DIGITALISIERUNG DES ÖFFENTLICHEN

Kompetenzzentrum
Öffentliche IT

VORWORT

Im Auto, am Handgelenk und zunehmend auch im Haushalt: Fast überall begegnet uns Informationstechnologie – schon lange nicht mehr nur im Smartphone oder am Laptop. Immer wieder gibt es und geht es um Neues: Neue Trends, neue Konzepte und neue Produkte bestimmen die Debatten. Sicher: Cloud-Computing und Big Data gewinnen weiter an Bedeutung. Aber in aller Munde sind schon längst künstliche Intelligenz, Smart City, das Internet der Dinge oder das autonome Fahren.

Das wirft neue Fragen auf – oder sagen wir besser: Das wirft die alten Fragen neu auf: Welche Folgen hat technischer Fortschritt für unsere Gesellschaft? Wie können wir in einem neuen Umfeld Sicherheit und Vertrauen im Internet und der IT herstellen? Welche Form von Datenschutz ist »zeitgemäß«? Diese Fragen müssen wir immer wieder stellen – auch neu.

Mit der Arbeit des IT-Planungsrates und der Verabschiedung des IT-Sicherheitsgesetzes sowie der Datenschutz-Grundverordnung in Europa konnten in den vergangenen Jahren bereits wichtige Erfolge erzielt werden. Gerade in einem derart schnelllebigen Feld wie der Digitalisierung ist es wichtig, dass das politische Handeln stets dem aktuellen wissenschaftlichen Erkenntnisstand entspricht. Daher unterstützt das Bundesministerium des Innern seit fast vier Jahren das Kompetenzzentrum Öffentliche IT des Fraunhofer-Instituts für Offene Kommunikationssysteme in seiner Grundlagenarbeit.

Mit dieser Publikation führt das Kompetenzzentrum Öffentliche IT die wesentlichen Aspekte seiner Studien der letzten Jahre zusammen. Das Werk definiert Konzepte und Anwendungsbereiche öffentlicher IT und zeigt das vielseitige Spektrum der Veränderungen und Entwicklungen. Es verspricht all jenen eine aufschlussreiche Lektüre, die die technischen Entwicklungen in einem Gesamtbild von gesellschaftlichen und politischen Wirkungen verstehen wollen.

Ich wünsche Ihnen viel Vergnügen beim Blättern und Lesen in diesem Buch.

Dr. Thomas de Maizière MdB
Bundesminister des Innern

INHALT

1.

DIGITALISIERUNG UND GESELLSCHAFTLICHER ZUSAMMENHALT

Digitalisierung verschiebt Grenzen: Grenzen zwischen öffentlich und geschlossen, zwischen individuell und gemeinschaftlich, zwischen real und virtuell – um nur einige zentrale Wandlungsprozesse zu skizzieren. Was gestern noch physische Anwesenheit erforderte, steht heute einem wachsenden Teil der Weltbevölkerung durch Informationstechnik (IT, s. Glossar) online zur Verfügung.

Die Digitalisierung bedeutet aber weit mehr als nur eine andere, vielleicht effizientere Verrichtung altbekannter Tätigkeiten. Sie verändert unser aller Leben und die gesellschaftliche Kommunikation mitunter in einer Geschwindigkeit, die sich im Voraus nicht abschätzen lässt. Technisch können die Änderungen klein sein. Hier eine Hardwareoptimierung, dort ein leichteres Bedienkonzept – und schon eröffnen sich Möglichkeiten, die binnen kurzer Zeit nicht mehr wegzudenken sind. Smarte Mobiltelefone mit ihren Kommunikationsmöglichkeiten markieren in dieser Hinsicht den vielleicht eindrucksvollsten Wandel des vergangenen Jahrzehnts.

Öffentlich bezeichnet eine möglichst leichte Zugänglichkeit für möglichst breite Kreise.

Bei vielen Menschen ist das Internet durch Smartphone, Tablet und PC bereits allgegenwärtig. Sie nutzen es unter anderem dafür, sich in sozialen Netzwerken zu repräsentieren und Interessengemeinschaften zu bilden. Zunehmend werden aber auch Alltagsgegenstände in die digitale Welt eingebunden. Daraus ergeben sich viele neue Anwendungsmöglichkeiten. Durch das Internet der Dinge erhalten physische Objekte digitale Schnittstellen. Sensoren erfassen bestimmte Daten und ermöglichen so eine virtuelle Abbildung der Umgebung. Aktuatoren bieten zudem die Möglichkeit, aktiv auf die Umgebung einzuwirken und Objekte zu steuern. Diese virtuelle Repräsentation und Interaktion mit dinglichen Objekten erweitert die physische Welt und reichert sie um zusätzliche Informationen und Dienste an. Bereits heute ist absehbar, dass, bedingt durch die Digitalisierung, langfristig ein Großteil der Objekte der physischen Welt eine oder mehrere Entsprechungen in der virtuellen Welt erhalten wird.

Die rasant fortschreitende Digitalisierung und ihren Einfluss auf Gesellschaft und Leben kann man mit dem Begriff »reale Virtualität« beschreiben. Es ist die sprachliche Umkehrung des Begriffs »virtuelle Realität«, mit dem oftmals die digitale Welt bezeichnet wird. Virtuell bedeutet der Begriffsdefinition nach physisch nicht existierend. Mit der Umkehrung »reale Virtualität« soll deutlich gemacht werden, dass die digitale Welt mittlerweile noch einen Schritt weiter geht. Sie wirkt auf ihre Umgebung und greift aktiv ein, beispielsweise indem reale Gegenstände gesteuert werden. Aufgrund ihrer realen Auswirkungen ist die digitale Welt sehr wohl real und entfaltet gesellschaftliche Bedeutung, sei es als Vehikel gesellschaftlicher Kommunikation, als Wirtschaftsfaktor oder als kritische Infrastruktur.

Die virtuelle Welt wirkt auf ihre Umgebung und greift aktiv ein, indem reale Gegenstände gesteuert werden.

Anonymität und Gestaltbarkeit des Virtuellen eröffnen Freiräume für den Einzelnen. Nicht körperlich wahrnehmbar zu sein, schafft Spielraum. Während natürliche Personen an Rollenmustern gemessen und durch Erwartungen geleitet werden, erlaubt die Erschaffung virtueller Identitäten die Neujustierung von Freiheiten und Interaktionsformen. Hier kann Jede und Jeder ein Lebensexperte, eine Drachenjägerin oder Vorsitzender einer selbst gegründeten Loge sein. Zugleich sorgt die Programmierbar-

keit der Umwelt für neuartige Erfahrungsmöglichkeiten. Das Sich-Hineinversetzen in eine virtuelle Umgebung, häufig mit in der Realität wenig genutzten Facetten der eigenen Persönlichkeit, wird als Immersion bezeichnet. [Trendthema Immersion][1]

Die reale Welt – Arbeitsumfeld, alltägliche Routinen, Privatleben – und der Zugang dazu werden durch die Digitalisierung unter Veränderungsdruck gesetzt. Globale Vereinheitlichung einerseits und die zunehmende Individualisierung andererseits erzeugen immer neue Herausforderungen für den Zusammenhalt des Gemeinwesens – lokal, regional und national. [Trendthema Glokalisierung]

Gesellschaftlicher Zusammenhalt entsteht nicht von selbst, sondern muss gestaltet werden. Moderne Informationstechnik erbringt in Zukunftsfeldern zentrale Querschnittsfunktionen, verändert bestehende Strukturen und treibt damit gesellschaftliche Veränderungen voran. Um diese Veränderungen und die Bedürfnisse der Bürger[2] rechtzeitig zu erkennen, braucht es wissenschaftliche Erhebungen, Analysen und Konzepte. Gesellschaftliche Auswirkungen der neuen Technologien müssen bewertet und eingeordnet werden, um beispielsweise Herausforderungen wie der digitalen Spaltung der Gesellschaft umfassend entgegenwirken zu können. Ein Leitgedanke öffentlicher IT ist daher die gemeinwohlorientierte Ausgestaltung digitaler Vernetzung und Kommunikation über gesellschaftliche Subsystemgrenzen hinweg.

Leitgedanke öffentlicher IT ist die gemeinwohlorientierte Ausgestaltung digitaler Vernetzung und Kommunikation über gesellschaftliche Subsystemgrenzen hinweg.

Profundes Wissen über Technologien und die immer wiederkehrende (Re-)Evaluierung und (Neu-)Definition der öffentlichen Funktionen sind Voraussetzungen, um erfolgreiche Strategien für staatliche Verantwortung zu entwickeln.

Abb. 1: Die Digitale Agenda der Bundesregierung als Word Cloud

[1] Auf Publikationen des Kompetenzzentrums Öffentliche IT (Trendthemen, Whitepaper und Expertisen) wird einheitlich ohne Jahreszahl verwiesen, ohne direkte Zitate kenntlich zu machen. Eine Übersicht über alle ÖFIT-Publikationen findet sich in Anhang A.

[2] Die weibliche Form ist der männlichen Form gleichgestellt; lediglich aus Gründen der Vereinfachung wurde teilweise nur die männliche Form gewählt.

2.

VERÄNDERUNGEN IN DER GESELLSCHAFT – MEGATRENDS

»Megatrends muss man nicht ›voraussagen‹, denn sie sind schon da und markieren Veränderungen, die uns schon lange prägen und auch noch lange prägen werden. Megatrends sind Tiefenströmungen des Wandels. Als Entwicklungskonstanten der globalen Gesellschaft umfassen sie mehrere Jahrzehnte. Ein Megatrend wirkt in jedem einzelnen Menschen und umfasst alle Ebenen der Gesellschaft: Wirtschaft und Politik, sowie Wissenschaft, Technik und Kultur. Aus diesem Grund ist es entscheidend zu wissen, welche Chancen und Risiken in diesen Trendentwicklungen liegen.« [Zukunftsinstitut 2015]

Verschiedene Entwicklungen kennzeichnen die globalen Veränderungen in der Gesellschaft, wie Bevölkerungswachstum, steigende Krankheitslasten, Urbanisierung, Klimawandel, zunehmende Probleme der Welternährung und Wasserknappheit, zunehmende Bedeutung der globalen Wissensgesellschaft und in Deutschland auch der demografische Wandel und sinkende Haushaltsgrößen. [Zweck et al. 2015]

Wesentliche Veränderungen werden aber auch durch die Digitalisierung bewirkt. Während andere Megatrends gesellschaftliche Entwicklungen und Bedarfe darstellen, zeichnet sich die Digitalisierung durch ein enges Wechselspiel zwischen technischer Innovation und gesellschaftlichem Geschehen aus.

2.1 VERNETZUNG

Informationstechnik ist allgegenwärtig. Daher ist die digitale Infrastruktur für das Funktionieren von Gesellschaft, Wirtschaft und öffentlicher Verwaltung unverzichtbar.

Analoge Telekommunikationsdienste über Kabel oder Funk wie Telefon, Telefax, Radio usw. dienten lange Zeit der Nachrichtenkommunikation. Die erste Übermittlung von Nachrichten über lokale Rechnernetze in den 60er Jahren, die Entstehung des Arpanets (dem Vorläufer des heutigen Internets), die Erfindung der paketvermittelnden Netze (wie des Internets) und des Ethernets (als eine leistungsfähige Technik zur Übertragung von Paketen) markieren nur einige Schritte in der Vernetzung von Computern. Das Internet war vor nicht allzu langer Zeit noch ein neues, eigenständiges Medium, genutzt zum Austausch von Informationen, zum Lesen von Nachrichten oder als zusätzlicher Vertriebsweg für einzelne Produkte.

Inzwischen hat sich das Bild grundlegend gewandelt: Informationstechnik ist allgegenwärtig. Mit immer mehr Anwendungsbereichen und zunehmender Vernetzung steigt die Komplexität der IT beständig an und bildet eine digitale Infrastruktur, die für das Funktionieren von Gesellschaft, Wirtschaft und öffentlicher Verwaltung unverzichtbar geworden ist.

In vielen Dingen des alltäglichen Lebens stecken bereits heutzutage Chips, die Daten erfassen oder Steuerungsaufgaben erfüllen. Diese oft unbemerkte Allgegenwart ist unter dem Begriff »Ubiquitous Computing« bekannt geworden. Mehr und mehr werden diese Geräte auch untereinander oder mit dem Internet vernetzt, um Daten auszutauschen. Dabei ist der Fortschritt der Vernetzung in den verschiedenen Industriezweigen in unterschiedlichem Tempo verlaufen. Zwar ist im Zeitalter der Smartphones die allgegenwärtige Verfügbarkeit von Telefonie, E-Mail und Webdiensten in der Hosentasche zur Selbstverständlichkeit geworden, im Bereich der Automobilin-

dustrie waren jedoch Fahrzeuge noch lange Zeit autarke, isolierte Systeme. Das begründet sich durch die viel längeren Produktzyklen und die hohen Sicherheitsanforderungen in diesem Bereich. In den letzten Jahren ist hier jedoch ein Wandel zu erkennen. Die Vernetzung von Fahrzeugen steigt und die Kommunikation mit der Außenwelt ist Teil konkreter Produkte geworden. Eingebettete Systeme in industriellen Steuerungsanlagen verdeutlichen die Durchdringung ehemals geschlossener Produktionssysteme und -infrastrukturen mit Informationstechnik.

Soziale Netzwerke, Cloud-Computing oder vernetzte IT-Systeme für Telemedizin sind Beispiele neuer öffentlicher Infrastrukturen. Längst ist Vernetzung auch eine globale gesellschaftliche Herausforderung, da nationale Grenzen, regionale Rechte- und Wertesysteme sowie kulturelle Eigenheiten mit der Internationalität des Internets kollidieren.

Vernetzung verändert wirtschaftliche, soziale und kulturelle Räume. Öffentliche IT berührt daher die Grundfragen der digitalen Interaktion innerhalb von und zwischen Zivilgesellschaft, Wirtschaft und öffentlicher Hand in verschiedenen Anwendungsdomänen wie Energie, Verkehr oder Gesundheit.

Möglichkeiten

- Unterstützung und Verbesserung in vielen Lebensbereichen
- Wirtschaftswachstum und Entstehung neuer Geschäftsmodelle
- Konzentration der menschlichen Aktivitäten auf das Notwendige und Wesentliche, da viele Leistungen, Hilfen und Aktionen automatisiert werden

Wagnisse

- neue Sicherheitsrisiken und Gefahren durch die Öffnung vormals geschlossener Systeme
- Datenschutz und Privatheit werden in verschiedenen Ländern beziehungsweise Kulturen unterschiedlich bewertet und nicht von allen Regierungen und gesellschaftlichen Gruppen respektiert
- das Sammeln von Daten aller Art birgt die Gefahr des gläsernen Bürgers
- zunehmende Abhängigkeit von digitalen Infrastrukturen als zentrale kritische Infrastruktur
- Verweigerung der Teilnahme am digitalen Leben führt zu Isolation und Chancenungleichheit

2.2 MOBILITÄT

Mobilität ist ein Grundbedürfnis des Menschen. Seit Jahrtausenden ermöglicht sie Zugriff auf räumlich verteilte Ressourcen und soziale Teilhabe. Im Zuge der Forschung zu Mobilität und Verkehr sind die Grundlagen und Motivationen von Mobilität in den letzten Jahrzehnten intensiv untersucht worden. In modernen Gesellschaften korreliert der Wohlstand mit der Verkehrsleistung. Damit wird die enorme Bedeutung von Mobilität für unsere Gesellschaft deutlich, wie sie sich auch in der seit Jahren breit

geführten gesellschaftlichen Diskussion zu Chancen und Auswirkungen des Themas »Mobilität und Verkehr« widerspiegelt. [White Paper Digitale Mobilität; Canzler und Knie 2002; Frank 1997]

In verschiedenen Fachgebieten wird der Begriff Mobilität unterschiedlich und teilweise diffus verwendet. In technischen Zusammenhängen steht der Begriff zunächst für die physische Mobilität, zumeist des Menschen, also die konkrete Raumüberwindung. [Zoche 2002] Im Zeitalter der rapide wachsenden Internetnutzung in allen Lebensbereichen und -situationen steigt damit der Bedarf nach Geräten und Diensten, die ihre Nutzer in Phasen der physischen Mobilität unterstützen, zum Beispiel im Bereich multimodaler Mobilität, also der kombinierten, effizienten Nutzung verschiedener Mobilitätsangebote (Auto, Fahrrad, Bus, Bahn, Leihfahrzeug).

In modernen Gesellschaften korreliert der Wohlstand mit der Verkehrsleistung.

Grundsätzlich muss Mobilität als individuelle Option verstanden werden – Mobilität bezeichnet die Möglichkeit zur Bewegung, nicht in erster Linie die Bewegung selbst. Ein Beispiel verdeutlicht dies: Auf Dienstreisen werden Mobilgeräte genutzt, um auf Ressourcen der eigenen Organisation zuzugreifen oder per E-Mail an aktuellen Prozessen beteiligt zu sein. Prinzipiell können dieselben Geräte ebenso am Ort der eigenen Organisation genutzt werden. Mobilität erweitert den eigenen Handlungsspielraum, auch wenn nicht jede Möglichkeit tatsächlich genutzt wird.

Digitale Mobilität ist übergreifend die durch Technik unterstützte Bewegung in physischen und virtuellen Räumen. Sie ermöglicht eine höhere Flexibilität und mehr Bewegungsfreiheit für die Nutzer. Dies schließt auch die mobile Nutzung von Anwendungen und Diensten ein, deren Ziel nicht direkt die Unterstützung von Mobilität ist. Für digitale Mobilität bedarf es aus technischer Sicht mobiler Endgeräte, leistungsfähiger Zugangs- und Übertragungsnetze und Anwendungen, welche mobil genutzt werden können, sowie angemessener Sicherheits- und Datenschutzmechanismen. Erst wenn diese Grundvoraussetzungen erfüllt sind, ist digitale Mobilität gegeben. Der Grad der digitalen Mobilität hängt dabei vom Grad der Umsetzung der jeweiligen Grundvoraussetzungen ab.

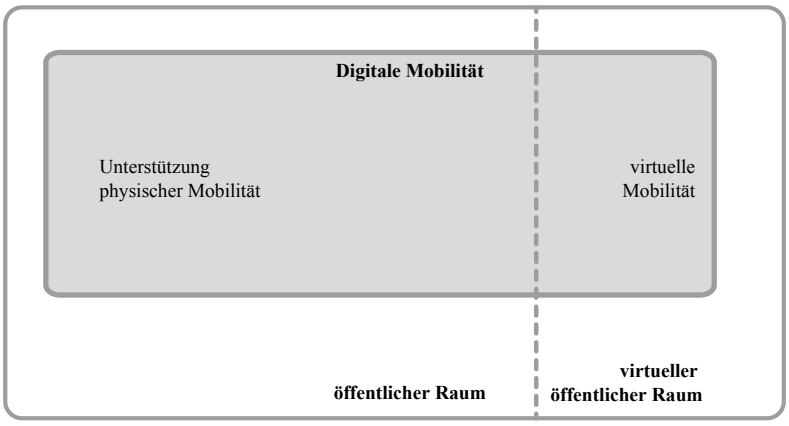

Abb. 2: Digitale Mobilität

Digitale Mobilität, insbesondere die mobile Nutzung von IT, wird mehr und mehr zum Normalfall, von dem die stationäre Nutzung eine spezielle Ausprägung darstellt. [Trendthema Digitale Mobilität] IT wird mobil, erleichtert Mobilität und verändert sie durch umfassende Erreichbarkeit. Trends wie der mobile Arbeitsplatz, mobile Endgeräte oder die Nutzung privater Geräte im beruflichen Umfeld (auch als Bring Your Own Device bezeichnet) zeigen die Richtung auf.

Die stete IT-Nutzung wirkt sich auch auf die physische Mobilität aus, wobei Navigationshilfen und Abfahrtspläne öffentlicher Verkehrsmittel erst den Anfang markieren. Moderne Carsharing-Konzepte mit bislang nicht gekannter Nutzungsflexibilität und die jederzeit verfügbare, bedarfsgesteuerte Kombination verschiedener Verkehrsmittel durch die Bürger selbst werden möglich. Während diese Szenarien letztlich auf die Frage zielen, auf welche Art digitale und mobile Techniken physische Mobilität optimieren können, so kann IT-gestützte Kommunikation diese auch ersetzen. Audio- und Video-Konferenzsysteme, die durch eine immer realistischere digitale Repräsentation des Gegenübers weiter optimiert werden, sind Beispiele für diese Entwicklung. Statt Menschen werden Daten auf die Reise geschickt, physische Mobilität und Raumbewegung werden durch virtuelle Mobilität und den elektronischen Austausch von Informationen substituiert.

Digitale Mobilität ist die durch Technik unterstützte Bewegung in physischen und virtuellen Räumen.

