung im Prozess der Arbeit anhand von Arbeitsinhalten an, die neben der inhaltlichen Aufgabenbewältigung übergreifende Kompetenzen wie Selbstorganisation, Analysefähigkeit, Problemlösungsfähigkeit, Kreativität, Medienkompetenz sowie den Umgang mit komplexen Anforderungen und Systemen in den Mittelpunkt stellt. Weiterbildung im Prozess der Arbeit kann wissenschaftliche Weiterbildung sein. Umgekehrt kann wissenschaftliche Weiterbildung auch in Arbeitskontexten stattfinden. Bei der Weiterbildung im Arbeitsprozess werden konkrete Arbeitskontexte und Arbeitsinhalte für die Weiterbildung genutzt. Bei der wissenschaftlichen Weiterbildung steht der Transfer von Forschung in die Praxis und von der Praxis in die Forschung im Mittelpunkt. Insbesondere innovative technologieorientierte Unternehmen, die oft wissenschaftsnah arbeiten, sind auf einen schnellen Transfer von Forschungsergebnissen in die Praxis angewiesen. Entsprechende Weiterbildungsangebote existieren derzeit allerdings kaum.

Im Rahmen der wissenschaftlichen Weiterbildung, die in den vergangenen Jahren besonders auch von Hochschulen als neues strategisches Betätigungsfeld erschlossen wird, können sowohl Arbeitsprozesse mit Forschungsprojekten verknüpft als auch Forschungsprojekte alleine zum Gegenstand der Weiterbildung gemacht werden. Auch hier steht neben der inhaltlichen Arbeit die Stärkung der genannten Kompetenzen im Mittelpunkt, ergänzt durch die Vermittlung von wissenschaftlichem Arbeiten.

Welche Anforderungen an Weiterbildung bestehen, wissenschaftlich oder nicht, wissen diejenigen, die in diesen Prozessen arbeiten, oft am besten. Entsprechend müssen die für die Weiterbildung Verantwortlichen und die Mitarbeitenden darin unterstützt werden, diese Veränderungsprozesse in und zwischen Unternehmen und den damit einhergehenden veränderten Bedarf, der oft von Unternehmen zu Unternehmen und von Arbeitsplatz zu Arbeitsplatz ganz unterschiedlich sein kann, zu erkennen, zu konkretisieren und zu nutzen. Dabei hilft es, wenn übergreifende Kompetenzen, wie Selbstorganisation, Problemlösefähigkeit oder der Umgang mit komplexen Anforderungen und Systemen, schon frühzeitig in Schule, Ausbildung oder Studium vermittelt wurden.

Passgenaue Weiterbildung in Losgröße 1

Für die passgenaue Weiterbildung und den Wissenstransfer zwischen Forschung und Praxis bieten sich Ansätze des arbeits-, problem- und forschungsbasierten Lernens besonders gut an. Folgende zwei Beispiele, die auch miteinander kombinierbar sind, sollen dies verdeutlichen.