Für nahezu alle Bereiche mobiler Anwendungen gilt ein Internetzugang ebenso als Voraussetzung wie die Verfügbarkeit von Ressourcen in Backend-Systemen. Digitale Mobilität wird so maßgeblich zu einem Thema von fortschrittlichen Netzen und IT-Infrastruktur, die innovative Anwendungen ermöglichen.

Die gesellschaftlichen Implikationen sind vielfältig. Flexible Mobilität ist eine wichtige Facette des Leitbilds einer sich als modern und dynamisch verstehenden Gesellschaft. Ununterbrochene Erreichbarkeit und permanenter Zugriff auf Daten und Dienste erlauben eine identische Abbildung in digitalen Kommunikationsmedien, mobil wie stationär.

Möglichkeiten

- Automatisierung und Personalisierung der Informationsbereitstellung zur richtigen Zeit am richtigen Ort
- einfacher, immer verfügbarer Zugang zu Informationen und Diensten (»Always-on«)
- ständige Erreichbarkeit
- ortsabhängige Notfalldienste, die gegebenenfalls sogar automatisch aufgerufen werden
- individuelle und gemeinschaftliche Optimierung multimodaler Verkehrsnutzung
- Substitution physischer Mobilität durch virtuelle

Wagnisse

- Herausforderungen für Datenschutz und Datensicherheit durch die Erfassung und mobile Übertragung vielfältiger Daten
- Risiko des umfangreichen Identitätsdiebstahls nach Verlust des Mobilgerätes
- verstärkte Vermischung von Privatem und Dienstlichem etwa bei dienstlicher Nutzung von privaten Geräten
- Abhängigkeit von Netzverfügbarkeit und Diensten
- Überforderung durch ständige Erreichbarkeit und durch die Vielzahl der Möglichkeiten
- digitale Spaltung durch unterschiedliche Nutzung und regionale Disparitäten

2.3 INDIVIDUALISIERUNG

Ein Selfie auf Reisen, interaktives Fernsehen, die vom Fahrstil abhängige Autoversicherung oder die Nutzung privater Geräte im Unternehmen – alle diese Entwicklungen basieren auf einer gemeinsamen Tendenz zur Individualisierung in unterschiedlichen Ausprägungen. Ob Werbung, Produkte oder Medien, in allen Bereichen eröffnet die Digitalisierung neue Möglichkeiten, um Bedürfnisse, persönliche Vorlieben, Eigenheiten und Wünsche zu berücksichtigen.

Durch die Auswertung vieler Daten sollen Werbung, Produkte und Dienste möglichst passgenau gestaltet werden.

Die Digitalisierung hat die Medien auf allen Wertschöpfungsstufen erfasst. Steigende Konvergenz und Multikanal-Angebote lassen die Grenzen zwischen den Medien und ihren Endgeräten mehr und mehr verschwimmen. Mitwirkungsmöglichkeiten werden ausgebaut und das Prinzip des Broadcastings zunehmend durch Rückkanäle ergänzt. Analog hierzu sinkt die Schwelle zur Produktion massenmedialer Inhalte. Technische Verbesserungen und neue Verbreitungswege eröffnen Möglichkeiten zur kreativen Beteiligung, die in Einzelfällen hinsichtlich Abrufzahlen und wirtschaftlicher Verwertbarkeit mit klassischen Fernsehserien konkurrieren können. [Trendthema Massenmedien]

Auch im Marketing ist die möglichst genaue Vorhersage von Kundenwünschen auf dem Vormarsch, um Werbung, Produkte und Dienste möglichst passgenau zu gestalten und damit die Wahrscheinlichkeit des Kaufes zu erhöhen. Das Sammeln von möglichst vielen Daten über den potenziellen Kunden (Big Data) ist hierfür die Grundlage. Sind beispielsweise Newsletter bisher meist nur in der Anrede personalisiert, so wird es zukünftig möglich sein, mit jedem Nutzer einen vollständig individualisierten und automatisierten Dialog zu führen. [Even 2015]

Hochautomatisierte individualisierte Produkte sind die Vision einer Entwicklungsstufe der industriellen Fertigung, die einen Aspekt von Industrie 4.0 [Trendthema Industrie 4.0] darstellt. Die Produktionsprozesse werden flexibler, um Produkte individuell an Kundenwünsche anpassen zu können.

Gleichzeitig findet aber auch eine Verlagerung von Teilen der Produktion hin zum Konsumenten statt, die als Prosumption bezeichnet wird. [Trendthema Prosument] Mit

Hilfe von 3D-Druckern etwa können Kleinteile wie Ersatzteile oder kleine Alltagsgegenstände eigenständig produziert werden. [Trendthema 3D-Drucker] Dadurch sind neue Produktionsformen oder neue Logistikkonzepte denkbar.

Auch wenn die Individualisierung wie ein Streben nach Einzigartigkeit durch freie Entscheidungen erscheint, ist dies häufig ein Trugschluss. Eine freie Entscheidung wird nur im Kontrollbereich des Anbieters gewährt. Ein einfaches Beispiel ist die »freie« Wahl der Farbe eines Neuwagens, die jedoch auf bestimmte Farbtöne begrenzt ist. Diese Entwicklung ist auch auf großen Internetplattformen zu beobachten, die schon lange die Personalisierung als Geschäftsmodell erkannt haben. Als Filterblase, engl. »Filter Bubble« [Pariser 2012], wird der Effekt bezeichnet, im Internet bevorzugt Suchergebnisse zu erhalten, die aufgrund persönlicher Neigungen zum eigenen Weltbild passen. Ein Beispiel ist die Google-Suche nach »Golf«: Mit diesem Begriff kann man das Auto meinen, den nächsten Golfplatz oder die ölproduzierenden Länder. Basierend auf Kenntnissen über Suchworte, Standort oder Surfverhalten werden die Resultate »personalisiert«. Bestenfalls wird so immer genau das Richtige gefunden, schlimmstenfalls wird die Welt auf den eigenen Horizont eingeschränkt.

Kleine Stupser (engl. »Nudges«) können Menschen auf sanfte Weise zu gewünschtem Verhalten bringen. Verhaltensökonomische Modellierungen dienen der Identifikation der richtigen Stupser. [Trendthema Stupsen] Durch die umfassende Beteiligung an sozialen Netzwerken, die rasante Verbreitung körpernaher Sensoren und neue Verfahren für die zeitnahe Auswertung großer Datenmengen ergeben sich vollkommen neue Analyse- und Beeinflussungsmöglichkeiten. Menschliches Verhalten kann so dauerhaft in kurzen Messintervallen in der jeweiligen Alltagswelt erfasst und ausgewertet werden, und die Ergebnisse lassen sich umgehend zurückspielen.

Kleine Stupser (engl. »Nudges«) können Menschen auf sanfte Weise zu gewünschtem Verhalten bringen.

Die Implikationen für die sozialwissenschaftlich-empirische Forschung sind beträchtlich. Unterschiedliche Fragestellungen lassen sich mit geringem zusätzlichem Aufwand zeitnah auswerten, wobei Beeinflussungsvarianten gezielt ausprobiert werden können. Aus einer politischen Steuerungsperspektive erscheinen die Möglichkeiten reizvoll. Die Wirkung politischer Maßnahmen lässt sich in bisher ungeahntem Detailgrad erfassen und deren Wirksamkeit durch ein sehr sanftes Mittel erhöhen. Statt etwa durch Verbote oder Steuerung massiv in die Entscheidungsfreiheit der Betroffenen einzugreifen, werden nur die Entscheidungssituationen modifiziert. Konnten diese Modifikationen bisher nur einheitlich erfolgen, erlaubt die Digitalisierung ihre Individualisierung.

Möglichkeiten

- Selbstverwirklichung und Differenzierung statt Uniformierung und Nivellierung
- individuelle Produkte trotz Massenproduktion
- Individualisierung von Informationen und Angeboten, beispielsweise passgenaues Medienangebot

Wagnisse

- Steuerung und Kontrolle durch Dienste- und Produktanbieter
- maßloses Sammeln und Auswerten personenbezogener Daten
- tiefgreifender Anpassungsbedarf industrieller Produktion
- unkoordinierte und unkontrollierte Minimärkte sowie kaum mehr überblickbare Produktvielfalt
- zunehmende Bildung von Filterblasen

2.4 ENTGRENZUNG

Entgrenzen bedeutet, etwas »aus seinen Grenzen lösen, aus der Begrenztheit befreien«. [Duden: entgrenzen] Dieses Phänomen kann man heute in vielen Bereichen beobachten. Zeitliche, örtliche, organisatorische und strukturelle Einschränkungen verlieren ihre Bedeutung. Freizeit, Arbeit, Unterhaltung und Bildung sind keine getrennten Lebensbereiche mehr. Arbeitszeitmodelle sind zunehmend flexibel.

Die Offenlegung alles Privaten könnte zu einer neuen Dimension gesellschaftlicher Toleranz führen.

Always-on, das heißt, die ständige Erreichbarkeit und ortsunabhängige Nutzung von Diensten verändert die menschliche Kommunikation. Flexibilität und Dynamik beeinflussen die Lebensgestaltung. Überall tun sich neue Formen von Gemeinschaften, Kollaborationen und Kooperationen auf. [Brühl und Pollozek 2015] Selbst das Mein und Dein verändert sich in der sogenannten Sharing Economy, die das systematische Ausleihen von Gegenständen und das gegenseitige Bereitstellen von Räumen und Flächen insbesondere durch Privatpersonen und Interessengruppen umfasst. Nach der Idee der Ökonomie des Teilens soll der Nachfrager das geteilte Objekt nicht erwerben, sondern vorübergehend benutzen, bewohnen beziehungsweise bewirtschaften. [Gabler Wirtschaftslexikon: Definition Sharing Economy]

Unterschiedliche Ausprägungen der Entgrenzung sind die Globalisierung im Räumlichen [Trendthema Glokalisierung] und Post Privacy [Trendthema Post Privacy] im Virtuellen: Glokalisierung bezeichnet die Gleichzeitigkeit von weltweiter kultureller Konvergenz und von Rückbesinnung auf lokale und regionale Besonderheiten. Während die weltweite Digitalisierung eher ein Treiber der Globalisierung ist, erfordert Lokalität eine Form von räumlicher Präsenz. Mit weltumspannenden Kommunikationsmöglichkeiten zu vernachlässigbaren Grenzkosten ging ein Schub für die Konvergenz einher. Die Auflösung des Raumes hat mit der Immersion in virtuelle Welten und der netzwerkartigen Neuverknüpfung von sozialen Beziehungen im Digitalen zum scheinbaren Bedeutungsverlust des Lokalen und der Territorialität geführt. Zugleich lässt sich eine Wiederentdeckung des lokalen physischen Raumes bei der Ausgestaltung von IT-Infrastruktur beobachten. Getrieben durch Datenschutzbedenken wird beispielsweise an Lösungen für ein auf dezentralen Servern ausgeführtes globales soziales Netzwerk gearbeitet. In der globalen digitalen Welt wird es für eine wachsende Zahl von Nutzerinnen und Nutzern wichtig, wo der Server mit den eigenen Daten steht,

wer darauf Zugriff hat und welchen Gesetzen die dort gespeicherten Daten unterliegen. Ortsbezogene Dienste erlauben die Rückbindung konkreter Orte an eine konvergente, virtuelle Welt.

Die Diskussion um Post Privacy beziehungsweise das Ende der Privatheit resultiert aus der freiwilligen und unfreiwilligen Datenoffenbarung in sozialen Netzwerken, beim Online-Einkauf, der Nutzung von Smartphones oder in Sensornetzwerken. Vernetzung, Bilderkennung und Analysemöglichkeiten für große, auch unstrukturierte Datenmengen eröffnen neue Möglichkeiten der Beobachtung jedes Einzelnen. Es stellt sich die Frage, ob angesichts der für die Teilnahme am gesellschaftlichen Leben unvermeidlichen Datenoffenbarung und des einfachen Datenzugriffs die Aufrechterhaltung von Privatheit in unserem heutigen Verständnis überhaupt noch möglich ist. Diese empirische Frage lässt sich auch normativ wenden: Statt eines aussichtslosen Abwehrkampfes könnte die gezielte Offenlegung personenbezogener Daten neue soziale Normen entstehen lassen.

Jenseits der psychologischen Funktion als Rückzugsgebiet erlaubt Privatheit das Verbergen und Vergessen diskreditierender Daten, was dem gesellschaftlichen Zusammenhalt förderlich sein kann. Dieses Verbergen geht stets mit dem Risiko des Entdeckens und der Skandalisierung einher. Fraglich ist, ob bei prinzipieller Offenheit der Daten die alten Mechanismen der medialen Aufdeckung von Einzelaspekten weiterhin Erfolg versprechen. Die Offenlegung alles Privaten könnte zu einer neuen Dimension gesellschaftlicher Toleranz führen. Ob sich dieser gesellschaftliche Wandel angesichts einseitig verfügbarer Abhör- und Analysemöglichkeiten als stabil erweisen würde, bleibt eine offene Frage.

Möglichkeiten

- Überwindung herkömmlicher technischer und gesellschaftlicher Grenzen
- flexible und dynamische Lebensgestaltung
- neue Formen von Gemeinschaften
- Offenheit kann mit einer neuen Kultur der Transparenz und Toleranz einhergehen

Wagnisse

- vollständige, unfreiwillige Offenlegung des Privaten
- Privatheit wird zu einem Privileg für technisch Versierte und Wohlhabende
- Informationsasymmetrien zwischen Individuen, Gruppen und Organisationen schaffen umfassende Kontrollmöglichkeiten und / oder Konformitätszwänge

2.5 SMARTIFIZIERUNG

Dinge aller Art mit Intelligenz anzureichern, wird auch als Smartifizierung bezeichnet. Möglich wird dies durch Miniaturelektronik und -sensorik, das heißt, durch Kleinstkomponenten mit elektromechanischen und elektronischen Teilen. Dadurch verfügen diese Dinge über neue Fähigkeiten, die über ihren ursprünglichen Zweck hinausgehen.

»Das Adjektiv ›smart‹ scheint gegenwärtig unverzichtbar, wenn es um die Charakterisierung innovativer Produkte und Dienstleistungen geht, die durch die Konvergenz der elektronischen Medien ermöglicht werden. Es beginnt bereits beim in den Sprachgebrauch übernommenen Anglizismus des Smartphone und findet sich darüber hinaus in zahlreichen Begrifflichkeiten wie zum Beispiel bei Smart Home, Smart Service, Smart Grid, Smart Assistant, Smart Mobility, Smart Governance, Smart City und sogar in der Vision eines Smart Planet.« [VDI/VDE-IT 2011]

Mehr Unterstützung, mehr Sicherheit, mehr Komfort, mehr Lebensqualität durch intelligente elektronische Helfer erhoffen sich Menschen verschiedenen Alters. Ob Selbstvermessung und Selbstoptimierung für mehr Gesundheit und Fitness, Assistenzsysteme für benachteiligte Menschen oder ein altersgerechtes Leben – die Anwendungsbereiche sind beträchtlich.

Ein Beispiel hierfür sind Wearables [Trendthema Wearables], Miniaturelektronik und -sensorik, die am Körper getragen wird und somit jederzeit verfügbar ist. Wearables erfassen und verarbeiten Körperdaten und leiten diese weiter. Sie können dabei als separate Accessoires in Form von Armbändern, Uhren oder Kopfhörern genutzt werden oder aber als zusätzliche, integrierte Funktionalität auftreten, beispielsweise in Bekleidung und Brillen. Aktuelle Forschungen gehen noch einen Schritt weiter, indem sie sich mit sprichwörtlichen »embedded« Wearables auseinandersetzen, die als Tattoo auf der Haut getragen oder sogar subkutan implantiert werden.

Smartifizierung nennt man die Anreicherung von Dingen aller Art mit Intelligenz. Mittels Miniaturelektronik und -sensorik verfügen diese Dinge über neue Fähigkeiten, die über ihren ursprünglichen Zweck hinausgehen.

Das Konzept von Wearables ist nicht neu. Seit 1979 gibt es den Walkman und im Gesundheitsbereich sind Herzschrittmacher und Hörgeräte etablierte Instrumente. Neu ist jedoch die Ausweitung auf zahllose andere Anwendungsfelder, die durch zunehmende Miniaturisierung und Kommunikationsmöglichkeiten der Bausteine sowie geringere Kosten möglich wird. Zu den derzeit besonders aktiven Entwicklungsbereichen zählen etwa Fitness und Wellness mit Messung des Bioprofils sowie die Medizin mit der Überwachung von Körperfunktionen und der Erweiterung eigenständiger Handlungsmöglichkeiten eingeschränkter Personen. Basierend auf der Datenverarbeitung können von Wearables individuelle Verhaltensänderungen ebenso ausgehen wie möglicherweise auch die verhaltensabhängige Differenzierung von Versicherungspolicen und neue Impulse für die Gesundheitsforschung.

Der Markt für Uhren und Armbänder mit Zusatzfunktionen wie etwa Pulsmesser als Smartphone-Zusatz oder -Ersatz hat sich in der letzten Zeit stark weiterentwickelt. Die aktuelle Gerätegeneration schüttelt langsam die Kinderkrankheiten ab und bietet zunehmend Lösungen für kritische Problemfelder wie Stromspeicher und -verbrauch sowie standardisierte Schnittstellen. Für optische Brillen mit erweiterten Funktionen wie Bildeinblendung zeichnet sich absehbar kein Durchbruch zur verbreiteten Anwendung im Alltag ab. Sie bleiben derzeit auf kommerzielle Anwendungen etwa im Bereich der Lagerhaltung und Logistik beschränkt. Ein Grund für die fehlende Verbreitung dürfte bei der Usability [Trendthema Usability] liegen, da gänzlich neue Methoden der Darstellung, des Bedienkonzepts und der Integration gefragt sind.

Die gesellschaftliche Dimension solcher zunächst als Modegadgets oder zur Selbstoptimierung getragenen Wearables ergibt sich in erster Linie aus offenen datenschutzrechtlichen und sicherheitsrelevanten Fragen. Im Kontext von Bring Your Own Device

führen Wearables langfristig zu einer Einbettung ihrer Funktionen in öffentliche Infrastrukturen, was zur Ablösung stationärer Lösungen für Eingabemöglichkeiten und Authentifizierungsmaßnahmen führen kann. Hier ergeben sich Fragen nach der Abgrenzung zwischen Öffentlichkeit und Privatheit sowie den damit verbundenen rechtlichen und technischen Konzepten. Im Kontext von Big Data sind Wearables automatisierte Datenproduzenten, sodass Aspekte wie Datenhoheit, Datenschutz und -sparsamkeit, Eigentums- und Urheberrechte, Aussagekraft und Manipulationssicherheit betroffen sind.

Möglichkeiten

- realistischere Selbsteinschätzung durch eine objektivierte Beobachtung von Körperfunktionen
- Notfallsysteme für körperliche Ausnahmezustände können automatisiert angestoßen werden
- Datenerfassung und -analyse in neuartiger Qualität und Quantität eröffnen ein weites Spektrum medizinischer Forschung
- neue biometrische Authentifizierungsmöglichkeiten über das kombinierte biometrische Profil des Nutzers (zum Beispiel Venenprofil oder Bewegungsrhythmen)
- Kommunikationsbarrieren durch körperliche Beeinträchtigungen können überwunden werden

Wagnisse

- erfasste Daten sind sensibel und erfordern eine Pseudo- oder Anonymisierung
- ermöglicht eine einfache Profilbildung, die zu Problemen wie sozialer Ausgrenzung und Mobbing führen kann
- vertieft digitale Gräben, etwa durch neue, miniaturisierte Bedienkonzepte
- scheinbar objektive Selbstbeobachtung kann in fragwürdigen Selbstdiagnosen und Selbstbehandlungen münden
- Abstimmung zwischen Nutzen und Datenschutz bei Festlegung des Umfangs an Kommunikation zwischen Wearables

3.

HERAUSFORDERUNGEN DURCH DIE DIGITALISIERUNG

Aufgrund der zunehmenden Durchdringung unserer Gesellschaft mit Informations- und Kommunikationstechnik muss diese auch als »kritische Infrastruktur« eingestuft werden. Als kritische Infrastrukturen werden Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen bezeichnet, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. [Geschäftsstelle des UP KRITIS 2014] Der Schutz dieser Infrastrukturen ist nicht nur eine technische, sondern eine politische Aufgabe, die durch UP KRITIS[3] unterstützt wird. »Sichere Gesellschaften zum Schutz der Freiheit und Sicherheit Europas und seiner Bürger« sind im EU Forschungsprogramm Horizont 2020 als eine der gesellschaftlichen Herausforderungen definiert, die auch im Digitalen gewährleistet werden müssen. [Bundesministerium für Bildung und Forschung 2015]

3.1 (UN-)SICHERHEIT UND VERTRAUEN

Angst, Unsicherheit oder aber fehlendes Sicherheitsbewusstsein prägen zunehmend den Umgang mit Informationstechnik. »Die seit 2013 öffentlich bekannt gewordenen Aktivitäten ausländischer Nachrichtendienste sowie der millionen- und milliardenfache Identitätsdiebstahl haben zu einer Vertrauenskrise im Internet geführt.« [Bundesamt für Sicherheit in der Informationstechnik (BSI) 2014, S. 4] Aus Sicht der Bürger ist die schnelle Veränderung durch moderne Technologien häufig mit Angst im Zusammenhang mit der Informationsflut und Furcht vor Überwachung, Kontrolle und Ausschluss verbunden. »Angesichts der Differenz zwischen Furcht und Angst können wir sagen, dass wir zwischen Furcht und Vertrauen schwanken, wenn wir uns im Netz bewegen.« [Capurro 2005]

Die zunehmende Vernetzung von Objekten erfordert einen Vertrauensraum, der rechtlich geregelt und technisch konzipiert werden muss.

Vertrauen in die Sicherheit und Integrität der IT-Systeme und das Internet ist allerdings eine zentrale Voraussetzung für die Ausgestaltung der digitalen Zukunft von Bürgern und Gesellschaft. [Vertrauenswürdige digitale Identität] Daher nimmt der Bedarf an vertrauenswürdigen Diensten und vertrauenswürdiger Kommunikation für die Zivilgesellschaft, öffentliche Hand und Wirtschaft gleichermaßen zu.

Um das Vertrauen zu stärken, müssen Netze, Daten und Systeme vor Angriffen geschützt werden. Aufgrund der heutigen technologischen Dynamik handelt es sich bei Sicherheit jedoch nicht mehr um einen angestrebten, fixen Zustand. Sicherheit kann nur in einem kontinuierlichen Verbesserungsprozess aufrechterhalten werden. Schlagworte wie benutzbare Sicherheit, Privacy Divide, Verschlüsselung und digitales Vergessen werden zu Schlüsselthemen einer modernen IT-basierten Gesellschaft.

Durch die wachsende Digitalisierung der Gesellschaft stehen viele Menschen einer immer höheren Komplexität ihrer Lebenswelt und einer zunehmenden Virtualisierung der sozialen Welt gegenüber. Dabei ist es häufig nicht möglich, alle technischen Hin-

[3] UP KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen, www.upkritis.de

tergründe und Voraussetzungen zu verstehen. Vertrauen gewinnt somit zunehmend als »Mechanismus der Reduktion sozialer Komplexität« an Bedeutung. [Luhmann 2000] Zwar wird Vertrauen im täglichen Sprachgebrauch häufig auf die Qualität einer zwischenmenschlichen Beziehung beschränkt, es ist aber ein elementarer Bestandteil des Lebens. Ohne jegliches Vertrauen wäre der Mensch nicht fähig, Kommunikation oder Kooperation zu vollziehen, wodurch Vertrauen letztlich zu einer wichtigen Voraussetzung für die Nutzung öffentlicher IT wird. Gerade bei elektronischer Kommunikation und der Erbringung elektronischer Dienste ist Vertrauen von herausragender Bedeutung.

In einer Gesellschaft bildet sich Vertrauen in einem kulturellen Prozess: Es wird von den jeweiligen Gewohnheiten, Sitten und Normen bestimmt – kurz gesagt: von der Kultur. [Fukuyama 1995, S. 42] Vertrauen erfordert zunächst Zutrauen in die eigene Identität, darüber hinaus aber auch in die Kommunikationspartner und deren Identitäten. Hinzu kommt bei der Digitalisierung der Beziehungen das Vertrauen in die zugrunde liegenden Technologien.

Die Informationstechnik gilt heute jedoch als neuralgischer Punkt. Sie ist nicht nur komplex, sondern aufgrund von Öffnung und Einbindung ihrer Komponenten in unterschiedliche Umgebungen auch immer schwerer abzusichern. Mit Risikoanalysen, Sicherheits- und Datenschutzkonzepten versucht man, diese Komplexität zu strukturieren und handhabbar zu machen. Oftmals handelt es sich dabei jedoch nur um eine Momentaufnahme, das heißt, die zum jeweiligen Zeitpunkt bekannten Angriffsmuster und typischen Schwachstellen werden nur zu Beginn beziehungsweise in Intervallen analysiert. Eine fortlaufende Analyse und Weiterentwicklung ist zwar aufwändig, aber unerlässlich. Nicht betrachtete oder neue Bedrohungen führen häufig zu hohen Anpassungserfordernissen.

Um Sicherheit und Vertrauen zu stärken sind nicht nur sichere Technologien erforderlich, beispielsweise durch Zertifizierung und Standardisierung, sondern Konzepte für eine ganzheitliche Sicherheit. Die Hauptverantwortung für Sicherheit liegt dabei bei den Herstellern und Betreibern, sie darf nicht auf den Endnutzer abgewälzt werden. Um dies zu erreichen, muss Sicherheit so unabhängig wie möglich von Benutzer und Benutzung werden (Security by Design).

Herausforderungen

- Unsicherheit und Angst aufgrund der hohen Komplexität von Informationstechnik
- Cyberangriffe wachsen ständig und lassen sich kaum noch abwehren
- Unkenntnis darüber, wo sich die eigenen Daten befinden und ob diese dort sicher sind
- Herstellung von Vertrauensbeziehungen als Basis für IT-Prozesse

3.2 KONTROLLVERLUST UND ÜBERWACHUNG

Ob NSA-Affäre, die Daten-Sammelwut großer Internet-Plattformen oder das Ausspähen von Nutzern über Smart-TV-Geräte [Lischka 2014] – immer größer werden die Ängste von Bürgern vor ständiger Überwachung und dem Verlust der Privatsphäre.

Verpackt wird das Sammeln von Daten gern in Bequemlichkeitsfunktionen für die Nutzer. Amazons Echo beispielsweise ist ein sprachgesteuerter Alltagsassistent. »Er spielt Musik ab, erzählt Witze und legt Einkaufslisten an. Jedes Kommando geht an die Server des Unternehmens.« [Beuth 2014] Auch die bequemen Installationsfunktionen »Übernehmen« oder »Expresseinstellungen verwenden« von Microsofts Windows 10 dienen der Einräumung von weitgehenden Rechten zur Übertragung von Benutzerdaten an Microsoft. [Schulz 2015]

Die Ängste von Bürgern vor ständiger Überwachung und dem Verlust der Privatsphäre steigen.

Personalisierte Werbung ist ebenfalls ein wachsendes Geschäftsfeld. Dafür werden individuelle Daten der Benutzer über Surfverhalten oder Smartphone-Nutzung benötigt. Facebook etwa kooperiert mit Datenhändlern, um diese Potenziale auszuschöpfen. Voraussetzung ist allerdings, dass die Nutzer eindeutig identifizierbar sind. Nur wenn die Beteiligten wissen, welche Daten sich auf dieselbe Person beziehen, können die Daten miteinander verbunden werden. Offiziell erfolgt zwar eine Anonymisierung, in Wirklichkeit wird allerdings nur eine Pseudonymisierung mit Hashwerten für bestimmte personenbezogene Daten durchgeführt, die sich einfach zusammenführen lassen. [Wolfie 2015]

Auch Suchmaschinen sitzen an einer unermesslichen Datenquelle. In Verbindung mit erweiterten Diensten hat man als Nutzer keinerlei Wissen, welche Daten in welcher Form abgerufen und weitergeleitet werden. [Maurer et al. 2007] Die Filterblase in Suchmaschinen ist nur eine Ausprägung des Kontrollverlustes. »Es ist erstaunlich, wie wenigen Internetnutzern bewusst ist, dass Software auf Basis ihres Surfverhaltens, ihres Orts, ihrer Kontakte die Onlinewirklichkeit für sie vorsortiert.« [Lischka 2011]

Zusätzlich zum mehr oder weniger legitimen Sammeln von Daten existieren Bedrohungen durch Cyberkriminalität, die einen unbemerkten Kontrollverlust verursachen können. Dies kann der Diebstahl von Identitätsdaten oder die Verwendung des eigenen Rechners durch Unbefugte in einem Botnetz sein.

Herausforderungen

- bewusste oder unbewusste Beeinflussung menschlichen Verhaltens
- Verlust der Freiheit durch Überwachung der Bürger
- wachsende Analyse- und Verknüpfungsmöglichkeiten von Datensätzen
- Cyberkriminalität

3.3 DIGITALE UNVERSEHRTHEIT

Körperliche Unversehrtheit ist die Voraussetzung für den Zusammenhalt eines jeden Gemeinwesens. Im Digitalen dagegen erscheint diese Sicht weit weniger selbstverständlich. Neue Qualitäten von Identitätsdiebstahl und Cybermobbing erscheinen als Auswüchse einer digitalisierten Gesellschaft, die ihr Wertegerüst noch nicht abschließend auf die neuen Gegebenheiten übertragen hat. Auch die öffentliche Hand ist diesem Werteaufbau nicht immer förderlich, wenn beispielsweise ihre Datenbegehrlichkeiten als unverhältnismäßig angesehen werden. Digitale Unversehrtheit bedarf einer

allgemeinen Ethik für den zwischenmenschlichen Umgang im digitalen öffentlichen Raum und verlangt damit nach der erforderlichen gesellschaftlichen Auseinandersetzung. [Trendthema Digitale Unversehrtheit]

Mit der zunehmenden Digitalisierung und Vernetzung der Gesellschaft stellt sich die Frage, wie das Grundrecht der körperlichen Unversehrtheit auf die digitale Welt übertragen werden kann und welche faktische Schutzwirkung diese Übertragung entfalten kann. Körperliche Versehrungen sind in der Regel durch den Betroffenen unmittelbar erfahrbar und oft auch für das soziale Umfeld erkennbar. Im Digitalen hingegen sind Verletzungen nicht immer leicht zu erfassen. Sie passieren mitunter über Jahre, ohne vom Betroffenen bemerkt zu werden. Dies bedeutet aber keinesfalls, dass die Versehrungen nicht mit beträchtlichen Folgen verbunden sein können. So kann etwa die digitale Identität gestohlen oder absichtlich fingiert und in diffamierender Weise genutzt werden.

Digitale Unversehrtheit bedarf einer allgemeinen Ethik für den zwischenmenschlichen Umgang im digitalen öffentlichen Raum.

Digitale Identitäten sind auch aus anderer Perspektive relevant, nämlich wenn Anonymität dafür missbraucht wird, die digitale Persona zu schädigen. Jeder dritte Schüler wurde bereits einmal Opfer von Cybermobbing. Trotz des virtuellen Raums, in dem die Demütigungen und Drohungen stattfinden, sind die Auswirkungen auf das Leben der Opfer gravierend real. Die Nutzung gestohlener Identitäten, die Vortäuschung von Urheberschaft und Cybermobbing eröffnen ein weites Feld für Beeinträchtigungen wie Demütigungen, Verleumdungen, ungesetzliche Überwachung und Spionage.

Eine notwendige, aber nicht zwingend hinreichende Voraussetzung für die Gewährleistung digitaler Unversehrtheit ist die Einhaltung der technischen Anforderungen für IT-Sicherheit und Datenschutz: Verfügbarkeit, Integrität, Vertraulichkeit, sowie Transparenz, Nichtverkettbarkeit und Intervenierbarkeit. [Bock und Rost 2011] Digitale Unversehrtheit geht aber noch darüber hinaus. Es gilt, digitale Selbstbestimmung, also einen souveränen Umgang mit den eigenen Daten, anzustreben. Daraus ergibt sich beispielsweise auch die Notwendigkeit, Daten wieder löschen zu können. »Digitales Vergessen« und »digitaler Radiergummi« bezeichnen Ideen für bislang ungelöste gesellschaftliche und technische Probleme in dieser Hinsicht.

Die Wahrnehmung der staatlichen Verantwortung zeigt sich in diesem Themenfeld in vielfacher Weise. Mit dem Recht auf informationelle Selbstbestimmung und dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, kurz IT-Grundrecht, hat das Bundesverfassungsgericht Grundsätze des allgemeinen Persönlichkeitsrechts auf das Digitale anwendbar gemacht. Auf europäischer Ebene findet sich in der Datenschutz-Grundverordnung [Europäische Union 27.04.2016] unter anderem ein Recht auf Löschung (digitales Vergessenwerden).

Technische Lösungen können allerdings nur einen Ausschnitt der Problematik adressieren, da etwa anonymen Demütigungen und Verleumdungen so nicht begegnet werden kann. Zudem nähren datenschutzrechtlich kritisierte Vorhaben und die Aufdeckung von Geheimdienstaktivitäten Zweifel an der Angemessenheit staatlicher Lösungen. Zugleich stellt sich die Frage, inwieweit gesetzliche Regelungen die digitale Unversehrtheit der Bürger überhaupt schützen können respektive wie weit staatlicher Eingriff gehen sollte. Auch zur Beantwortung dieser Fragen bedarf es einer, gesamtgesellschaftlichen Werte-Diskussion. Ziel einer solchen Auseinandersetzung

muss die Bewusstseinsschärfung für im Digitalen oft schwerer zu identifizierende Regelverletzungen und die notwendige Anpassung bewährter Regeln sein. Da diese Diskussion eine globale sein muss, sind weder Wirtschaft noch Staat von der Verantwortung entbunden, sie zu begleiten und zu unterstützen.

Herausforderungen

- Selbstbeschränkung bei der Nutzung der technischen Möglichkeiten
- schwieriger Aushandlungsprozess gemeinsam respektierter Regeln
- anhaltende Ungleichheit durch Bedeutung von Technikkenntnissen und Medienkompetenz

3.4 DIGITALE GRÄBEN

Die Souveränität im Umgang mit digitalen Medien ist nicht bei allen Menschen in gleicher Weise ausgeprägt. Die stark gestiegene Online-Nutzung überwindet digitale Gräben nur scheinbar. [Trendthema Digitale Gräben] Rasante Technikentwicklung und sehr kurze Innovationszyklen führen zum Aufreißen immer neuer Gräben. Trotz aller Wandlung im Detail bleibt das Thema eines der gesellschaftlichen Teilhabe.

Durch Innovationsschübe entstehen immer wieder neue digitale Gräben. Die stark gestiegene Online-Nutzung überwindet digitale Gräben nur scheinbar.

Immer mehr gesellschaftlich relevante und persönlich wichtige Funktionen finden ihre Abbildung im Digitalen. Hier können neue Arbeitgeber gesucht, über soziale Netzwerke alte und neue Freundschaften gepflegt und zahllose Medien bis hin zur Hindustan Times eingesehen werden. Um diese Funktionen nutzen zu können, bedarf es eines Netzzugangs sowie entsprechender Bereitschaft und Kompetenzen. Dieser digitale Graben zwischen Nutzenden und Nonlinern scheint sich bei wachsender Nutzung des allgegenwärtigen Netzes zu schließen. Tatsächlich eröffnen sich jedoch neue Diskrepanzen, die durch digitale Innovationsschübe entstehen. Nutzungsformen wie mobiler Internetzugriff und die Akzeptanz körpernaher Sensoren kennzeichnen die aktuelle Differenz ebenso wie der Unterschied zwischen denjenigen, die ihre Privatheit schützen können, und jenen, die dies nicht können (Privacy Divide).

Der digitale Graben ist hinlänglich untersucht und spiegelt in vielerlei Hinsicht gesellschaftliche Chancen. Die Spaltung verläuft zwischen Jung und Alt, zwischen einkommensstark und einkommensschwach, zwischen städtischem und ländlichem Raum, zwischen hohem und niedrigem Bildungsgrad. Bereits mit einem dieser oftmals in Kombination auftretenden Merkmale kann die Netznutzung deutlich variieren. Unterschiede zeigen sich in den Bereichen Zugang, Kompetenz und Benutzung. Sie bestimmen zugleich die Möglichkeiten zur gesellschaftlichen Teilhabe: wirtschaftliche Gelegenheiten, politische Partizipation und soziale Integration.

Die Überwindung digitaler Gräben stellt somit eine gesamtgesellschaftliche Aufgabe von hoher Priorität dar. Dabei kann es nicht darum gehen, den bereits beträchtlichen Druck zur umfassenden Partizipation an der digitalen Welt zu erhöhen. Vielmehr geht es um Hilfestellungen und Übersetzungsleistungen. Für Nonliner müssen dabei insbesondere bei öffentlichen Angeboten alternative Kanäle offengehalten werden.

Herausforderungen

- Ausgrenzung Einzelner und ganzer gesellschaftlicher Gruppen
- Wegfall analoger Angebote und systematische Ausgrenzung aus sozialer Teilhabe
- Behinderung technischer und gesellschaftlicher Innovationen zur Vermeidung von Verwerfungen

3.5 DISRUPTIVE ENTWICKLUNGEN

Disruptive Entwicklungen sind Innovationen, die bestehende Technologien oder Dienstleistungen, aber auch kulturelle Gepflogenheiten teilweise oder komplett verdrängen und irreversible Veränderungen hervorrufen.

Ein zentrales Merkmal einer disruptiven Technologie ist ihre anfängliche Kommerzialisierung in einem Nischenmarkt beziehungsweise -segment, da die Technologie im Massenmarkt anfangs aufgrund ihrer Unterlegenheit bezüglich der wichtigsten Leistungsattribute im Vergleich zur herkömmlichen Technologie nicht attraktiv ist. [Weitert 2014, S. 14–15]

Einige Beispiele für disruptive Technologien listet Horton [Horton 2015] auf: Waren es in der Vergangenheit die Dampfmaschine oder die Glühlampe, in der Gegenwart Smartphones oder die digitale Fotografie, so könnten es in Zukunft 3D-Drucker oder Roboter sein. Es ist allerdings nicht die Technologie allein, die diese Veränderungen hervorruft. Das mp3-Format hat seinen Durchbruch von einer zukunftsweisenden Technologie zu einem weltweiten Standard erst in Verbindung mit dem Internet und geeigneten mp3-Playern erreicht. [Fraunhofer-Institut für Integrierte Schaltungen IIS 2012]

Die Folgen disruptiver Entwicklungen reichen von der Verdrängung etablierter Unternehmen bis hin zur Veränderung ganzer Branchen. Bestimmte Berufe wandeln sich oder werden gänzlich überflüssig. Die sozialen Auswirkungen sind radikal und müssen gegebenenfalls staatlich abgefedert werden. Gleichzeitig werden aber auch neue Geschäftsfelder und Märkte erschlossen, neue Geschäftsmodelle entwickelt und Verhaltensweisen verändert.

Herausforderungen

- Verdrängung von Firmen, Branchen oder Berufen
- unklare Auswirkungen und verspätete Reaktionen
- soziale Probleme durch plötzliche Veränderungen für Beschäftigte

4.

ÖFFENTLICHE IT

Die Digitalisierung der Gesellschaft berührt Kernfragen des Gemeinwesens. Welche Rolle dem öffentlichen Sektor in diesem Zusammenhang zukommt, ist eine nicht abschließend geklärte und in der kurzen Technologiegeschichte durchaus unterschiedlich beantwortete Frage. Das Konzept der öffentlichen IT bietet ein Analyseraster zur Behandlung dieser und ähnlicher Fragestellungen. [Öffentliche Informationstechnologie] Bevor öffentliche IT von anderen Konzeptionen und Ansätzen abgegrenzt werden kann (vgl. 4.2), bedarf es zunächst einer begrifflichen und konzeptionellen Annäherung (vgl. 4.1). Aus dieser ergibt sich eine breite Palette von Anforderungen an die Politik, die Verwaltung und den öffentlichen Sektor insgesamt (vgl. 4.3).

4.1 CHARAKTERISTIKA ÖFFENTLICHER IT

4.1.1 Die Heuristik des öffentlichen Raumes

Jedes Gemeinwesen kennt Räume, die zur Entfaltung gemeinsamer Interessen und Tätigkeiten genutzt werden. Ein Vereinsheim etwa dient dem Treffen Gleichgesinnter und dem Austausch über gemeinsame Interessen. Solche Vereinsräume sind zunächst nur für Mitglieder zugänglich. Sobald ihre Funktionen jedoch übergreifende Bedeutung erlangen, besteht ein öffentliches Interesse an ihrer Nutzung. Richtet der Verein etwa ein tief im Brauchtum verwurzeltes Volksfest in seinen Räumlichkeiten aus, gewinnen diese eine übergreifende Bedeutung für die Region. Die gesellschaftliche Funktion der von der Gemeinschaft bereitgestellten Leistung führt dazu, dass sich die Räume für Dritte öffnen. Die Zugänglichkeit für eine möglichst große Gruppe und die gesellschaftliche Funktion, die den Unterschied zu anderen frei zugänglichen Orten markiert, machen das Wesen des öffentlichen Raumes aus.

Die Zugänglichkeit und die gesellschaftliche Funktion machen das Wesen des öffentlichen Raumes aus.