- Gerade dort, wo Arbeitsprozesse sich schnell verändern und neue Herausforderungen durch die Digitalisierung bewältigt werden müssen, ist der Arbeitsgegenstand an sich auch gleichzeitig exzellenter Lerngegenstand. Beim arbeitsbasierten Lernen liegt die Herausforderung in der Systematisierung des Lernens im Arbeitskontext und im Bewusstmachen von Lernprozessen. Hierzu gibt es schon Erfahrungen und Ansätze. Ein erster systematischer Ansatz war das IT-Weiterbildungssystem[21], das auf dieser Idee aufgebaut war und durch generalisierte Prozesse, Dokumentation des Lernens, fachliche Unterstützung und Lernprozessbegleitung dem Arbeitsgegenstand als Lerninhalt Struktur gegeben hat. Die Idee wurde auch in anderen Zusammenhängen aufgegriffen und ist immer dann erfolgversprechend, wenn eben genau keine Lerninhalte im Sinne von Wissenselementen zur Verfügung gestellt werden können, die Arbeitsprozesse aber selbst viele Chancen zum Lernen bieten. Aktuell beschäftigen sich zum Beispiel Projekte aus dem Wettbewerb „Aufstieg durch Bildung: offene Hochschulen“[22] mit solchen Lernformen, teilweise auch unter Nutzung digitaler Medien. Diese Form des arbeits- und projektbasierten Lernens bietet sich generell für die Weiterbildung an, auch für die wissenschaftliche.
- Für den Transfer von Exzellenzwissen zwischen Hochschulen und Unternehmen erscheinen Tandems zwischen exzellenten Studierenden sowie Mitarbeitern von Unternehmen geeignet, die in innovativen Feldern arbeiten und auf Wissen aus der Forschung angewiesen sind. Ziel ist der Transfer von Forschungs-Know-how in die Praxis und von Anforderungen der Praxis in die Forschung. Die Studierenden bearbeiten dabei definierte forschungsnahe Projekte, die zugleich Input für ihre Abschlussarbeiten liefern können. Tandempartner auf Seiten der Unternehmen unterstützen die Studierenden in ihrer Arbeit und lernen selbst in diesem Prozess. Eine wissenschaftliche Betreuung dieser Tandems durch qualifizierte Personen aus dem Lehrkörper stellt dabei sicher, dass das wissenschaftliche Potenzial

[21] *Siehe hierzu auch Wikipedia zum Begriff „APO-IT“ (Arbeitsprozessorientierte Weiterbildung in der IT-Branche). Verfügbar unter: https://de.wikipedia.org/wiki/APO-IT, zuletzt zugegriffen am 19.07.2017.*

[22] *Siehe hierzu z. B. „Work Based Learning“ (Lernen an Realprojekten aus dem professionellen Umfeld der Lernenden) im Projekt „beSt – berufsbegleitendes Studium nach dem Heilbronner Modell“ (Verfügbar unter: www.hs-heilbronn.de/projekt-best, zuletzt zugegriffen am 28.08.2017); Lernen in realen Forschungs- und Entwicklungsprojekten in den Projekten „Freiräume für wissenschaftliche Weiterbildung“ der Universität Freiburg (Verfügbar unter: www.offenehochschule.uni-freiburg.de, zuletzt zugegriffen am 28.07.2017) und continu.ing der TU Hamburg-Harburg (Verfügbar unter: http://continuing.de/wp, zuletzt zugegriffen am 28.07.2017).*

dieser Projekte für beide Seiten ausgeschöpft wird. Der Fokus der Tandems ist zwar auf die inhaltliche Arbeit gerichtet, auf strategischer Ebene stehen aber der Wissenstransfer und die betrieblichen Weiterbildungsprozesse im Vordergrund. Gleichzeitig werden auch die Kooperationen zwischen Hochschule und Unternehmen intensiviert.[23] Dieser Ansatz ist ein Beispiel für die wissenschaftliche Weiterbildung.