Der mittelalterliche Marktplatz kann als Sinnbild für öffentliche Räume angesehen werden. Hier wurde gleich eine Vielzahl unterschiedlicher gesellschaftlicher Funktionen an einem Ort gebündelt: Neben dem eigentlichen Waren- und Dienstleistungsangebot diente er dem Austausch von Informationen und politischen Standpunkten, war oftmals der Verkehrsknotenpunkt des Ortes und brachte das gesellschaftliche Leben auf engem Raum zusammen.

Die heutigen Ausprägungen öffentlicher Räume sind vielfältig und ihre Abgrenzung muss mitunter neu gezogen werden. Die bereits genannten Vereinsräume können hier als Beispiel für zuvor verschlossene Räume herangezogen werden. Andere Räume werden gezielt für die öffentliche Nutzung geschaffen. Verkehrswege bieten hier ein anschauliches Beispiel. Die höchstrichterliche Feststellung, dass etwa Flughäfen als öffentliche Räume zu verstehen sind und dort dementsprechend Grundrechte unmittelbar Anwendung finden, spiegelt diese Sichtweise [Bundesverfassungsgericht 2011]. Aber auch Einkaufszentren lassen sich als für den gesellschaftlichen Bedarf der Güterversorgung geschaffene Räume verstehen, deren Funktionserfüllung eine allgemeine Zugänglichkeit erforderlich macht.

Die Heuristik des öffentlichen Raumes orientiert sich somit weniger an geographischen Räumen oder an Eigentumsverhältnissen, sondern berücksichtigt vielmehr gesellschaftliche Funktionen samt staatlicher Verantwortung und einem möglichst hohen Grad an freier Zugänglichkeit. Aus einer funktionalen Perspektive lassen sich öffentliche Räume als offene, gesellschaftliche Kommunikationssysteme verstehen. Solchen Kommunikationssystemen ist eigen, dass Akteure mit ganz unterschiedlichen Rollen und Selbstverständnissen interagieren: wirtschaftliche Rationalitäten treffen auf moralische, Eigeninteressen auf Gemeinwohlorientierung, weltanschauliche Überzeugungen auf pragmatische Ansichten. Diese Bündelungs- und in der Folge auch Koordinations- und Ausgleichsfunktion begründet die gesamtgesellschaftliche Bedeutung dieser Räume.

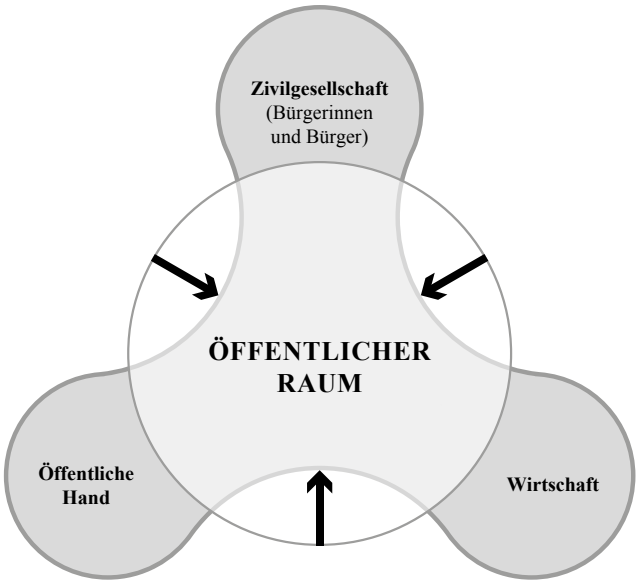

Abb. 3: Öffentlicher Raum und ihn konstituierende gesellschaftliche Subsysteme

4.1.2 Begriffliche Annäherung an öffentliche IT

Die Heuristik des öffentlichen Raumes eröffnet Anknüpfungspunkte für die begriffliche Annäherung an öffentliche IT, die am ersten Teil des Begriffspaares ansetzen kann. Öffentlich bedeutet zunächst die prinzipiell freie Zugänglichkeit des damit Bezeichneten. Möglichst geringe Zugangsbarrieren für möglichst breite Bevölkerungskreise können damit als substanziell für die Begriffsfassung angesehen werden. Die Interpretation dieser Kriterien unterliegt jedoch wiederum einem weiten Spielraum, wie sich im interkulturellen Vergleich besonders anschaulich verdeutlichen lässt. So wird im kontinentaleuropäisch geprägten Sprachgebrauch und Staatsverständnis der Begriff »öffentlich« in der Regel auch mit staatlich respektive quasistaatlich oder politisch

assoziiert. Im Gegensatz dazu betonen angloamerikanische Sprecher eher die private und privatwirtschaftliche Seite. »Going-public« bezeichnet dort einen Börsengang und eben keine politische Kampagne.

Der Begriff »öffentlich« bewegt sich demnach in einem Spektrum, das sich von staatlich und gesetzlich auf der einen Seite bis zu privatwirtschaftlich und persönlich auf der anderen Seite aufspannen lässt. Zusätzlich beschreibt er die Differenz zwischen offen und geschlossen. Während sowohl staatliche als auch persönliche Daten, Informationen, Gegenstände und Leistungen zunächst nicht für Dritte bereitstehen, zeichnen sich öffentliche Daten, Informationen, Gegenstände und Leistungen durch eine möglichst leichte Zugänglichkeit aus.

öffentlich zugänglich	Webseite Leserbrief Blogeintrag	Gesetze offene Verwaltungsdaten öffentliche Konsultationen
nicht zugänglich	Tagebucheintrag Gespräche am Frühstückstisch Betriebsgeheimnisse	Bürgerdaten, zum Beispiel Steuerbescheide Geheimdienstinformationen Staatsgeheimnisse
	privatwirtschaftlich / persönlich	staatlich / gesetzlich

Abb. 4: Beispiele öffentlicher und nichtöffentlicher Informationen

Im Gegensatz zu öffentlicher IT lässt sich private IT demnach durch die Anwendung von Informationstechnologie in einem abgeschlossenen und dadurch privaten Raum charakterisieren. Dass sich diese theoretisch klare Abgrenzung empirisch immer weniger aufrechterhalten lässt, zeigt das Bild eines nicht verbundenen Familienrechners: Die große Mehrzahl der privaten Haushalte ist breitbandig an das Internet angebunden. [Statistisches Bundesamt 2016] Mit der Verbreitung von Smartphones und der Nutzung von webbasierten Applikationen wird die Konnektivität auf immer mehr Lebensbereiche übertragen. Durch smarte Technologien im Internet der Dinge lässt sich zu einem beträchtlichen Grad eine Entkoppelung der Daten und der Datenübermittlung von Personen erwarten. Eine von der Außenwelt abgeschlossene, in diesem Sinne rein private Nutzung von IT lässt sich immer weniger beobachten.[4]

Ähnlich verhält es sich mit staatlicher IT. Wenn ein zentraler Aspekt von E-Government die Verlängerung zuvor verwaltungsinterner Prozessketten nach außen ist, dann beeinflussen organisationsinterne Abläufe zunehmend ihre Umwelt. Der Trend zur Offenlegung von Verwaltungsdaten deutet in die gleiche Richtung. Dabei gilt es fest-

[4] Hierbei ist zwischen Kommunikationsbeziehungen beziehungsweise der Nutzung öffentlicher Infrastrukturen und den gegebenenfalls vertraulichen Kommunikationsinhalten zu unterscheiden, wobei gleichzeitig ein Trend zur Verschlüsselung beobachtet werden kann.

zuhalten, dass die zunehmende Verschmelzung von staatlicher IT und öffentlichem Raum eben nicht aus der sprachlichen Analogie zwischen staatlich und öffentlich erwächst. Bezogen auf Informationstechnik muss also eine Differenz im Verständnis zu anderen Definitionen von öffentlich konstatiert werden.

Der zweite Teil der begrifflichen Annäherung erscheint zunächst ungleich einfacher. Informationstechnik bezeichnet die Verarbeitung von Informationen respektive Daten sowie die hierfür benötigte Hard- und Software. Ein abstraktes Modell der IT umfasst also die Verarbeitung der Daten, die Schnittstellen zur Ein- und Ausgabe von Daten und die Daten selbst. Die Schnittstellen von IT-Systemen umfassen auch Kommunikationsfunktionen, sodass sich die Unterscheidbarkeit zwischen Systemen der Informations- und der Kommunikationstechnik weiter verringert. Bereits heute lässt sich eine weitgehende Konvergenz dieser Technologien feststellen, die zunehmend auch den Bereich der Unterhaltungselektronik umfasst. Die Funktionen von IT haben sich damit, ausgehend von der Speicherung und Verarbeitung von Daten, dramatisch weiterentwickelt. Immer mehr Bereiche aus Wirtschaft und Gesellschaft greifen auf Informationstechnologien zurück, sodass der IT eine Querschnittsfunktion zukommt wie kaum einer anderen Technologie. Zugleich fungiert sie als Innovationstreiber insbesondere in ehemals IT-fernen Branchen.

Die Durchdringung von Branchen und Lebensbereichen mit informationstechnischen Komponenten und Konzepten erfährt eine immer stärkere Dynamik. Die digitale Repräsentation von Gegenständen und intelligente Formen der Auswertung enormer Datenmengen markieren neue Sprünge in dieser Entwicklung. Handelt es sich im Kern um IT, so werden die Gesamtphänomene meist unter dem Stichwort der Digitalisierung angesiedelt. Der Siegeszug der IT geht also mit ihrer immer schwierigeren Abgrenzbarkeit einher.

4.1.3 Öffentlicher Raum und öffentliches Gut

Öffentliche Güter zeichnen sich durch Nicht-Ausschließbarkeit und Nicht-Rivalität im Konsum aus.

Die Digitalisierung bleibt nicht ohne Auswirkungen auf den Staat und den öffentlichen Sektor insgesamt. Der Bedeutungszuwachs der Informationstechnologie führt zu einer doppelten Verantwortung staatlicher Institutionen, die sich mit den Konzepten vom öffentlichen Raum und vom öffentlichen Gut umreißen lassen. Das Internet als in diesem Kontext wohl grundlegendste informationstechnologische Errungenschaft bietet sich als Beispiel für diese Überlegungen an.

Öffentliche Güter gelten als ein paradigmatischer Fall von Marktversagen, der staatliche Eingriffe rechtfertigt. (Grundlegend: [Bator 1958]) In dieser ökonomisch geprägten Gütertypologie bilden öffentliche Güter den Gegenpol zu privaten Gütern. Sie unterscheiden sich von diesen hinsichtlich Ausschließbarkeit vom und Rivalität im Konsum. Vom Konsum reiner öffentlicher Güter kann niemand ausgeschlossen werden und ihr Konsum beeinträchtigt das Angebot nicht. Innere und äußere Sicherheit sind klassische Beispiele für rein öffentliche Güter, von denen alle in gleicher Weise profitieren. Die Produktion öffentlicher Güter führt zum Trittbrettfahrerproblem. Da niemand ausgeschlossen werden kann, ist es für jeden Einzelnen rational, keinen Beitrag zur Produktion öffentlicher Güter zu leisten. Reine Marktallokation führt hier also

zu einer Unterversorgung, die staatliches Eingreifen erforderlich machen kann. Wie im Fall der inneren und äußeren Sicherheit wird die gemeinschaftliche Finanzierung und Produktion dieser Güter oftmals über Steuern sichergestellt. Wenn das Internet die beiden Kriterien für ein öffentliches Gut erfüllt, ergibt sich daraus somit ein möglicher Handlungsbedarf des Staates.

Der Internetzugang von Privathaushalten und Personen ist zunächst kein rein öffentliches Gut, da der Zugang durch die Netzbetreiber kontrolliert und so beschränkt werden kann, dass die Zahlung einer Nutzungsgebühr durchsetzbar ist. Auch eine Rivalität im Konsum lässt sich schnell beobachten, wenn etwa auf der Letzten Meile viele Nutzer gleichzeitig auf Videostreaming-Dienste zugreifen wollen. Handelt es sich beim Internetzugang also zunächst nicht um ein rein öffentliches Gut, so lassen sich doch einige wesentliche Charakteristika eines solchen identifizieren. Rivalität im Konsum etwa tritt derzeit faktisch nur an wenigen Stellen im Netz auf. Gerade die Letzte Meile, auf der die Dienste zum Endkunden gelangen, ist eine solche Schwachstelle. Für weite Teile des Gesamtnetzwerks gelten diese Beschränkungen nicht. In der Gesamtbetrachtung fällt die Rivalität im Konsum also sehr schwach aus, was zum Beispiel aus niedrigen Grenzkosten für die Bereitstellung weiterer Bandbreite resultiert. Dies könnte sich allerdings mit rasant steigendem Datenverkehr, der aktuell insbesondere durch Streaming-Dienste bedingt ist, absehbar ändern. Solche Engpässe können auch politisch relevante Diskussionen etwa um die Netzneutralität anstoßen. Eindrucksvoll zeigte sich das beim Versuch, Geschwindigkeitsbeschränkungen für Festnetzanschlüsse einzuführen, nachdem diese ein festgelegtes Datenvolumen verbraucht haben.

IT-Netze sind eine kritische Infrastruktur, für die dem Staat eine Gewährleistungsverantwortung zufällt.

Auch die Ausschließbarkeit erweist sich bei näherer Betrachtung als lückenhaft. Freie WLAN-Hotspots sind hier ein prominentes Beispiel. Zugleich werden die Zugangswege vielfältiger. War es vor einem Jahrzehnt noch klassischerweise der über Telekommunikationskabel angeschlossene Computer, werden heute immer mehr Endgeräte und Objekte mittels verschiedener Technologien über das Internet vernetzt. Eine solche nicht immer bewusste Vernetzung scheint den Aspekt der Ausschließbarkeit eher umzudrehen: Faktisch stellt sich immer weniger die Frage nach der Ausschließbarkeit, sondern vielmehr die, ob die Bürger noch frei über den Nichtzugang zum Netz entscheiden können.

Das Internet weist also durchaus wesentliche Charakteristika öffentlicher Güter auf. Hinzu kommt, dass der öffentlichen digitalen IT-Netzinfrastruktur für Wirtschaft und gesellschaftliche Teilhabe eine so überragende Bedeutung zukommt, dass sie sich als kritisch ansehen lässt. Ein Ausfall des öffentlichen Kommunikationsnetzes kann mit volkswirtschaftlichen, politischen und persönlichen Schäden verbunden sein, die mit denen eines Ausfalls des Stromnetzes vergleichbar sind. Dies trifft umso mehr zu, als immer mehr kritische Infrastrukturen ohne öffentliche IT-Netze nicht mehr einwandfrei funktionieren können. Die Gewährleistung des Funktionierens der öffentlichen IT-Infrastruktur wird damit zur Staatsaufgabe, die es durch geeignete technische und organisatorische Maßnahmen zu erfüllen gilt. Wichtig ist dabei nicht die Art der Leistungserstellung oder der Typ des Leistungserstellers. Ob die IT-Infrastruktur durch eine staatliche Instanz oder durch privatwirtschaftliche Akteure aufgebaut und betrieben wird, ist in dieser Hinsicht unerheblich. In historischer Perspektive unterlag bei-

spielsweise die Art der Leistungserstellung in der Elektrizitätswirtschaft beträchtlichen Schwankungen zwischen privatwirtschaftlicher, staatlicher und kommunaler Zuständigkeit. [Otter und Weber 2012] In jedem Fall jedoch wird der Staat in der Verantwortung gesehen zu gewährleisten, dass die Infrastruktur betrieben und für alle Interessierten in geeigneter Weise nutzbar gemacht wird. Aus der Betrachtung der Internet-Infrastruktur als öffentliches Gut ergibt sich somit ein Dreiklang öffentlicher Verantwortung für ihre Bereitstellung: Sie ist eine kritische Infrastruktur, für die dem Staat eine Gewährleistungsverantwortung zufällt, was bis zur Aufnahme des Netzzugangs in den Katalog kommunaler Daseinsvorsorge reicht.[5]

Nicht nur Zugang und Infrastruktur, auch die Ausgestaltung digitaler Räume berührt staatliche Verantwortung. Hier kann an die Überlegungen zum öffentlichen Raum angeknüpft werden (vgl. 4.1.1). Je mehr gesellschaftliche Funktionen von digitalen öffentlichen Räumen übernommen werden, desto wichtiger wird die Einhaltung gesellschaftlich geteilter Regeln im Digitalen. Dass beispielsweise auch der Digitalverband Deutschlands den »Staat als Gestalter der digitalen Welt« in die Pflicht genommen und damit die Chancen für eine rein marktwirtschaftliche Selbstorganisation als gering bewertet hat [Bitkom 2012b], unterstreicht die Notwendigkeit eines staatlichen Engagements.

Das Funktionieren der öffentlichen IT-Infrastruktur wird zur Staatsaufgabe, die es durch geeignete technische und organisatorische Maßnahmen zu erfüllen gilt.

Ebenso wie die Gewährleistung des Zugangs kann die Verantwortung für die Ausgestaltung digitaler öffentlicher Räume auf sehr unterschiedliche Arten wahrgenommen werden. Aufgrund der Komplexität der Materie müssen weite gesellschaftliche Kreise einbezogen werden. Dies gilt gleichermaßen für eigene Angebote der öffentlichen Hand, indem sie nutzerzentriert entwickelt und ausgestaltet werden, ebenso wie für Regulierungsfragen, wenn die Möglichkeiten der Selbstregulierung unter Gesetzesvorbehalt intensiv sondiert werden. In jedem Fall zählt ein Kanon an Abwehrrechten der Bürger gegenüber staatlichen Eingriffen im Digitalen zu dieser Ausgestaltungsverantwortung.

4.2 DAS KONZEPT DER ÖFFENTLICHEN IT

Die dreifache Annäherung an öffentliche IT hat gezeigt, dass eine an das Alltagsverständnis angelehnte Begriffsfassung dem Phänomen nicht gerecht werden kann. Ein solches Alltagsverständnis grenzt öffentliche IT von nichtöffentlicher respektive privater IT ab. Ein mustergültiges Beispiel für so verstandene öffentliche IT wäre etwa die AusweisApp: Vom Staat zum freien Download öffentlich bereitgestellt, erfüllt diese Software zur Nutzung der Online-Ausweisfunktion des Personalausweises alle Aspekte der begrifflichen Annäherung in klar abgrenzbarer Weise. Wie bereits unter 4.1.2 diskutiert, lässt sich eine solche trennscharfe Abgrenzung jedoch immer weniger aufrechterhalten. Der Bedeutungszuwachs der IT und die damit einhergehende Ent-

[5] In globaler Perspektive wird schnell deutlich, dass diese staatliche Verantwortung derzeit in weiten Teilen der Welt nicht wahrgenommen wird respektive wahrgenommen werden kann. S. hierzu etwa: World Bank [World Development Report 2016: Digital Dividends 2016]

grenzung stehen dem entgegen. Zudem bleibt bei der den Begriffen »öffentlich« und »IT« verhafteten Definition der Aspekt der gesellschaftlichen Funktionen und staatlichen Verantwortung unberücksichtigt. Dabei sind die Konzepte von öffentlichem Raum und öffentlichem Gut eng mit dem der öffentlichen IT verwandt.

Eine Begriffsfassung, die diese Aspekte berücksichtigt, muss die gesellschaftlichen und politischen Dimensionen des Wechselspiels aus technologischer Entwicklung und gesellschaftlicher Dynamik erfassen. Anders ausgedrückt: Öffentliche IT bezeichnet den gesellschaftspolitischen Gestaltungsanspruch an die Digitalisierung.

Das Konzept von öffentlicher IT hebt also, ausgehend von den informationstechnologischen Grundlagen, auf die gesellschaftlichen Implikationen und ihre politische Gestaltbarkeit ab. Der Untersuchungsgegenstand öffentlicher IT ist damit ein stetig komplexer werdendes Beziehungsgeflecht. Wie sieht dies genau aus?

Öffentliche IT bezeichnet den gesellschaftspolitischen Gestaltungsanspruch an die Digitalisierung.

Die Digitalisierung hat etablierte Wirtschaftssektoren von Grund auf verändert: Die Druckindustrie ist hier ein recht frühes Beispiel, wobei die aktuellen Entwicklungen möglicherweise diese transformierte Branche erneut zu Veränderungen zwingen, wenn etwa Druckerzeugnisse durch digitale Publikationen und Lesegeräte substituiert werden. Die Auswirkungen bleiben nicht auf die Wirtschaft beschränkt: Berufe verändern sich ebenso dramatisch wie der Arbeitsmarkt, das Bildungssystem sieht sich mit neuen Anforderungen konfrontiert und die Erstellung sowie Verbreitung von Informationsmaterialien ändern sich grundlegend.