Weiterbildung braucht Support-Strukturen – Rollen verändern sich

Ein wichtiges Element der Weiterbildung mittels arbeits-, problem- und forschungsbasiertem Lernen sind Begleitprozesse, also Tandems, Lernprozessbegleitungen oder der Austausch zwischen den Teilnehmern einer Weiterbildung. Sie unterstützen insbesondere die Motivation und Einordnung des Gelernten. Am Beispiel der Aufgaben, die hier Weiterbildungsanbieter übernehmen können, soll dies im Folgenden kurz verdeutlicht werden: Die Rolle der Weiterbildungsanbieter verändert sich vom Vermittler von Inhalten zum Prozessorganisator. Bei diesem ganzheitlichen Ansatz besteht die anfängliche Aufgabe darin, ein oder mehrere für die Weiterbildung geeignete Projekte aus dem Forschungs- oder Arbeitskontext zu identifizieren und mit dem Arbeitgeber abzustimmen. Diese Projekte müssen lernhaltig im Sinne der zu vermittelnden Kompetenzen und herausfordernd für den Lernenden sein sowie einen vorher definierten Umfang haben und an aktuellen Prozessen der Unternehmen orientiert sein. Weiterbildungsanbieter können in der Identifikation solcher Projekte unterstützen. Die Aufgabe der Bereitstellung von Inhalten durch Weiterbildungsanbieter nimmt dagegen eine eher untergeordnete Rolle ein. Denkbar sind eher allgemeine Angebote wie wissenschaftliches Arbeiten, Projektmanagement oder Hinweise darauf, wie man im Internet zum jeweiligen Thema aktuelle Informationen findet und damit umgeht. Schließlich sind Zertifizierungsformen der Weiterbildung festzulegen und zu definieren, was diese Zertifikate strategisch bedeuten sollen im Hinblick etwa auf internationale Anerkennung oder die Anrechenbarkeit auf ein Studium.

Diese Form der Weiterbildung kann sehr gut auf ganz spezielle Bedarfe zugeschnitten werden. Umgekehrt fordert sie von Lernenden ein hohes Maß an Eigenständigkeit und Selbstreflexionsfähigkeit. Auch ist die Weiterbildung durch die Verschränkung mit Arbeit und Forschung grundsätzlich mit Risiken behaftet: Reale Projekte im Arbeitskontext können sich verändern oder gar wegbrechen, neue Aufträge können Weiterbildungsprozesse verändern oder verzögern, Forschung kann Ergebnisse her-

[23] *Siehe zum Thema „Wissenschaftliche Weiterbildung für Unternehmen" auch: www.vdivde-it.de/ips/archiv/dezember-2007/wissenschaftliche-weiterbildung-fuer-unternehmen, zuletzt zugegriffen am 28.07.2017*

vorbringen, die man sich nicht erwünscht hat. Vor diesem Hintergrund muss Weiterbildung auch inhaltlich und zeitlich flexibel gestaltet sein.

Digitalisierung minimiert Risiken und ermöglicht Freiräume

Digitalisierung bietet die Möglichkeit, individuelle Lernprozesse zu unterstützen und auch abzusichern:

- Digital können verschiedene (Micro-)Lerneinheiten bereitgestellt werden, die dann punktuell und genau bei Bedarf von den Weiterzubildenden selbst abgerufen werden.

- Learning Analytics kann darin unterstützen, individuelle Lernprozesse sichtbar und die Ergebnisse zur Grundlage einer Zertifizierung zu machen.

- Mittels Simulationsumgebungen und virtuellen Laboren ist es möglich, Weiterbildungsprozesse abzusichern. So kann es sein, dass ein als Lerngegenstand identifiziertes Projekt doch nicht so umfassend ist, wie ursprünglich angenommen; es verändert sich aufgrund äußerer Rahmenbedingungen oder es gibt Elemente, die aufgrund von Sicherheitsbestimmungen des Unternehmens nicht als Lerngegenstand genutzt werden dürfen. Dann kann gezieltes Lernen in Simulationsumgebungen und virtuellen Laboren helfen, genau diese Lücken zu schließen.

- Weiterbildung auf Losgröße 1 lässt sich schwer in Gruppen umsetzen oder durch Peers unterstützen, wenn sie auf Präsenz ausgerichtet ist: Die Weiterbildungsgegenstände unterscheiden sich thematisch-inhaltlich sowohl vom Umfang her als auch im Bearbeitungstempo. Wann gibt es ein geeignetes Projekt im Arbeits- oder Forschungskontext? Bis wann muss es bearbeitet sein? Was macht man, wenn sich plötzlich Prioritäten im Arbeitskontext verschieben und ein anderes Projekt vorerst vorgezogen werden muss oder das Projekt schneller als ursprünglich geplant bearbeitet werden muss? Die digitale Vernetzung im Rahmen von Forenbeiträgen oder Chats im Internet bietet hierbei Gleichgesinnten über verschiedene Weiterbildungsanbieter hinweg die Chance, eine kritische Masse an Personen zu erreichen, die sich gegenseitig in der Bearbeitung ihrer sehr individuell zugeschnittenen Projekte direkt unterstützen können.

- Synchrone und asynchrone digitale Kommunikations- und Kollaborationswerkzeuge wie auch Werkzeuge zum Wissenstransfer können die schnelle Unterstützung der Weiterzubildenden durch Prozessorganisatoren oder Mentorenschaft bei Bedarf sicherstellen. Visionär lässt sich zumindest in Teilen in absehbarer Zeit auch automatisiertes Lerncoaching durch den Einsatz entsprechender Algorithmen umsetzen.

- Online-Lerntagebücher oder auch Online-Kurz-Assessments, die mit gezielten Fragen das Gelernte sichtbar machen, oder auch Projektplanungstools zur Unterstützung der Organisation der Weiterbildung und der Dokumentation der Arbeiten bieten gute Möglichkeiten, die Lernenden zu motivieren und bei der Selbstreflexion zu unterstützen.

Für diese individuelle Form der Weiterbildung mittels arbeits-, forschungs- und projektbasiertem Lernen sind Freiräume und eine unterstützende Lehr-Lernkultur sehr wichtig, um die Tätigkeiten sowohl in der Forschung als auch in der Arbeit in einem Unternehmen reflektieren zu können – und um zu recherchieren, wie man etwas auch auf andere Weise tun kann. Digitale Medien, also der Austausch per Chat, Videokonferenz, Webinar, „Virtual Classroom" oder andere Kommunikations- und Kollaborationswerkzeuge, und didaktische Trends wie „Casual Learning", Mikrolerneinheiten, Lernen nach Bedarf oder „Reversed-Konzepte" können maßgeblich dabei unterstützen, diese Freiräume zu schaffen.

Ausblick

Selbstverantwortliches, erfahrungsbasiertes Lernen steht im Zentrum einer Kompetenzentwicklung, die auf digitale Souveränität abzielt. Dadurch werden über alle Bildungsbereiche hinweg unterschiedliche Neujustierungen notwendig. Diese Neujustierungen beziehen sich auf das Rollenverständnis der Lehrenden und Lernenden, auf den Prozess der Organisationsentwicklung, auf die gesellschaftlichen Anforderungen hinsichtlich der Leistung und Funktion von Bildungsinstitutionen sowie auf den Einbezug digitaler Medien:

Rollenverständnis der Lehrenden: Die Aufgabe, das Lehren konsequent aus der Lernendenperspektive anzubieten („The shift from teaching to learning"; siehe Wildt 2003), bedeutet für Lehrende in der Schule vor allem, adaptiv und aktivierend zu unterrichten, in der Hochschule zunehmend anleitend und kooperativ in Forschungsgemeinschaften zu agieren und in der beruflichen Bildung ebenso wie auch der wissenschaftlichen Weiterbildung lernbegleitend zu wirken.

Rollenverständnis der Lernenden: Die Chance für Lernende, sich weitgehend selbstbestimmt und eigenverantwortlich mit lebensnahen, authentischen Fragen und Problemstellungen auseinanderzusetzen, bezieht sich in der Schule insbesondere darauf, das Lernen zu lernen; in der beruflichen Bildung bedeutet sie, Verantwortung für das Lernen zu übernehmen; Studierende in Hochschulen sind angehalten, eigenverantwortlich und proaktiv Forschungs- und Problemgegenstände über den bekannten Horizont hinauszudenken; und bei Studierenden der wissenschaftlichen Weiterbildung steht der Gedanke des lebenslangen Lernens im Mittelpunkt.