IT und Digitalisierung treiben nicht nur die Gesellschaft, sie werden zugleich auch von ihr beeinflusst. Konsum- und Nutzungsverhalten sind hier mögliche Hebel, die sich an einem Zitat veranschaulichen lassen, das Bill Gates zugeschrieben wird: »In fünf Jahren wird das Tablet in den USA die beliebteste Form eines PCs sein.« [Dirscherl und Fogarty 2016] Was wie eine kühne und fast zutreffende Vision klingt, relativiert sich unmittelbar beim Blick auf das Entstehungsjahr 2002. Die Aussage bezog sich auf ein neues Produkt, das jedoch in der Folge kaum angenommen wurde. Erst mit knapp zehn Jahren Verspätung setzt sich das Tablet als ernstzunehmende Alternative insbesondere zu kleinen Notebooks durch.

Die wechselseitige Beeinflussung von informationstechnologischer und gesellschaftlicher Entwicklung erfährt in den letzten Jahren eine neue Dynamik. Es entstehen neuartige Wechselwirkungen, die längst nicht mehr nur von – klassisch mit solchen Fragestellungen betrauten – Teildisziplinen wie der Techniksoziologie und Forschungsfeldern wie Informatik und Gesellschaft behandelt werden. Die Digitalisierung wird dabei maßgeblich durch öffentlich zugängliche IT-Infrastruktur beflügelt. Vernetzung bedeutet immer auch einen Grad der Öffnung zuvor möglicherweise abgeschlossener Systeme. Dies zeigt sich im Privaten ebenso wie im Arbeitsumfeld, in dem einzelne oder nur intern vernetzte Computer inzwischen die Ausnahme bilden. Unterschiedliche Endgeräte und zukünftig vermehrt auch Alltagsgegenstände werden mit Internetzugang ausgestattet.

Die durch die öffentliche IT-Infrastruktur dynamisierte Digitalisierung erfasst Personen und Organisationen ebenso wie gesellschaftliche Funktionssysteme und die Gesamtgesellschaft. Aus einer gesellschaftlichen Perspektive stellt sich dabei die Frage, welche Teile der Gesellschaft von der Digitalisierung besonders betroffen sind und sie zugleich nachhaltig beeinflussen können.

Zunächst scheint die Digitalisierung ein stark wirtschaftlich geprägtes Phänomen zu sein. Konzerne nutzen Technologien und tragen sie in die Fläche. Ihre Innovationskraft bestimmt wesentlich, welche technischen Möglichkeiten faktisch zur Verfügung stehen. Dies verändert gerade auch das Wirtschaftssystem selbst. Nicht nur die IT-Branche ist starken Verwerfungen mit teils atemberaubendem Aufstieg und Fall von dominierenden Unternehmen unterworfen.

Die durch die Diffusion von Technologien ausgelösten Veränderungen reichen bis auf die individuelle Ebene. Digitalisierung verändert, wie wir kommunizieren und soziale Beziehungen pflegen, welche Medien den Zugang zur Welt eröffnen, wie wir arbeiten und vieles mehr. Aus der Perspektive der öffentlichen IT ist bemerkenswert, wie hierdurch aus dem Leben Vieler ein öffentliches Leben wird: Soziale Netzwerke fassen das eigene Leben übersichtlich und für Dritte zugänglich zusammen, das zuvor in verschlossenen und versteckten Tagebüchern niedergeschrieben wurde. Mit dieser Veröffentlichung gehen neue Vergemeinschaftungs- und gesellschaftliche Produktionsformen einher, die eine genauso große disruptive Kraft entfalten können wie neuste Technologien. Open-Source-Software und Wikipedia sind zwei eindrucksvolle Beispiele dafür, dass das Internet von Anbeginn an auch eine gesellschaftspolitische Vision war. Öffentliche IT bietet die Plattform und Formgebung für dieses von IT gestützte öffentliche Leben. Die Gestaltung digitaler öffentlicher Räume lässt sich mit den gesellschaftlichen Funktionen der Zivilgesellschaft fassen.

Digitalisierung verändert, wie wir soziale Beziehungen pflegen, welche Medien wir nutzen und vieles mehr. Aus der Perspektive der öffentlichen IT ist bemerkenswert, dass so aus dem Leben Vieler ein öffentliches Leben wird.

Gesamtgesellschaftliche Fragen sind immer auch politische Fragen oder, allgemeiner, Fragen des öffentlichen Sektors. Seine Gemeinwohlverpflichtung führt, wie die kurze Diskussion der Konzepte von öffentlichem Gut und öffentlichem Raum gezeigt hat (vgl. 4.1.3), zur Verantwortung, Funktionen der öffentlichen IT-Infrastruktur und der Sicherheit der digitalen öffentlichen Räume zu gewährleisten. Die Gestaltungsmöglichkeiten bleiben trotz der teilweise beklagten Einschränkungen durch Globalisierung und wirtschaftliche Machtmonopole beträchtlich. Auch die Beeinflussung des öffentlichen Sektors selbst darf trotz mitunter ernüchternder Befunde zum Stand des dortigen IT-Einsatzes [White Paper E-Government] nicht unterschätzt werden, spiegeln sich gesellschaftliche und mediale Änderungsprozesse doch sowohl in den öffentlichen Aufgaben und Regulierungsanforderungen als auch in der politikrelevanten öffentlichen Kommunikation.

Bei der Betrachtung des öffentlichen Sektors als gesellschaftliches Funktionssystem in der Digitalisierung wird erneut der doppelte Wortsinn von »öffentlich« augenscheinlich (vgl. 4.1.2). Die Öffnung der Verwaltung macht aus einem Teil ihres Leistungsangebotes ein öffentliches Gut, das einen öffentlichen Raum schafft – und damit zu einem öffentlichen Anliegen wird. Darüber hinaus interagieren nahezu alle übrigen gesellschaftlichen Funktionssysteme mehr oder minder stark mit Digitalisierungsphänomenen: Bildung, Wissenschaft, Kunst und Gesundheit, um nur einige zentrale zu nennen. Öffentlicher Sektor, Zivilgesellschaft und Wirtschaft unterscheiden sich von diesen durch einen größeren Gestaltungsanspruch bei Fragen der Digitalisierung. Diese Einschätzung ist keinesfalls eindeutig und nicht notwendig konstant. So konnte

etwa die Wissenschaft in frühen Entwicklungsstadien große Gestaltungsmacht entfalten. Unabhängig davon, ob diese Gestaltungsmacht auch mit einem entsprechenden Gestaltungsanspruch einhergeht, scheint sie in den letzten Jahren insbesondere in Relation zu wirtschaftlichen Dynamiken eher abzunehmen.

Aus der Perspektive der öffentlichen IT lässt sich die Betrachtung auf drei gesellschaftliche Funktionssysteme fokussieren. Dem öffentlichen Sektor kommt die Aufgabe zu, Gemeinwohlaspekte durch die Wahrung von Schutz- und Leistungsrechten durchzusetzen. Diese Gemeinwohlperspektive rechtfertigt die Betrachtung der Dynamiken digitaler Transformation mit einem Schwerpunkt auf Handlungsfelder und Handlungsnotwendigkeiten von Politik, Verwaltung und öffentlichem Sektor. Abbildung 5 fasst die Überlegungen zusammen.

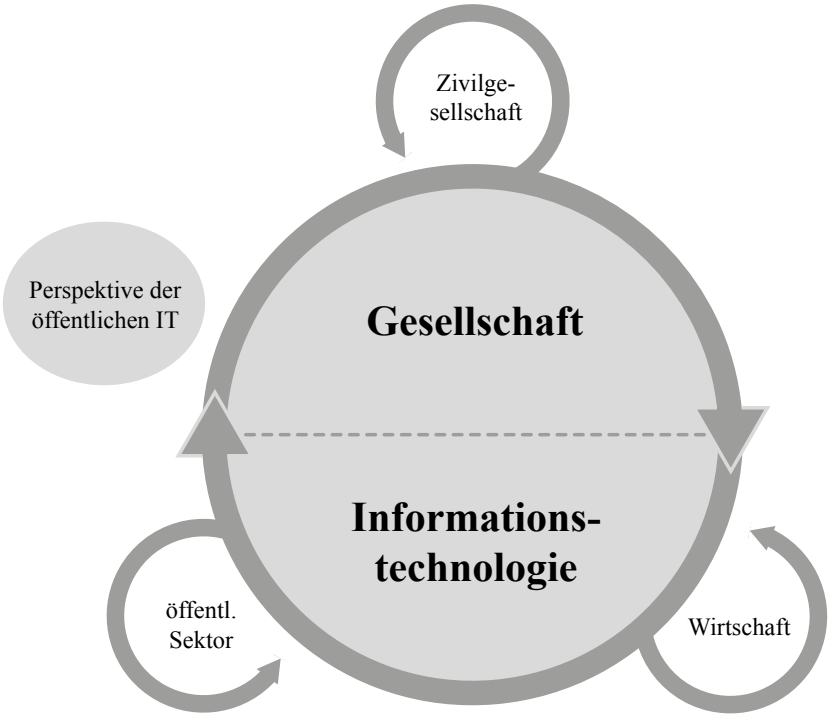

Abb. 5: Digitalisierungsdynamiken aus der Perspektive öffentlicher IT

Diese Reflexionen erlauben nun, die obige Definition, nach der die öffentliche IT den gesellschaftspolitischen Gestaltungsanspruch an die Digitalisierung bezeichnet, weiter fruchtbar zu machen. Kern des Konzepts bilden Prozesse der digitalen Transformation der Gesellschaft. Diese werden insoweit betrachtet, als sie gesamtgesellschaftlich sichtbar werden: durch die öffentliche Zugänglichmachung oder durch Wirkungen, die Fragen des Gemeinwohls betreffen. Ausgehend von diesem Begriffskern wird nach dem gesellschaftspolitischen Gestaltungsanspruch respektive dessen Ausgestaltung gefragt. Einen solchen Anspruch reklamieren Akteure aus unterschiedlichen gesell-

schaftlichen Gruppen und Funktionssystemen in unterschiedlicher Intensität. Die Überlegungen von Wirtschaftsvertretern zur Einrichtung sogenannter Mikrogesellschaften [Trendthema Peripherie], die exterritorial geschaffen und nach Start-up-Prinzipien geführt werden können, lassen sich als besonders deutliche Ausprägung eines solchen gesellschaftspolitischen Anspruchs verstehen. Ursprünglich obliegt die Ausgestaltung des gesellschaftlichen Zusammenlebens jedoch dem Wechselspiel aus Zivilgesellschaft, die in diesem Sinne die Gesamtheit der Bürger mit umfasst, und dem öffentlichen Sektor. Die Verantwortung, den Gestaltungsanspruch auch zu stellen, kommt dem öffentlichen Sektor also auch dann zu, wenn seine tatsächliche Gestaltung eher zurückhaltend ausfällt.

Die Definition führt zu einer ganzen Reihe von Fragestellungen, die sich aus der Befassung mit öffentlicher IT ergeben. Wie verändert sich die informationstechnische Basis der Digitalisierung? Welche Konsequenzen ergeben sich daraus für das Gemeinwesen? Welche Anforderungen richten Menschen und Gesellschaft an die Informationstechnologie? Wie ist der öffentliche Sektor in der Informationstechnologie aufgestellt? Welche zivilgesellschaftlichen und staatlichen Handlungsräume eröffnen oder verändern sich; zu welchen Handlungsnotwendigkeiten führt dies? Mit welchen Instrumenten lassen sich am Gemeinwohl orientierte Ziele effektiv und effizient erreichen? Wie lässt sich die politische, soziale und wirtschaftliche Teilhabe an der gesellschaftlichen Wohlfahrt in der Digitalisierung sicherstellen und ausbauen? Wie können digitale öffentliche Räume und digitale Identitäten sicher gestaltet werden? Wie kann gewährleistet werden, dass die Errungenschaften der Digitalisierung als öffentliches Gut erhalten bleiben? Kurz: Wie interagieren informationstechnologische Entwicklung und gesellschaftliche Verantwortung derzeit miteinander – und wie könnten sie miteinander interagieren?

Wesentlich für die Auseinandersetzung mit Fragestellungen öffentlicher IT ist das Verstehen der Wechselwirkungen zwischen Technik, Mensch und Gesellschaft.

Wesentlich für die Auseinandersetzung mit diesen Fragen bleibt also das Verstehen der Wechselwirkungen zwischen Technik, Mensch und Gesellschaft. Die reale Virtualität in der Digitalisierung knüpft hier an sozialkonstruktivistische Ansätze an. (Grundlegend etwa: [Berger und Luckmann 1972]) Diese gilt es vor dem Hintergrund der informationstechnologischen Entwicklung bis hin zur anwendungsorientierten Beratung für gesamtgesellschaftliche Fragen fruchtbar zu machen.

Diese Sichtweise auf öffentliche IT offenbart sich in vielgestaltigen Spannungsfeldern: zwischen ressortspezifischen Betrachtungen, disziplinären Vorgehensweisen und föderalen Ebenen; zwischen gesellschaftlichen Funktionssystemen wie Wirtschaft, Zivilgesellschaft und öffentlichem Sektor; zwischen visionärer Grundlagenforschung und konkreten Anwendungen; zwischen Gesellschaftspolitik und Technologie; und insbesondere zwischen Realität und hohen Erwartungen, die ein immer größerer Teil der Gesellschaft an öffentliche IT richtet und zunehmend als Anforderungen formuliert.

4.3 ANFORDERUNGEN AN DEN ÖFFENTLICHEN SEKTOR

So vielfältig die Ausprägungen öffentlicher IT sind, so verschiedenartige Anforderungen lassen sich an sie richten. Diese sind in hohem Maße von der spezifischen Domäne abhängig. Darüber hinaus lassen sich jedoch generelle Anforderungen identifizieren, die quer zu den einzelnen Handlungsfeldern liegen und entsprechend für die Konzeption als konstitutiv gelten können. Die Anforderungen werden an den öffentlichen Sektor gerichtet, der gegenüber anderen gesellschaftlichen Funktionssystemen den entscheidenden Vorteil hat, als ein vergleichsweise eindeutig zu identifizierender Adressat zu gelten. Dabei gilt es zu berücksichtigen, dass es sich bei öffentlicher IT um ein im Vergleich zu anderen staatlichen Aufgaben noch junges, seine Komplexität gerade erst entfaltendes Themengebiet handelt. Die konkrete staatliche Verantwortung gilt es entsprechend laufend neu zu bestimmen.

4.3.1 Infrastrukturbereitstellung und -betrieb gewährleisten

Öffentliche IT benötigt eine vernetzte Infrastruktur. Diese Infrastruktur weist viele Charakteristika eines öffentlichen Guts auf.

Allen hier herangezogenen Aspekten von öffentlicher IT ist gemein, dass sie eine vernetzte Infrastruktur für die Datenerfassung, -speicherung und -verarbeitung voraussetzen. Unabhängig von der auf ihr aufsetzenden Komplexität bedarf es zunächst dieser Infrastruktur. Eine solche Infrastruktur weist viele Charakteristika eines öffentlichen Guts auf, durch das weitergehende Wohlfahrtseffekte erst ermöglicht werden. Dass es hier zur partiellen Unterversorgung kommt, wie es für öffentliche Güter charakteristisch ist, lässt sich sowohl global als auch national in informationstechnologisch peripheren Gebieten beobachten.

Weite Teile der öffentlich zugänglichen IT-Netzinfrastruktur befinden sich in privatwirtschaftlichem Eigentum und werden privatwirtschaftlich betrieben. Die Privatisierung zuvor oftmals staatlicher Telekommunikationsunternehmen einerseits und die Öffnung der Märkte für neue Akteure aus dem In- und Ausland andererseits haben zu einer Dominanz privatwirtschaftlicher Bereitstellung geführt. Dies hat sich sowohl national als auch global für die digitale Vernetzung von Metropolen bewährt, wie die kurzen Innovationszyklen in der Übertragungstechnik eindrucksvoll zeigen. Es entstehen hierbei jedoch beträchtliche internationale und interregionale Ungleichgewichte. So ermöglichen dichte globale Kommunikationsnetze zwischen den industriellen Ballungszentren einen intensiven Datenaustausch bei gleichzeitiger Konkurrenz konvergierender Übertragungstechniken vor Ort, während sowohl ganze Staaten als auch dünn besiedelte ländliche Räume in Deutschland nicht von schnellen Zugängen profitieren können.

Der Bedeutungszuwachs des breitbandigen Netzzugangs, der etwa durch das Grundsatzurteil des BGH zum Schadensersatzanspruch bei dessen Ausfall unterstrichen wurde [Bundesgerichtshof 2013], führt zu einer Verantwortung der öffentlichen Hand für die Versorgung aller, wie sie auch in anderen Bereichen der Daseinsvorsorge gegeben ist. Dabei geht es stets um die Gewährleistung der konkreten Funktionen des Netzzugangs etwa für die regionale Wirtschaft, zur Realisierung von Homeoffice-

Konzepten oder zur Ermöglichung gesellschaftlicher Teilhabe. Dienstleistungen von allgemeinem öffentlichen Interesse müssen nicht zwangsläufig staatlich aufgebaut und betrieben werden. Die bestehenden Lücken zeigen aber staatlichen und kommunalen Handlungsbedarf, um der Gewährleistungsverantwortung in unterversorgten Gebieten gerecht zu werden.

Empirisch zeigt sich, dass die staatliche und kommunale Rolle über die Bereitstellung finanzieller Mittel hinausgeht. Die Breitbandversorgung der schleswig-holsteinischen Ämter Dänischenhagen, Dänischer Wohld und Hüttener Berge kann zur Veranschaulichung herangezogen werden [Betz 2012]. Erst ein Zweckverband zum Aufbau eines breitbandigen Kommunikationsnetzes konnte durch Selbstverpflichtung der Kommunen und nach Anpassung der technischen Lösungen die Versorgung sicherstellen. Die Bereitstellung selbst erfolgt nun zu akzeptablen Preisen und weit höheren als den erwarteten Übertragungsraten durch einen Privaten. Die Kombination aus angepasster Technik, kommunaler Selbstorganisation im Zweckverband, staatlicher Förderung und privatwirtschaftlicher Leistungserstellung hat die Versorgung der Region ermöglicht. Mit dem Breitbandbüro des Bundes (www.breitbandbuero.de), den Kompetenzzentren der Länder und der Vorstellung von beispielhaften Projekten und Ansprechpartnern ([BREKO 2016] als Beispiel) ist eine Voraussetzung für die Vernetzung von Akteuren geschaffen worden.

Auch aus der Bündelung von Anforderungen können Impulse für die flächendeckende Breitbandversorgung erwachsen. So basiert die Regulierung von LTE-Frequenzen im Bereich von 800 MHz durch die Bundesnetzagentur auf der üblichen Versteigerung von Frequenzblöcken an Mobilfunkprovider, sie umfasst aber auch eine Auflage für die Breitbandversorgung. [Bundesnetzagentur 26.11.2012] Diese Auflage besagt, dass zunächst schlechter versorgte Gemeinden mit Breitbandzugängen versorgt werden müssen, bevor der für Mobilfunkprovider technisch und wirtschaftlich interessante 800-MHz-Bereich auch in Ballungsgebieten freizügig genutzt werden kann. Interessant ist dabei, dass die Breitbandversorgung technologieneutral betrachtet wird. Die anzuschließenden Gemeinden, also insbesondere periphere Kleingemeinden, können auch durch kabelgebundene Lösungen versorgt werden.

Der Netzzugang entscheidet über die Möglichkeit, an der dynamischen Entwicklung der Digitalisierung mit ihren radikalen Innovationssprüngen zu partizipieren.

Bereits die Gewährleistung des Netzzugangs erfordert Kreativität in der Kombination der Ausgestaltungsinstrumente. Der Netzzugang selbst entscheidet über die Möglichkeit, an einer dynamischen Entwicklung mit radikalen Innovationssprüngen zu partizipieren. Der angemessene Zugang zu Kommunikationsnetzen berührt demnach Fragen der Gleichheit der Lebensverhältnisse und entscheidet über die Verteilung von Lebenschancen und gesellschaftlicher Teilhabe mit. Für die Nutzung öffentlicher Kommunikationsnetze ist der technische Zugang eine notwendige, nicht jedoch hinreichende Bedingung. Bezogen auf öffentliche IT bedarf es zur Sicherstellung gesellschaftlicher Teilhabe nicht nur des Zugangs zur Infrastruktur, sondern entsprechender Dienste sowie der Kompetenzen, diese zu nutzen. In diesem Sinne tangiert der Ausbau breitbandiger Netzinfrastruktur zugleich regionalökonomische, demografische und bildungspolitische Aspekte.