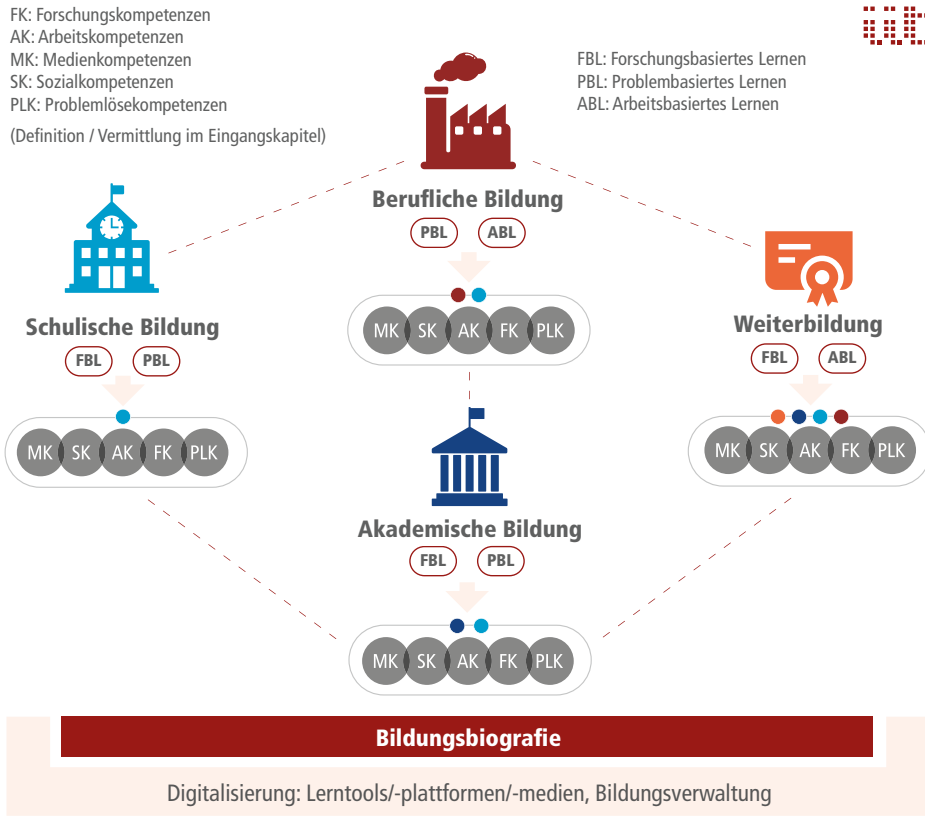

Abbildung 3.3.1: Bildung als Voraussetzung digitaler Souveränität[24]

[24] *In den vorangegangenen Abschnitten wurde bereits deutlich, welche Lehr- und Lernformen in welchen Bildungsbereichen besondere Anwendung finden, und welche Kompetenzen sie vermitteln. Mit diesem Schaubild soll deutlich werden, dass neu erworbene Kompetenzen aufeinander aufbauen und in den speziellen Bildungsbereichen ihre eigene „Färbung" bekommen sollten (siehe farbige Punkte an den Kompetenzmarkern). Die Verbindungslinien zwischen den Bildungsbereichen verdeutlichen, dass auf eine höhere Durchlässigkeit individueller Lernwege geachtet werden muss. Während Medienkompetenzen durch die proaktive Erfahrung, Anwendung und Entwicklung digitaler Artefakte vermittelt werden, sollen Lerntools, Lernmedien und Lernplattformen jegliche Art von Kompetenzvermittlung unterstützen. Diese sollen den Lernenden während ihrer Bildungsbiografien begleiten und aufeinander aufbauen, auch wenn Lernende zwischen Bildungsbereichen wechseln.*

Organisationsentwicklung: Im Sinne von lernenden Organisationen stehen Schulen vor der Herausforderung, ein Profil zu entwickeln und, sollten sie mehr Autonomie gewinnen, diese zur Umsetzung ihres Profils zu nutzen. Beruflichen Schulen obliegt es, Lernen zunehmend an unterschiedlichen Ausbildungsorten zu ermöglichen und noch stärker mit den Praxisanforderungen zu verzahnen, Hochschulen, eine noch stärkere Verzahnung der drei Säulen Forschung, Lehre und Transfer vorzunehmen, und Einrichtungen der wissenschaftlichen Weiterbildung sind aufgefordert, Kooperationen entlang der Wertschöpfungskette – welche sowohl Wirtschaft als auch Wissenschaft umfassen – vorzunehmen bzw. auszubauen.

Gesellschaftliche Anforderungen: Das Erfordernis, Bildungsbereiche und -institutionen durchlässiger zu gestalten und individuelle Lerninhalte und Lernwege zuzulassen, heißt für Schulen, formative Bewertungen nicht nur vorzunehmen, sondern bei der Vergabe formaler Qualifikation diese auch anzuerkennen; für berufliche Schulen sind infolge sich schnell verändernder beruflicher Anforderungen flexible Curricula notwendig; Hochschulen sehen sich, aufgrund der Nachfrage hochqualifizierter Fachkräfte, gezwungen, eine höhere Durchlässigkeit zwischen Lehre, Forschung und Praxis sowie zwischen einzelnen Semesterjahrgängen oder Fachdisziplinen zuzulassen; für Institutionen der wissenschaftlichen Weiterbildung erscheinen vor allem individuelle Curricula notwendig.

Digitalisierung: Die Nutzung digitaler Medien zur Unterstützung von Lehr- und Lernprozessen und die zeitgleiche Förderung eines souveränen und mündigen Umgangs mit digitaler Technik bedeutet, die Didaktik und Methodik in allen vier Bildungsbereichen entsprechend neu aufzustellen.

Auch wenn die einzelnen Bildungsbereiche unterschiedliche Spezifika, Bedürfnisse und Entwicklungsstadien bei den Neujustierungen vorweisen, dürfen bei den Punkten Kompetenzentwicklung und Digitalisierung keine Brüche entstehen. Die Grundlagen für ein mündiges und verantwortungsvolles Leben in analogen und digitalen Welten unserer Gesellschaft werden bereits in der Schule gelegt und müssen bei jeder der nachfolgenden Bildungsstationen eingefordert und erweitert werden. Die grundlegenden Prinzipien und Stufen der Kompetenzentwicklung wie auch des Medieneinsatzes sollten hierbei für die Lernenden verständlich und nachvollziehbar bleiben. Die Ermöglichung individueller Lernwege und zugleich durchlässige Gestaltung der Übergänge zwischen den Bildungsbereichen ohne Brüche auf Kompetenzebene und medialer Ebene eröffnen eine bildungsbiografische Entwicklungsperspektive (siehe Abbildung 3.3.1). Die Voraussetzung dafür scheint, Bildungserfolge systematisch zu erschließen und den Anforderungen einer zunehmend digitalisierten Welt adäquat zu begegnen.

Literatur

Baker, R. S.; Inventado, P. S. (2014). Educational Data Mining and Learning Analytics: Springer New York. Verfügbar unter: http://link.springer.com/chapter/10.1007/978-1-4614-3305-7_4/fulltext.html, zuletzt zugegriffen am 20.07.2017.

Bandura, A. (1977). Self-Efficacy: Toward a Unifying Theory of Behavioral Change. In: Psychological Review 84 (2), S. 191–215.

Bundesministerium für Bildung und Forschung (BMBF) (2016). Bildungsoffensive für die digitale Wissensgesellschaft. Strategie des Bundesministeriums für Bildung und Forschung. Verfügbar unter: www.bmbf.de/pub/Bildungsoffensive_fuer_die_digitale_Wissensgesellschaft.pdf, zuletzt zugegriffen am 26.07.2017.