Wie umfänglich die zu koordinierenden Infrastrukturelemente sind, verdeutlicht die Diskussion über den Schutz kritischer Infrastrukturen [Bundesministerium des Innern 2009]. Hier wird zwischen technischen Basisinfrastrukturen und sozioökonomischen Dienstleistungsinfrastrukturen (Gesundheitswesen, Ernährung; Notfall- und Rettungswesen, Katastrophenschutz; Parlament, Regierung, öffentliche Verwaltung, Justizeinrichtungen; Finanz- und Versicherungswesen; Medien und Kulturgüter) unterschieden. Um funktionierende Infrastrukturen zu gewährleisten, bedarf es demnach der intensiven Zusammenarbeit, Abstimmung und Information unterschiedlichster Akteursgruppen. Wirtschaft und Verwaltung müssen ebenso Berücksichtigung finden wie Wissenschaft, Forschung, die Öffentlichkeit (Bevölkerung, Medien) sowie internationale und supranationale Einrichtungen.

Bereitstellung und Betrieb der erforderlichen öffentlichen IT-Infrastruktur berühren also in gleicher Weise Anforderungen, die sich aus ihrem Charakter als öffentliches Gut, aus dem Aspekt der Daseinsvorsorge sowie aus dem Schutz kritischer Infrastrukturen ergeben. Ungeachtet des empirischen und aktuell normativ-rechtlichen Primats privatwirtschaftlicher Leistungserstellung steht der öffentliche Sektor in der Verantwortung, das Funktionieren der Infrastruktur zu gewährleisten.

4.3.2 Innovationen anwenden und vorantreiben

Ein Gestaltungsanspruch lässt sich nur dann glaubhaft vermitteln, wenn öffentliche Stellen die Chancen der Digitalisierung selbst verantwortungsvoll nutzen.

Der staatliche Gestaltungsanspruch richtet sich nicht nur an die Verfügbarkeit der technologischen Basis für Wirtschaft und Gesellschaft, er betrifft auch staatliches Handeln selbst. Ein Gestaltungsanspruch für die Digitalisierung lässt sich nur dann glaubhaft vermitteln, wenn öffentliche Stellen die Chancen der Digitalisierung selbst verantwortungsvoll nutzen. Dabei zeigt sich die doppelte Wortbedeutung des Begriffs »öffentlich« auf andere Weise neu: das Handeln von Staat, Kommunen und anderen öffentlichen Einrichtungen bleibt nicht ohne Wirkung auf andere gesellschaftliche Subsysteme. Der öffentliche Sektor entfaltet in diesem Sinne stets eine beträchtliche Öffentlichkeitswirkung.

Die Wirkungen zeigen sich bereits bei der eigenen technischen Ausstattung. Staat, Kommunen und andere öffentliche Einrichtungen halten eine Vielzahl von IT-Infrastrukturbausteinen und Diensten vor. Einigen dieser IT-Bausteine öffentlicher Einrichtungen kommt eine gewichtige Funktion für die Entwicklung und Verbreitung von Innovationen zu. Beispielhaft ist hier die phasenweise beträchtliche Bedeutung der Wissenschaft für heute alltägliche Internetstandards zu nennen, die etwa die Entstehung des World Wide Webs erst ermöglicht haben. Aus solchen Mechanismen ergeben sich mindestens drei Aspekte, die hier Berücksichtigung finden müssen: die Effektivität und die Effizienz des Betriebs eigener Kommunikationsnetze und Dienste, die sich daraus ergebende Notwendigkeit der ebenen- und bereichsübergreifenden Zusammenarbeit sowie die Rolle des öffentlichen Sektors als direkter und indirekter Impulsgeber für die Entstehung und Verbreitung von Innovationen.

Die Frage nach effektiven und effizienten Kommunikationsnetzen und Diensten der öffentlichen Hand verweist auf einschlägige E-Government-Diskussionen. Öffentliche Einrichtungen verfügen oftmals über ausgereifte IT-Lösungen, die für ein spezi-

fisches Anforderungsprofil entwickelt wurden, das sich aus ihrer öffentlichen Aufgabe ergibt. Hier ist beispielsweise an die IT-Systeme der Sozialversicherungsträger zu denken, bei denen sich gleich eine Vielzahl von überaus anspruchsvollen Anforderungen kumuliert: große Datenmengen, die rechtssicher über lange Zeiträume gespeichert und bearbeitet werden müssen und an die hohe Anforderungen hinsichtlich Datensicherheit, Datenintegrität und Datenschutz gerichtet werden. Diese IT-Systeme wurden oftmals für die spezifischen Bedarfe der jeweiligen Einrichtung maßgeschneidert entwickelt. Die damit erzielte Effektivität der IT steht spätestens dann in einem Spannungsverhältnis zu ihrer Effizienz, wenn Systeme für eine Öffnung angepasst werden müssen. Zuvor nicht vorgesehene Kooperationen sind hier ebenso zu nennen wie die generelle Öffnung der Verwaltungsnetze hin zum Bürger und Kunden. Soll die IT des öffentlichen Sektors über öffentliche Netze nutzbar gemacht werden, kann dies mit einem Paradigmenwechsel ihrer Entwicklung und Bereitstellung einhergehen: Statt monolithischer Einzellösungen sind modulare Gesamtlösungen gefragt. Dabei birgt die Öffnung prinzipiell Effizienzpotenziale, die es schon aufgrund des Wirtschaftlichkeitsgrundsatzes im Haushaltsrecht zu realisieren gilt.

Existierende Insellösungen erklären sich nicht immer aus der Spezifität der Anforderungen, sondern auch aus historischen Pfadabhängigkeiten, bei denen einmal eingeschlagene Technologiepfade die zunächst offene Entwicklung maßgeblich beeinflussten. Solche auch in Kommunen vorzufindenden Einzellösungen stehen nicht nur dem unter anderem durch Cloud-Infrastrukturen ermöglichten Trend zur Virtualisierung und Modularisierung der IT entgegen. Sie verweisen aus der Verantwortung des Staates für öffentliche IT heraus auch auf die Notwendigkeit, Kooperationsmöglichkeiten zwischen föderalen Ebenen und Zuständigkeitsbereichen zu erleichtern. Allein die Bereitstellung der erforderlichen Informationen über föderale Ebenen hinweg ist mit beträchtlichen Anstrengungen verbunden. So ist es beispielsweise Aufgabe des Projektes »Föderales Informationsmanagement (FIM)« [IT-Planungsrat – Föderales Informationsmanagement 2015], unter Rückgriff auf wesentliche Vorarbeiten etwa aus den Vorhaben »Leistungskatalog für die öffentlichen Verwaltungen (LeiKa)« und »Nationale Prozessbibliothek (NPB)«, eine Vereinheitlichung in der Beschreibung von Informationen zu Verwaltungsvorgängen unter Wahrung der gegebenen Autonomiegrade zu erzielen. Die intensive Kooperation muss unter Zuhilfenahme solcher Projekte über Gebietskörperschafts- und Zuständigkeitsgrenzen hinweg aufgebaut und gepflegt werden. Dabei geben die fachlichen und regionalen Anforderungen den Rahmen für die gemeinsame Bearbeitung von Problemstellungen und ihre informationstechnische Abbildung vor.

Die beträchtlichen Anforderungen an die Informationstechnik staatlicher, kommunaler und anderer öffentlicher Einrichtungen führen zum dritten hier zu behandelnden Aspekt. Zur Erfüllung der anspruchsvollen öffentlichen Aufgaben muss der Staat sicherstellen, dass eine diesen Ansprüchen genügende IT zur Verfügung steht. Die aktive Beeinflussung bestehender Infrastrukturen, die Förderung nationaler IT-Forschung und der Einkauf zeitgemäßer respektive zukunftsweisender Lösungen sind dazu erforderlich. Hohe Sicherheitsanforderungen können sich dabei als wichtiger Treiber für die Entwicklung neuer Lösungen erweisen. Gerade angesichts der großen Bedeutung der IT für die Erstellung öffent-

Aus der Gestaltungsmacht des öffentlichen Sektors folgt zugleich eine Gestaltungsverantwortung.

licher Dienstleistungen und der ebenfalls großen Bedeutung öffentlicher Einrichtungen für die IT-Branche ergeben sich vielfältige Gestaltungsmöglichkeiten. Oftmals tritt der Staat als »Lead User« [von Hippel 1986] auf, der anspruchsvolle Lösungen als Erster zum Einsatz bringen muss oder aufgrund politischer Programmatiken einen solchen Einsatz anstrebt. In der Summe ergeben sich dadurch informationstechnische Gestaltungsmöglichkeiten für die öffentliche Hand, wie sie in kaum einem anderen Technologiefeld und seiner korrespondierenden Branche gegeben sind. Aus dieser Gestaltungsmacht folgt zugleich eine Gestaltungsverantwortung des öffentlichen Sektors.

Die Sichtbarkeit des öffentlichen Sektors steigert die Wirkung eigener Handlungen. Sie geht mit einer Vorbildfunktion für die Umsetzung der Digitalisierung einher – sowohl technisch als auch organisatorisch und politisch. Über den öffentlichen Einkauf wirkt diese Umsetzung zugleich direkt auf Umsatzchancen innovativer Anbieter.

4.3.3 Digitales Gemeinwesen mitgestalten

Öffentliche Räume als Kristallisationspunkte des Gemeinwesens entstehen mitunter selbstorganisiert, sind jedoch nicht notwendigerweise dauerhaft stabil. So wie mittelalterliche Marktplätze vorzugsweise im Schutzbereich der lokalen Herrscher entstanden, so können auch digitale öffentliche Räume nicht immer durch die sie tragende Community verteidigt werden. Wie sehr die gesellschaftliche Bedeutung solcher digitalen Räume inzwischen gewachsen ist, zeigt sich an dem derzeit wiedererstarkenden Trend der virtuellen Realität.

Digitale öffentliche Räume als kollektive Form realer Virtualität sind in besonderer Weise geeignet, Gemeinwohl und gesellschaftlichen Zusammenhalt zu befördern – oder zu beeinträchtigen.

Das Eintauchen in als nicht real verstandene Welten ist ein altes Phänomen. Allzu oft geht mit der Beschreibung eine Pathologisierung dieses auch als Immersion bezeichneten Verhaltens einher: Die Person löst sich aus als real definierten Kontexten und sammelt Erfahrungen in virtuellen Welten, die ihr weiteres Verhalten beeinflussen. Diese Welten müssen keineswegs IT-generiert sein, wie sich bei leidenschaftlichen Anhängern von Rollenspielen eindrucksvoll beobachten lässt. Die IT bietet jedoch umfassende neue Möglichkeiten, die längst eine direkte Ansprache gleich mehrerer Sinnesorgane erlauben. Visuelle Reize durch dreidimensionale Welten darstellende Brillen, haptische Eindrücke und Akustik zählen zur Ausstattung moderner virtueller Realitäten. IT wird daher ein beträchtliches Potenzial zur Intensivierung der virtuell zu sammelnden Erfahrungen zugesprochen. Diese Erfahrungen werden, wie sich in Anlehnung an das Thomas-Theorem [Thomas 1928] formulieren ließe, zunehmend realer in ihren Konsequenzen. Stärker noch als die prägende Wirkung von Massenmedien werden virtuell und nicht virtuell gesammelte Erfahrungen in ihren Wirkungen kaum mehr unterscheidbar sein.

Zugleich lassen sich virtuelle – oder besser: digitale – Elemente immer weniger von Alltagserlebnissen abgrenzen. Was unter »Augmented Reality« diskutiert wird, bleibt längst nicht mehr nur auf die spielerische Erweiterung der Weltwahrnehmung beschränkt. Digitale Assistenzsysteme bestimmen über den Alltag mit und beeinflussen entscheidend, ob beispielsweise Termine rechtzeitig wahrgenommen werden kön-

nen. Der Rückgriff auf digitale Helfer, die aktuell in Wearables (vgl. 2.5) ihren Ausdruck finden, führt zu einer Durchdringung des Alltags mit digitaler Technik. Dies gilt auch ohne eigene Nutzung, da die Umwelt immer mehr von digitalen Diensten beeinflusst wird. Smart Cities und Ambient Assisted Living [Trendthema Ambient World] markieren hier nur Extreme einer Welt, die immer weiter digitalisiert wird. Digitale öffentliche Räume als kollektive Form realer Virtualität sind in besonderer Weise geeignet, Gemeinwohl und gesellschaftlichen Zusammenhalt zu befördern – oder zu beeinträchtigen. Die Geschwindigkeit, in der sich mitunter Nachrichten unabhängig von ihrem Wahrheitsgehalt in sozialen Netzwerken verbreiten, bietet hierfür beeindruckendes Anschauungsmaterial. Entsprechend real sind die Auswirkungen von Angriffen auf diese Räume.

Für den öffentlichen Sektor ergeben sich daraus mindestens drei grundlegende Anforderungen. Zunächst gilt es, (1) die gesellschaftliche Teilhabe im Digitalen zu ermöglichen und zu unterstützen. Sowohl das Ob als auch das Wie der Abbildung im Digitalen respektive der Unterstützung durch das Digitale gilt es zu gestalten. Hierzu kann (2) das gezielte Angebot funktionaler Äquivalente zur dinglichen Welt zielführend sein. Das Austarieren von Anonymität und Identifizierbarkeit im digitalen Raum liefert hierfür ein Beispiel. Während in der Alltagswelt durch grundsätzliche Anonymität bei möglicher Bekanntheit und jederzeitiger Ausweisbarkeit ein komplexes und zugleich vertrautes Wechselspiel zu beobachten ist, müssen die funktionalen Äquivalente dazu im virtuellen Raum erst noch geschaffen werden. Schließlich gilt es, (3) diese öffentlichen Räume genauso sicher und vertrauenswürdig auszugestalten, wie es die Bürger von ihrem Marktplatz um die Ecke erwarten.

5.

MODELLIERUNG ÖFFENTLICHER IT

Modelle erlauben die Darstellung und Diskussion komplexer Sachverhalte, indem das zu beschreibende System abstrahiert und vereinfacht wird. Gleichzeitig werden damit bestimmte Zusammenhänge explizit hervorgehoben und können leichter erkannt werden. Aus diesem Grund sind technisch orientierte Modelle auch ein wichtiges Hilfsmittel, wenn die Digitalisierung der Gesellschaft und öffentliche IT diskutiert werden. Die Abstraktion führt allerdings auch dazu, dass nicht alle Details dargestellt werden können und bestimmte Aspekte eines Systems im gewählten Modell nicht sichtbar sind.

5.1 GENERISCHES IT-MODELL

Einfache, inzwischen allgemein bekannte Modelle der Datenverarbeitung stellen die Eingabe, die Verarbeitung (gegebenenfalls ergänzt um die lokale Speicherung) und die Ausgabe von Daten in den Mittelpunkt (vgl. 4.1.2). Dieses denkbar einfache Modell stellt zwar sehr anschaulich die Arbeitsweise eines Computers dar, macht aber nicht sichtbar, wie stark der Alltag mit Informationstechnik durchdrungen ist.

Ein abstraktes, generisches IT-Modell muss sich von dem einzelnen Computersystem lösen, wobei weiterhin die Daten im Mittelpunkt stehen. Die Verarbeitung der Daten erfolgt durch Anwendungen. Die Ausführung der Anwendungen sowie Speicherung, Transport und Bearbeitung der Daten erfordern einen technischen Unterbau, der im Modell ganz allgemein mit Infrastruktur bezeichnet ist. Diese grundsätzliche Einteilung zwischen Anwendung und Infrastruktur ist in einem weiten Bereich skalierbar und kann sowohl einzelne Computer als auch komplexe, vernetzte Systeme beschreiben. Der Dreiklang aus Daten, Anwendungen und Infrastruktur ist universell für die Digitalisierung und bildet ein wiederkehrendes Muster, unabhängig von Blickwinkel und Abstraktionsgrad seiner Betrachtung.

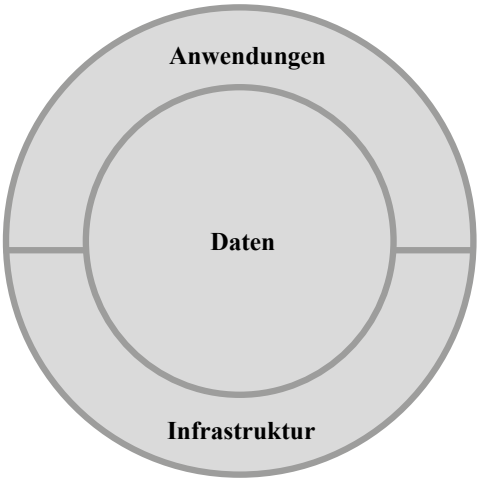

Abb. 6: Generisches IT-Modell

Das in der Abbildung dargestellte Modell verzichtet vollständig auf die Darstellung einzelner technischer Komponenten und kann beispielsweise auf einen einzelnen, eingebetteten Rechner bezogen werden. In diesem Fall wird die Infrastruktur durch die Hardware und das Betriebssystem gebildet, die alle zur Ausführung von Anwendungen notwendigen Ressourcen bereitstellen. Wahlweise kann das Modell auch die Grundlage für ein komplexes Szenario bilden, bei dem auf einer heterogenen Infrastruktur aus vernetzten Systemen verschiedene Anwendungen ausgeführt werden, die Daten verschiedener Formate miteinander austauschen.

5.2 REFERENZMODELL

Das Referenzmodell soll die komplexen Zusammenhänge öffentlicher IT visualisieren und den jeweiligen Bedürfnissen verschiedener Anwendungsbereiche angepasst werden können.

Eine konkrete Ausprägung des generischen IT-Modells ist das Referenzmodell öffentliche IT. Das Ziel des Referenzmodells ist, die komplexen Zusammenhänge öffentlicher IT und deren Anpassbarkeit an die jeweiligen Bedürfnisse verschiedener Anwendungsbereiche zu visualisieren. Dabei ist das Referenzmodell nicht als Schichtenmodell zu begreifen. Einzelne Teile des Modells können gelöscht, verändert oder ergänzt werden, um die Passgenauigkeit für ein bestimmtes Anwendungsgebiet zu erreichen. [Referenzmodell Öffentliche IT]

Eine Reihe technischer Bausteine deckt ein breites Spektrum an Querschnittsfunktionen ab, die je nach Anwendungsfall unterschiedlich ausgeprägt sind. Die Anwendungsfälle finden sich meist in einer spezifischen Anwendungsdomäne wie beispielsweise Bildung, Verkehr, Umwelt, Versorgung, Verwaltung oder Gesundheit. Diese Anwendungsdomänen sind nicht vollständig, repräsentieren aber ein breites Spektrum der öffentlichen IT. Jeder Baustein steht für Komponenten, die unterschiedliche Funktionen bereitstellen. Werden die technischen Komponenten miteinander kombiniert, entsteht ein informationstechnisches System. Beispielsweise besteht ein Computer als Gesamtsystem aus einer Anzahl von Teilkomponenten und kann bestimmte Aufgaben erfüllen, ohne dass der Endanwender Details zu internen Zusammenhängen und Abläufen wissen muss. Über Schnittstellen ist ein System mit der Umgebung verbunden, die andere Systeme beinhalten kann. Die Abstraktion und die Kombinierbarkeit sind mächtige Prinzipien, um leistungsfähige technische Systeme aus Teilsystemen aufzubauen.

Ein informationstechnisches System im beziehungsweise für den öffentlichen Raum wird jedoch nicht nur durch funktionale Komponenten geprägt, sondern muss auch bestimmte Anforderungen erfüllen:

- Qualitative Anforderungen konkretisieren die Eignung der Bausteine hinsichtlich bestimmter Ziele (beispielsweise Sicherheit, Benutzbarkeit und Kompatibilität) und werden in Anlehnung an ISO/IEC 25010 [ISO/IEC 25010] festgelegt.
- Gesellschaftliche Anforderungen dienen dazu, die Verantwortung der Akteure im öffentlichen Raum darzustellen und die Auswirkungen ihrer Entscheidungen und Aktivitäten auf die Gesellschaft und die Umwelt zu betrachten. Als Grundlage hierfür dient die Norm DIN ISO 26000 [DIN ISO 26000].

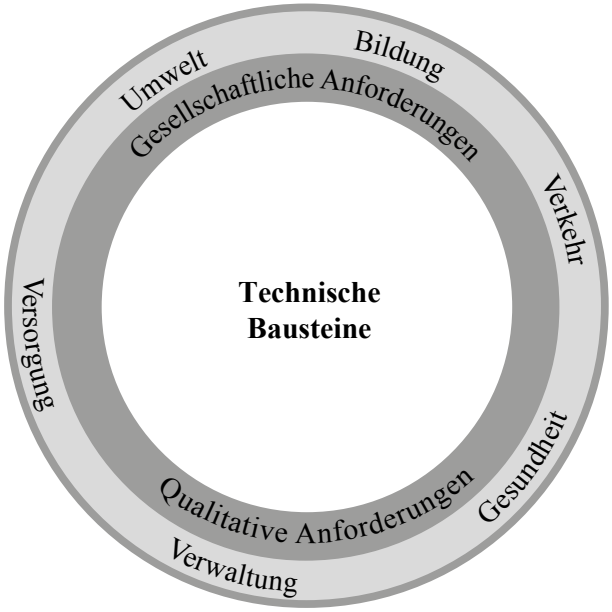

Abb. 7: Basis-Referenzmodell

5.2.1 Technische Bausteine

Die Komposition verschiedener Bausteine und deren Beziehung untereinander bildet ein informationstechnisches System für einen bestimmten Anwendungsfall. Die Komplexität der Bausteine reicht dabei von einfach bis sehr komplex. Häufig sind die Bausteine im realen System nicht klar voneinander abgrenzbar. Ebenfalls muss auch nicht jeder Baustein vorhanden sein. Ziel ist es jedoch, die wesentlichen Bausteine zu erkennen und zu beschreiben sowie ihre Ausprägungen anhand von Beispielen zu erläutern.