Bundesinstitut für Berufsbildung (BIBB). Teil 1 – Industrie 4.0 und ihre Auswirkung auf die Arbeitswelt. Websiteauftritt. Verfügbar unter: www.foraus.de/html/foraus_3324.php, zuletzt zugegriffen am 26.07.2017.

Demetriadis, S.; Karakostas, A. (2008). Adaptive collaboration scripting: A conceptual framework and a design case study. International Conference on Complex, Intelligent and Software Intensive Systems, CISIS 2008, S. 487–492.

Deutsche Kinder- und Jugendstiftung (DKJS). Forschendes Lernen. Websiteauftritt. Verfügbar unter: http://forschendes-lernen.net/index.php/gute-gruende.html, zuletzt zugegriffen am 26.07.2017.

Hickman, L. A. (2004). John Dewey – Leben und Werk. In: Hickman, L., A.; Neubert, S.; Reich, K. (Hrsg.). John Dewey. Zwischen Pragmatismus und Konstruktivismus (1), S. 1–12.

Huber, L. (2009). Warum Forschendes Lernen nötig und möglich ist. In: Huber, L.; Hellmer, J.; Schneider, F. (Hrsg.). Forschendes Lernen im Studium. Bielefeld: Universitätsverlag Webler, S. 9–35.

Jonassen, D. H. (1997). Instructional design models for well-structured and Ill-structured problem-solving learning outcomes. In: ETR&D 45 (1), S. 65–94. DOI: 10.1007/BF02299613.

Kergel, D.; Heidkamp, B. (2015). Forschendes Lernen mit digitalen Medien. Ein Lehrbuch. Münster: Waxmann.

Kultusministerkonferenz (KMK) (2016). Bildung in der digitalen Welt: Strategie der Kultusministerkonferenz. Verfügbar unter: www.kmk.org/fileadmin/Dateien/pdf/PresseUndAktuelles/2016/Bildung_digitale_Welt_Webversion.pdf, zuletzt zugegriffen am 20.07.2017.

Merriënboer, J. J. G. v.; Sweller, J. (2005). Cognitive Load Theory and Complex Learning. Recent Developments and Future Directions. In: Educ Psychol Rev 17 (2), S. 147–177. DOI: 10.1007/s10648-005-3951-0.

Messner, R. (2009). Forschendes Lernen aus pädagogischer Sicht. In: Messner, R. (Hrsg.). Schule forscht. Ansätze und Methoden zum forschenden Lernen. Hamburg: Körber Stiftung, S. 15–30.

Odendahl, A. (2017). Digitalisierung muss Chefsache sein. Bildungsklick. Verfügbar unter: https://bildungsklick.de/aus-und-weiterbildung/meldung/digitalisierung-muss-chefsache-sein, zuletzt zugegriffen am 20.07.2017.

Siemens, G. (2012). Learning analytics: envisioning a research discipline and a domain of practice. In: LAK '12 Proceedings of the 2nd International Conference on Learning Analytics and Knowledge, S. 4–8. Verfügbar unter: http://dl.acm.org/ft_gateway.cfm?id=2330605&type=pdf, zuletzt zugegriffen am 20.07.2017.

Stubbe, J. (2017). Von digitaler zu soziodigitaler Souveränität. In: Wittpahl, V. (Hrsg.). Digitale Souveränität. Bürger – Unternehmen – Staat. iit-Themenband. 1. Aufl. Berlin, Heidelberg: Springer. (*vgl. Kapitel 1.3 in diesem Band*)

Wildt, J. (2003). „The Shift from Teaching to Learning" – Thesen zum Wandel der Lernkultur in modularisierten Studiengängen. In: Bündnis 90 / Die Grünen im Landtag NRW (Hrsg.). Unterwegs zu einem europäischen Bildungssystem. Reform von Studium und Lehre an den nordrhein-westfälischen Hochschulen im internationalen Kontext. Düsseldorf, S. 14–18.