5.2.1.1 Identitäten

In der öffentlichen Diskussion werden digitale Identitäten oftmals gleichgesetzt mit Identitäten von Personen, die sich im Internet bewegen. [Vertrauenswürdige digitale Identität] Eine klassische Definition von digitaler Identität beschreibt diese als »jede mögliche Form von technisch abgebildeten Daten, die zu einer Person gehören«. [ULD 2007] Die Digitalisierung des öffentlichen Raumes geht aber noch einen Schritt weiter. So ist es möglich, vielfältige reale Objekte zu identifizieren, mit ihnen zu kommunizieren oder diese zu steuern. Damit benötigen auch diese Objekte eine digitale Identität. Mit neuen Technologien, die auf IPv6 [Fortschrittliche Netze, s. a. 7.5] beruhen, ist es theoretisch möglich, weltweit jedem Objekt eindeutige Internet-Adressen zuzuweisen.

Im Kontext öffentlicher IT spielen digitale Identitäten eine zentrale Rolle. Wann immer Personen, Organisationen, Objekte oder Dienste miteinander kommunizieren, werden Mechanismen für sichere und vertrauenswürdige Identitäten benötigt. Für Personen ist dabei der Grad der Anonymität häufig Gegenstand gesellschaftlicher Debatten. Er gibt an, mit welchem Aufwand es möglich ist, auf eine reale Identität schließen zu können. Eine der größten Herausforderungen des Identitätsmanagements aus der Perspektive der öffentlichen IT ist es daher, einerseits den Wunsch nach Personalisierung in virtuellen Räumen zu erfüllen, andererseits den Schutz von Identitäten jeglicher Art damit in Einklang zu bringen. Personalisierung erfordert immer möglichst viel Wissen über eine Identität. Datenschutz, Vertraulichkeit und Privatheit schränken aber die Verfügbarkeit hierfür erforderlicher Daten und Informationen ein. In elektronischen Kommunikationssystemen bedarf es daher funktionaler Äquivalente zu Praktiken und Gepflogenheiten, die das Identitätsmanagement im Alltagsleben strukturieren.

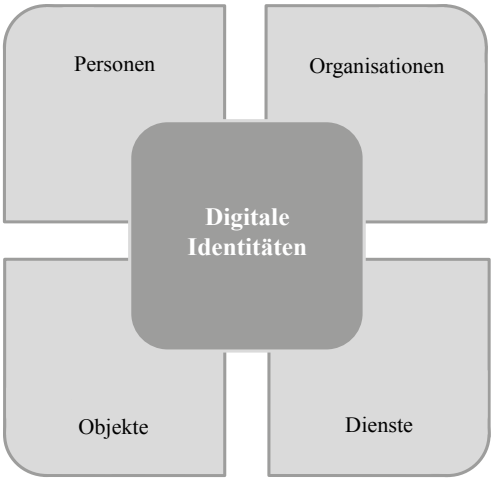

Abb. 9: Verschiedene Typen digitaler Identitäten

5.2.1.2 Information und Wissen

Daten werden immer wichtiger, was durch die Flut an Begriffen und Konzepten wie Open Data, Linked Data, Big Data, Smart Data, Datability oder Data Analytics verdeutlicht wird. Dabei waren Daten schon zu Beginn der informationstechnischen Revolution integraler Bestandteil der elektronischen Datenverarbeitung. Was ist passiert, dass sich das Thema Daten inzwischen einer so großen Aufmerksamkeit erfreut? Mit der Weiterentwicklung der Hardware und der Integration immer neuer Zwischenebenen begann die Emanzipation: Digitale Daten lösten sich immer mehr von ihren Trägersystemen und wurden zu selbstständigen Objekten. Die modernen Systeme und Virtualisierungstechniken erlauben eine immer weitergehende Abstrahierung von der eigentlichen Infrastruktur und ermöglichen die Verarbeitung sowohl in lokalen Systemen als auch in der Cloud. [White Paper Big Data]

Digitale Daten sind in erster Linie technische Kodierungen, die verarbeitet, gespeichert und übertragen werden können. Ein gemeinsames Verständnis davon, was diese Daten repräsentieren, sorgt dafür, dass sie als Informationen interpretiert werden können. Vereinfacht gesehen besteht eine digitale Information aus einer Trias von Syntax, Semantik und Pragmatik beziehungsweise Form, Inhalt und Wirkung. Syntax allein strukturiert nur die Daten, erst die Semantik weist ihnen Bedeutung zu und erlaubt so ihre Interpretation. Nutzen entsteht erst dann, wenn die Information eine Wirkung (Pragmatik) hat, also etwas Bestimmtes auslöst. Information bildet die Grundlage für Wissen, das heißt, Wissen erfordert eine Vielzahl von begründeten, geordneten Informationen, um gefestigt und erweitert werden zu können. [Arnold 2009]

5.2.1.3 Plattformen, Dienste und Anwendungen

Plattformen abstrahieren von Details und stellen eine einheitliche Basis für die Entwicklung und/oder Ausführung von Anwendungen und Diensten bereit.

Softwareanwendungen verschiedenster Art und in unterschiedlichen Bereichen stehen für die direkte Nutzung durch Bürger, die Wirtschaft oder die öffentliche Hand zur Verfügung oder werden als Webdienste für die Nutzung durch andere Anwendungen und Dienste angeboten. Waren die Softwareprogramme in der Anfangszeit der Computer eher monolithisch, so nutzen heutige Anwendungen und Dienste wiederum andere komplexe Programme, Anwendungen und Dienste, um gewünschte Funktionen auszuführen. Die Abstraktion komplizierter Details und die Bereitstellung einer einheitlichen Basis für die Entwicklung und/oder Ausführung von Anwendungen und Diensten werden häufig auch als Plattform bezeichnet. Plattformen können in vielen unterschiedlichen Ausprägungen angetroffen werden:

- Webportale beziehungsweise Webplattformen ermöglichen den Zugang zu allgemeinen Anwendungen und Diensten.
- Soziale Medien sind Plattformen für die Erstellung und den Austausch medialer Inhalte zwischen den Teilnehmern beziehungsweise Communities wie beispielsweise Google+, Facebook, YouTube oder Flickr.
- Domänen- und kontextspezifische Plattformen unterstützen Dienste und Angebote in bestimmten öffentlichen oder wirtschaftlichen Anwendungsbereichen wie beispielsweise E-Government, E-Health oder Vermittlungsangebote wie Airbnb oder Ebay.
- Elektronische Zahlungssysteme bieten einen einfachen Weg für das Bezahlen von Dienstleistungen im Internet.

Grundsätzlich kann man zwischen offenen, meist dezentralen Plattformen (Beispiele sind Internet und WWW) und geschlossenen, meist zentral gesteuerten Plattformen unterscheiden. »Es ist das Schicksal jeder erfolgreichen Plattform, dass sich irgendwann ein Iterationsschritt vollzieht und sich eine andere Plattform über ihr positioniert.« [Seemann 2014] Problematisch an vielen großen, zentral gesteuerten und international agierenden Plattformen ist, dass diese sich nur schwer auf nationaler Ebene regulieren lassen.

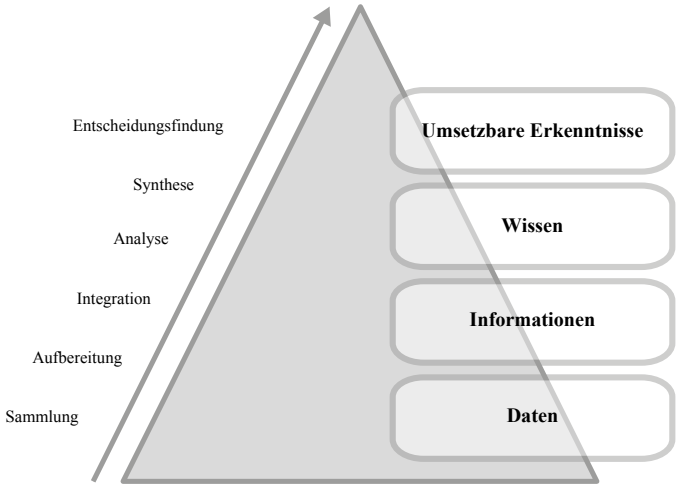

Abb. 10: Prozessschritte für Datenanalysen

5.2.1.4 Prozesse

Damit eine Organisation (auch der Staat beziehungsweise die Zivilgesellschaft) wirksam funktionieren kann, »muss sie zahlreiche miteinander verknüpfte Tätigkeiten bestimmen, leiten und lenken. Eine Tätigkeit oder eine Gruppe von Tätigkeiten, die Ressourcen verwendet und die ausgeführt wird, um die Umwandlung von Eingaben in Ergebnisse zu ermöglichen, kann als Prozess angesehen werden. Oft bildet das Ergebnis des einen Prozesses die direkte Eingabe für den nächsten.« [DIN ISO 9001]

Auch in der Informationstechnik wird dieser Ablauf als Prozess bezeichnet. Die Ablauflogik wird durch Regeln festgelegt. Jeder Prozess hat einen definierten Anfang und ein definiertes Ende. Ein Input (Eingabe, Auslöser), der materiell oder immateriell sein kann, wird durch die Bearbeitung zu einem Output (Ergebnis, Wert) transformiert. Ein Prozess kann in eine Kette von Teilprozessen zerlegt werden. In die Prozesse einbezogen werden zudem die Akteure. Um die korrekte Ausführung der Prozesse zu überwachen, müssen geeignete Methoden und gegebenenfalls geeignete Messungen stattfinden. Werden die geplanten Ergebnisse nicht erreicht, sollten Korrekturmaßnahmen erfolgen. Die Darstellung mit festen Regeln und einer vergleichsweise einfachen Datenverarbeitung von Eingabe zu Ausgabe bezieht sich auf herkömmliche Systeme. Bei der Anwendung von lernenden Algorithmen oder kognitiven Computersystemen werden interne Systemstrukturen komplexer (vgl. auch [Trendthema Denkende Maschinen]), die externe Prozesssicht kann dabei allerdings beibehalten werden. Inter- und intraorganisationale Prozesse werden zunehmend durch Informations- und Kommunikationstechnologien begleitet. Diese umfassen beispielsweise:

– Electronic Government: Abwicklung geschäftlicher Prozesse im Zusammenhang mit Regieren und Verwalten (Government) mit Hilfe von Informations- und Kommunikationstechnik über elektronische Medien. [von Lucke und Reinermann 2000]

– Automatisierung und Robotik: Automatisierte Prozesse zur Vermeidung von Produktionsfehlern, zur Steigerung der Produktivität beziehungsweise zur Optimierung von Abläufen. Neue Einsatzbereiche finden sich zum Beispiel im Katastrophenschutz (Reinigung verseuchter Bereiche) oder auch, mit Rasenmähern oder Drohnen, im öffentlichen Raum [Trendthema Drohne].

Grundlage für die Beschreibung und Ausführung der Prozesse sind offene und standardisierte Schnittstellen, mittels derer unterschiedliche Komponenten miteinander kommunizieren können. Für die Prozesssteuerung und -ausführung ist es notwendig, den Prozessen oder deren Teilprozessen Rollen und Ressourcen dynamisch zuzuordnen.

5.2.1.5 Dokumente

Elektronische Dokumente können verschiedene Medien enthalten, wie Text, Grafik, Audio oder Video, aber auch jede andere Form von unstrukturierten, semi-strukturierten oder vollstrukturierten Daten. Ein elektronisches Dokument ist durch Inhalt, Struktur und Layout charakterisiert, jedoch sind diese Merkmale elektronisch nicht immer eineindeutig. Inhalt kann unterschiedlich transportiert werden, Struktur hängt oftmals von der Anwendung ab und kann transformiert werden, und Layout ist meist nur in der Darstellung für Menschen erforderlich.

Aktivitäten rund um Dokumente umfassen das Generieren, Ablegen, Wiederfinden, Übermitteln, Speichern und Archivieren. Im Zusammenhang mit Prozessen dienen sie als Input und werden von diesen bearbeitet oder sie dienen als Output. Im öffentlichen Raum sind elektronische Dokumente in sehr unterschiedlicher Art vorhanden:

– Formulare findet man besonders in E-Government-Prozessen als Eingabedokumente, während die Ausgabedokumente Bescheide der Behörde sind.
– Elektronische Urkunden und Zeugnisse dürfen nicht veränderbar sein. Die Authentizität dieser Dokumente und deren Integritätsschutz werden durch elektronische Signaturen gewährleistet.
– E-Mails sind ebenfalls Dokumente, die von einem Empfänger interpretiert werden.
– Die E-Akte oder die elektronische Patientenakte sind Beispiele für verteilte Dokumente in einem Netzwerk. Kommunikation und Kooperation, Datenschutz, Integrität und Zugriffsberechtigungen sind nur einige Anforderungen beziehungsweise Merkmale dieser hochkomplexen Systeme.

Herausforderungen für die öffentliche IT entstehen durch die stetige Zunahme von elektronischen Dokumenten. Beispielsweise stellt sich die Frage, wie nach dem Ableben eines Menschen mit dessen elektronischen Dokumenten umgegangen werden soll [Trendthema Digitaler Nachlass]. Digitales Eigentum ist ein weiteres aktuelles Thema, insbesondere mit Blick auf die Unterscheidung zwischen Originaldokument und Kopie oder auch auf das Urheberrecht.

5.2.1.6 Ressourcen

Um Prozesse durchführen und überwachen zu können, werden Ressourcen benötigt. Ressourcen können beispielsweise Personal, Ausstattung, finanzielle Mittel, aber auch Lizenzen oder geistiges Eigentum sein. Ressourcen für die öffentliche IT umfassen Hardware und Software unterschiedlicher Art wie beispielsweise Netze und Endgeräte, Sensoren oder cyber-physische Systeme.

5.2.1.7 Kommunikation

Kommunikation im Sinne öffentlicher IT bezeichnet ganz allgemein den Austausch von Informationen, unabhängig vom genutzten Übertragungsweg. Öffentliche Räume konstituieren sich unter anderem durch gesellschaftlich relevante Kommunikation. Das Internet ist hierfür das derzeit wohl bedeutendste Beispiel. Ohne elektronische Kommunikation über Kommunikationsnetze würde es öffentliche IT kaum geben.

Einige Beispiele für Kommunikation im öffentlichen Raum sind:

- Online-Kommunikation in sozialen Netzwerken: Sie dient nicht nur dem persönlichen Austausch, sondern kann auch öffentliche Funktionen erfüllen, wie beispielsweise Hilfe und Koordination in Notsituationen wie Hochwasser.
- E-Mail oder Instant Messaging: Mit E-Mail oder Instant-Messaging kann spontan eine Nachricht an einen Kommunikationspartner oder eine Gruppe versandt werden, wobei es zwischen verschiedenen Anwendungen und Methoden große Unterschiede in Bezug auf die Vertraulichkeit der Kommunikation sowie die Sicherstellung von Authentizität und Integrität gibt.
- Neue Kommunikationsfunktionen: Kommunikationsfunktionen werden in immer mehr Klassen von – bisher nicht vernetzten – technischen Systemen eingebaut (zum Beispiel in Fahrzeugen) und sind ein Teil der Smartifizierung. (vgl. 2.5)

5.2.1.8 Netze

Netze zur Übertragung von Sprache, Daten, Dokumenten und Multimedia-Inhalten begleiten uns heute täglich im privaten wie im beruflichen Umfeld. In vielen Lebenslagen sind diese Kommunikationsnetze für den Nutzer unsichtbar. Oft sind wir uns der Technik im Hintergrund gar nicht bewusst, weil das genutzte Endgerät per Funkschnittstelle auf Netze zugreift oder wir uns an viele Anwendungen gewöhnt haben. [White Paper Fortschrittliche Netze]

Für öffentliche IT stehen der Netzzugang zum Internet beziehungsweise Mechanismen an der Schnittstelle zwischen dem Internet und den lokalen Netzen der Nutzer im Fokus.

Gleichzeitig steigt die Bedeutung der Netze. Immer mehr Vorgänge sind von reibungsloser Kommunikation abhängig. Für öffentliche IT stehen der Netzzugang zum Internet beziehungsweise Mechanismen an der Schnittstelle zwischen dem Internet und den lokalen Netzen der Nutzer im Fokus. Für Bürger ist ein

möglichst einfach zu konfigurierender und zu benutzender Zugang erforderlich. Über diesen Netzzugang werden auch Informationen oder Dienste der Wirtschaft und der öffentlichen Hand bereitgestellt. Dies geschieht aufgrund der Interessen von Akteuren oder weil die Organisationen dazu verpflichtet sind.

Attraktive Endgeräte treiben die Entwicklung an und führen zu Forderungen der Nutzer an die Netzbetreiber. Die tägliche Nutzung von praktischen, leicht bedienbaren Anwendungen führt zu steigenden Erwartungen an die Verfügbarkeit von Netzen und bezüglich der Bereitstellung von Diensten und Anwendungen.

5.2.2 Gesellschaftliche Anforderungen

Bei der Entscheidungsfindung und Ausgestaltung öffentlicher IT stehen die Interessen der Allgemeinheit – das Gemeinwohl – im Mittelpunkt. Die Auswirkungen der Digitalisierung auf die soziale und natürliche Umwelt sind dabei von Bedeutung. Insbesondere der Staat muss diese gesellschaftliche Verantwortung tragen und soziale und umweltbezogene Überlegungen in seine Entscheidungsfindung einbeziehen, sowie Rechenschaft über die Auswirkungen seiner Entscheidungen und Aktivitäten auf Gesellschaft und Umwelt ablegen. Dies muss auch technisch unterstützt werden, wozu in Anlehnung an [DIN ISO 26000] bestimmte Anforderungen erfüllt sein sollten:

- *Rechenschaftspflicht* ist die Fähigkeit einer Organisation, für ihre Entscheidungen und Aktivitäten Rede und Antwort zu stehen. Technisch muss dazu eine Nachvollziehbarkeit von Entscheidungen, Aktionen und deren Wirkungen unterstützt werden, um die jeweilige Verantwortlichkeit feststellen zu können. Dies kann sehr unterschiedliche Ausprägungen haben, wie etwa die Bestätigung von Quelle oder Ziel bei der Datenübermittlung, die Zurechenbarkeit von Aktivitäten zu Personen oder Rollen oder den Nachweis, dass Gesetze und Richtlinien hinsichtlich der Informationssicherheit oder des Datenschutzes eingehalten werden.
- *Transparenz* ist die Offenheit in Bezug auf Entscheidungen und Aktivitäten, die die Gesellschaft, die Wirtschaft oder die Umwelt beeinflussen, verbunden mit der Bereitschaft, diese zu kommunizieren. Vorgaben, Entscheidungen und Aktivitäten sowie voraussichtliche Auswirkungen auf die Gesellschaft und die Umwelt sollten dabei durchschaubar werden. Das bedeutet jedoch nicht, dass vertrauliche Informationen oder geheime Akten veröffentlicht werden müssen. Transparenz tritt in sehr unterschiedlichen Formen und Zusammenhängen auf. »Open«-Bewegungen wie Open Source, Open Data und Open Government öffnen vormals geschlossene Bereiche, um diese allen zugänglich zu machen und Partizipation zu ermöglichen, Statusmeldungen in E-Government-Prozessen erlauben die Kenntnis des Bearbeitungsstands und der für die Bearbeitung verantwortlichen Akteure.
- *Ethisches Verhalten* ist nach anerkannten Grundsätzen richtiges oder gutes Verhalten. Allgemein wird unter ethischem Verhalten Ehrlichkeit, Gerechtigkeit und Rechtschaffenheit verstanden. Informationstechnik kann ethisches Verhalten unterstützen (beispielsweise durch soziale Plattformen) oder aber sie muss so konzipiert und eingesetzt werden, dass ihre Anwendung keine unfairen Folgen hat. Beispiele dafür sind die Technikfolgenabschätzung zur Bewertung der Chancen und Risiken einer bestimmten Technik, die Einhaltung technischer Anforderungen und Regeln

für Datenschutz und IT-Sicherheit oder die Verhinderung digitaler Versehrungen wie die Nutzung gestohlener Identitäten, die Vortäuschung von Urheberschaft oder Cybermobbing. [Trendthema Digitale Unversehrtheit]

5.2.3 Qualitative Anforderungen

Die Hard- und Software muss nicht nur funktionale Anforderungen erfüllen, sondern auch qualitativ geeignet sein, die Digitalisierung des öffentlichen Raumes zu gestalten. Basierend auf den Qualitätseigenschaften zur Bewertung von Softwaresystemen und -produkten der ISO/IEC 25010 [ISO/IEC 25010] ergeben sich folgende Anforderungen:

- *Kompatibilität:* Neben der Funktionalität ist es für alle Komponenten des Referenzmodells öffentlicher IT wesentlich, dass sie mit anderen Komponenten zusammenarbeiten beziehungsweise kommunizieren können. Dies umfasst die Fähigkeit zur Koexistenz und Interoperabilität von Komponenten. Interoperabilität kann technisch durch die Einhaltung von Standards realisiert werden. In der Praxis sind jedoch häufig auch abgestimmte Konfigurationen erforderlich.
- *Benutzbarkeit:* Die Benutzbarkeit von Anwendungen, Diensten oder anderen IT-Komponenten durch die intendierten Nutzer für einen bestimmten Zweck entscheidet oft, ob diese auch akzeptiert werden. Gute Erlernbarkeit und Bedienbarkeit fördern gesellschaftliche Teilhabe und eröffnen zuvor Unbeteiligten den Zugang zur digitalen Welt. Schlechte Benutzbarkeit wird zum Risikofaktor, wenn beispielsweise medizinische Geräte nicht bedient werden können. [Trendthema Usability]
- *Sicherheit:* Die Sicherheit von Komponenten, Systemen und Informationen bildet die Grundlage für die Funktionsfähigkeit öffentlicher IT-Systeme. Bedrohungen erkannt, Risiken und Gefahren müssen minimiert und geeignete Sicherheitsmaßnahmen müssen zur Vermeidung von Schäden an Menschen, Dingen, Daten oder ideellen Werten müssen ergriffen werden.

6.

ÖFFENTLICHE IT – BEISPIELE AUS VERSCHIEDENEN PERSPEKTIVEN

Zur Veranschaulichung des Konzepts von öffentlicher IT werden im Folgenden verschiedene Beispiele erläutert, die für Staat, Wirtschaft und Zivilgesellschaft von besonderer Relevanz sind. Die Breite der Thematik bringt es mit sich, dass die Beispiele nur ausschnittartig einzelne Aspekte abdecken können. Sie beanspruchen somit keineswegs Vollständigkeit – weder in Bezug auf die Darstellung öffentlicher IT, noch in Bezug auf die dargestellten Themen –, sondern skizzieren vielmehr relevante Einzelaspekte. Die Auswahl der hier dargestellten Beispiele richtet sich danach, öffentliche IT möglichst breit zu repräsentieren sowie die Megatrends zu konkretisieren.

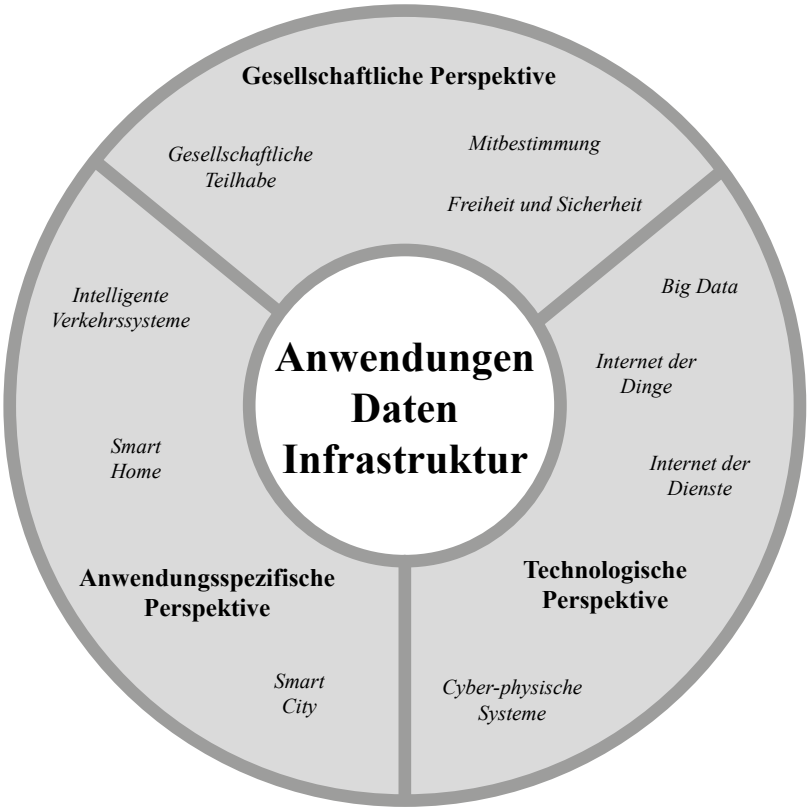

Abb. 11: Perspektiven der öffentlichen IT

Die hier vorgestellten Beispiele zeigen, dass basierend auf den Megatrends sehr ähnliche Ansätze und Ziele verfolgt werden. Dadurch sind diese nicht immer klar voneinander abzugrenzen und weisen teils gemeinsame Schnittmengen auf. An Konzepten wie »Smart Home« und »Smart City« wird außerdem deutlich, dass einige Beispiele eine domänen- beziehungsweise anwendungsspezifische Sicht repräsentieren, während andere, wie das »Internet der Dinge«, eine technische Perspektive darstellen oder gesellschaftspolitisch relevant sind, wie »Bürgerschaftliches Engagement«.

6.1 ANWENDUNGSSPEZIFISCHE SICHT

Öffentliche IT ist neuerdings in vielen Anwendungsbereichen unseres Lebens anzutreffen. Meist wird dies durch die Begriffe »smart«, »intelligent« oder »4.0« charakterisiert.

6.1.1 Smart Home

Im Heimanwenderbereich angesiedelt ist die Vision des Smart Home, die die Vernetzung und Smartifizierung von Dingen im eigenen Zuhause beinhaltet und sich an den Bedürfnissen der Bewohner ausrichtet. Im Mittelpunkt stehen dabei sowohl die Hausinfrastruktur wie Heizung, Wasser und Strom als auch Haushaltsgeräte und Elektronik, die über digitale Schnittstellen verfügen und gegebenenfalls auch über das Internet erreichbar sind. Zur Steuerung kommt beim Smart Home die Automatisierung hinzu. Anwendungen agieren sowohl in den Geräten als auch übergreifend teilautonom und können die Geräte je nach Situation eigenständig steuern. Als Entscheidungsgrundlage dienen unterschiedlichste Messdaten aus Sensoren oder Smart-Meter-Geräten.

Zunehmend sollen auch Assistenzsysteme das Leben im eigenen Umfeld erleichtern. [Trendthema Ambient World] Als Ambient Assisted Living (AAL) werden technologische Lösungen, Konzepte, Dienstleistungen und technische Infrastrukturen erfasst, die häusliche Umgebung mit Hilfsinstrumenten ausstatten. Viele solcher Systeme sollen dazu beitragen, älteren und beeinträchtigten Menschen ein selbstbestimmtes Leben zu ermöglichen. Die Überwachung des Gesundheitszustands und das automatisierte Auslösen eines Notrufs sind hier zu nennen. Andere Anwendungen, wie dem Bewohner folgende Musik und Beleuchtung oder die automatisierte Steuerung der Raumklimatisierung, zielen stärker auf generelle Komfortsteigerung.

Vernetzte und in Teilen autonome Geräteinstallationen aus Sensoren, Aktuatoren und Computern haben das Potenzial, Komfort und Sicherheit in der heimischen Lebenswelt zu steigern und Inklusion zu fördern. Technologische Lösungen für ein selbstbestimmtes Leben können aber auch als Bevormundung oder gar als Entmündigung aufgefasst werden, wenn die das alltägliche Leben bestimmenden Technologien nicht verstanden werden. Befürchtungen über die Intelligenz der Dinge im Haus äußert zum Beispiel Rauterberg: »Sie schlagen Alarm, sobald ein Dieb sich nähert. Sie rufen den Arzt, sollte ich stolpern und nicht mehr aufstehen können (…) Ich wohne, und es wohnt mich. Es regelt, schaltet, knipst mich an.« [Rauterberg 2014]

Vernetzte und in Teilen autonome Geräteinstallationen aus Sensoren, Aktuatoren und Computern können Komfort und Sicherheit in der heimischen Lebenswelt steigern und Inklusion fördern.

Vernetzung und Smartifizierung der Geräte im heimischen, privaten Umfeld bedeuten aus technischer Sicht, dass für ihre korrekte Funktionswese viele neue Schnittstellen zur Außenwelt geschaffen werden, die häusliche Daten übermitteln oder externe Steuerungsmöglichkeiten eröffnen. So öffnet sich schon rein technisch der vielleicht privateste aller Räume nach außen. Dadurch wird es leichter, diesen privaten Raum für gesellschaftliche Zielsetzungen nutzbar zu machen, und zwar für gesellschaftliche Teilhabe körperlich Beeinträchtigter ebenso wie für das Erreichen von Energieeffizienzzielen. Aus der Perspektive der öffentlichen IT stellen sich dadurch ganz grundle-

gende Fragen: Wie kann sichergestellt werden, dass die heimische Lebenswelt trotz stets vorhandener Sicherheitslücken geschützt wird? Wie kann einem Kontrollverlust über häusliche Regelungssysteme bis hin zu einer Totalüberwachung des privaten Lebensumfelds mit Hilfe von Technik oder Gesetzgebung entgegengewirkt werden? Welche personenbezogenen oder personenbeziehbaren Daten müssen wirklich geschützt werden? Ist Privatsphäre noch möglich?

6.1.2 Smart City

Die weltweite Urbanisierung ist eine zentrale Herausforderung des 21. Jahrhunderts. Seit 2007 wohnen erstmals mehr Menschen in Ballungsräumen als in ländlichen Regionen. [acatech 2011] Schlaue Städte, sogenannte Smart Cities, sind der Inbegriff des globalen Wandels unserer Lebensräume. Die moderne Stadt avanciert zum zentralen Knotenpunkt menschlichen Lebens und ist auf Informations- und Kommunikationstechnologien angewiesen. Intelligente Städte zielen darauf ab, knappe Ressourcen nachhaltig zu nutzen. [Fraunhofer FOKUS 2015]

Die schlaue Stadt avanciert zum zentralen Knotenpunkt menschlichen Lebens und ist auf Informations- und Kommunikationstechnologien angewiesen. Technik soll jedoch für die Bürger möglichst unsichtbar sein.

Smart Cities sind ein Konglomerat öffentlich verantworteter Informationstechnik aus Anwendungsbereichen wie Energie, Wohnen, Bildung, Kultur, Mobilität, Transport, Gesundheit, Verwaltung und öffentlicher Sicherheit. Damit sind nahezu alle Bereiche der Daseinsvorsorge umfasst, die durch Informationstechnik verknüpft werden. Smarte Objekte helfen bei Entscheidungen, tauschen Daten über Status und Kapazitäten untereinander aus, steuern die Informationsflüsse und bewerten komplexe Situationen. Trotzdem soll die Technik dabei für die Bürger möglichst unsichtbar bleiben, jedoch mit nutzerfreundlichen Bedienkonzepten ausgestattet sein, die sich in den Alltag einfügen und die Gewohnheiten der Menschen respektieren. Innovative Konzepte sind erforderlich, um diese verschiedenen Anwendungsbereiche zu gestalten. Beispiele hierfür sind die Fraunhofer Morgenstadt [Fraunhofer Morgenstadt] oder urbane Technologien in Berlin [Erbstößer 2013].

Dazu ist unter anderem der Auf- beziehungsweise Ausbau von Sensornetzen und Mobilkommunikation notwendig. Neben Schutz und Sicherheit ist insbesondere die Interoperabilität aller Anwendungsbereiche unerlässlich. Konzeption, Systemintegration, Steuerungs- und Umsetzungsprozesse, Standardisierung und geeignete Rahmenbedingungen sind bisher nur für Teilbereiche vorhanden. Verhindern Inkompatibilität der verschiedenen Plattformen und Insellösungen in den Anwendungsbereichen den technischen Fortschritt? Sind die bedarfsgerechte Auswertung von Informationen, die proaktive Steuerung und die dynamische Anpassung an Veränderungen in allen Lebensbereichen realisierbar, ohne dass damit die Kontrolle und Überwachung der Bürger einhergeht? Welche technischen Werkzeuge und Maßnahmen sind dafür erforderlich? Wie können die neuen Angriffsmöglichkeiten durch umfassende Vernetzung, Öffnung von Schnittstellen und Verwendung cyber-physischer Systeme entdeckt und verhindert werden?

6.1.3 Smart Energy

Die durch die Energiewende politisch priorisierten Veränderungen in der Energieversorgung erfordern neuartige Systeme zur effizienten Verwendung und zum dezentralen Gewinnen, Erzeugen, Verteilen und Speichern von Energie. Die Einführung sogenannter Smart-Meter-Systeme zur Messung und gegebenenfalls zur Übermittlung des Verbrauchs an den Energieversorger hat bereits begonnen. Bis zum Jahr 2020 sollen laut einer EU-Richtlinie [Europäische Union 13.07.2009] mindestens 80 % des EU-Marktes mit solchen Geräten ausgestattet werden, soweit dies wirtschaftlich vertretbar ist. [Öffentliche Informationstechnologie; Gesetzentwurf der Bundesregierung 2015]

Von der Stromproduktion bis zum verbrauchenden Gerät sollen langfristig alle relevanten Netzknoten in ein intelligentes Stromnetz, auch als Smart Grid bezeichnet, integriert werden. Smart Meter erfassen die dafür benötigten Messdaten über Verbrauch und Produktion. Die Werte werden über verschiedene Kommunikationsschnittstellen zur weiteren Verarbeitung bereitgestellt. Diese Systeme sind ein erster Schritt hin zu identitätsbasierten, elektronischen Messsystemen für Verbrauchsdaten im Haushalt wie Gas, Wasser, Elektrizität und Fernwärme. Diese smartifizierten Systeme bringen gleichsam Herausforderungen mit sich, wie eine sichere Infrastruktur, personalisierte Objekte, Schutz persönlicher Daten sowie Anwendungen, die die Dinge des häuslichen Umfelds verbinden.

Von der Stromproduktion bis zum verbrauchenden Gerät sollen langfristig alle relevanten Netzknoten in ein intelligentes Stromnetz, auch als Smart Grid bezeichnet, integriert werden.

Die Technische Richtlinie des BSI TR-03109 für Smart-Metering [BSI TR-03109] beschreibt die Anforderungen an die Funktionalität, Interoperabilität und Sicherheit, die die Einzelkomponenten in einem Smart-Metering-System erfüllen müssen, sowie die Anforderungen zur Prüfung dieser Eigenschaften. Aus Sicht der öffentlichen IT ist die Steuerung von Lastspitzen oder Geringverbrauch ein positiver Effekt, der dazu beiträgt, in diesem wichtigen Feld der Daseinsvorsorge das Gemeinwohl zu fördern. Zugleich stellen sich aus dieser Perspektive jedoch Fragen hinsichtlich der Sicherheit, beispielsweise angesichts von Cyberangriffen auf mögliche Schwachstellen in intelligenten Stromzählern. Können intelligente Stromzähler auch als Einstiegspunkt für weitere Angriffe auf intelligente Smart-Home-Systeme dienen? Wie kann verhindert werden, dass Lebensgewohnheiten durch Datensammeln ausgeforscht werden?

6.1.4 Intelligente Verkehrssysteme

Sicher, umweltverträglich und effizient sollen die Verkehrs- und Transportsysteme in Zukunft funktionieren, um den Herausforderungen an Mobilität gerecht zu werden. [Öffentliche Informationstechnologie] In der EU-Richtlinie 2010/40/EU sind intelligente Verkehrssysteme als Systeme definiert, »bei denen Informations- und Kommunikationstechnologien im Straßenverkehr, einschließlich seiner Infrastrukturen, Fahrzeuge und Nutzer, sowie beim Verkehrs- und Mobilitätsmanagement und für Schnittstellen zu anderen Verkehrsträgern eingesetzt werden«. [Europäische Union 07.07.2010]

Für den motorisierten Individualverkehr lässt sich hier eine zum Smart Home analoge Entwicklung der Öffnung zuvor geschlossener Systeme beobachten. Mag die fahrzeuginterne IT noch als weitgehend abgeschlossen angesehen werden, so sind Fragen der öffentlichen IT spätestens dann berührt, wenn das Fahrzeug mit externen Systemen wie anderen Fahrzeugen (Car2Car), Ampelanlagen oder Leitsystemen (Car2X) kommuniziert.

Dies schafft neue Möglichkeiten – und wirft eine Reihe von alten und neuen Sicherheitsfragen auf: Werden unsere Autos zu rollenden Botnetzen? Bei der Fahrzeugkommunikation zur Erhöhung der Verkehrssicherheit werden zwischen Fahrzeugen sowohl regelmäßige als auch ereignisbezogene Nachrichten ausgetauscht. Regelmäßig wird die aktuelle Position, Richtung und Geschwindigkeit je nach Situation etwa ein- bis zehnmal pro Sekunde ausgesandt. Ereignisbezogene Nachrichten dienen beispielsweise der Warnung vor Gefahrensituationen wie Glätte, Stauenden, Falschfahrern oder plötzlichem Bremsen. Für die Kommunikation zwischen Fahrzeugen und der Verkehrsinfrastruktur kommen weitere Nachrichten hinzu, welche zum Beispiel Ampelphasen oder eine Kreuzungsgeometrie übermitteln. Dies erlaubt die Anpassung von Route und Fahrweise. Beispiele dafür sind eine individualisierte Routenführung oder Geschwindigkeitsempfehlungen, um eine grüne Welle zu nutzen. Zugleich können die übermittelten Daten genutzt werden, um die Verkehrslage hochaktuell und präzise zu erfassen. [Trendthema Sichere Fahrzeugkommunikation] Die entscheidende Frage dabei wird sein, wie Vertrauen zwischen den diversen digitalen Teilnehmern der kritischen Infrastruktur Verkehr hergestellt werden kann. Denn die umfassende Vernetzung von Fahrzeugen mit der Verkehrsinfrastruktur, den Fahrzeugherstellern, Anwendungen von Drittanbietern, dem Internet und Notfallsystemen eröffnet auch ein großes Angriffspotenzial. Sicherheitslücken können ohne Kenntnis der Fahrer entdeckt und ausgenutzt werden. Angriffe richten sich dabei gegen die Anwendungen der Fahrzeugkommunikation oder gegen ihre Nutzer und deren Privatsphäre.

Die Kommunikation des Fahrzeugs mit anderen Fahrzeugen, mit Ampelanlagen oder Leitsystemen sind Fragen der öffentlichen IT.

Zukünftig sollen die Verkehrsinfrastrukturen auch das vollautonome Fahren ermöglichen. [Trendthema Autonomes Fahren] Hier stellen sich grundsätzliche Fragen hinsichtlich der Ziele von Algorithmen: Wie soll sich ein Fahrzeug verhalten, wenn ein Unfall nicht mehr vermeidbar ist? Soll es vorrangig die Insassen schützen oder eher andere Beteiligte? Wie viel Spielraum erhält das System in der Interpretation der Verkehrsregeln? Wem soll Zugriff auf welche Daten ermöglicht werden? Muss sich ein Fahrer durch die Freigabe von Fahrzeugdaten selbst belasten?

6.1.5 Verwaltung x.0

Mit der politisch getriebenen Vision von der Industrie 4.0 scheint die Versionsnummer 4.0 Garant für öffentlich zugesprochene Modernität zu sein. Doch wie manifestiert sich 4.0 in der öffentlichen Verwaltung? [Trendthema Verwaltung x.0] Der Begriff Verwaltung 4.0 findet bereits bei der konsequenten Umsetzung von E-Government-Lösungen Anwendung. Ein darüber hinausgehendes Verständnis greift die Veränderungspotenziale durch intelligent vernetzte Objekte und Dienste im Internet der Dinge

beziehungsweise im Internet der Dienste für den öffentlichen Sektor auf. Daraus ergeben sich Gestaltungsmöglichkeiten für diesen Bereich der öffentlichen IT (vgl. 4.3.2).

Eine einfache Übertragung der Konzepte von der Industrie auf die Verwaltung verbietet sich. Bei der Industrie 4.0 steht die dingliche Güterproduktion im Zentrum, bei der das Internet der Dinge zunehmende Bedeutung erlangt. Die öffentliche Kernverwaltung arbeitet demgegenüber in erster Linie mit Daten und Informationen. Die spezifischen Anforderungen aus der Digitalisierung sind folglich andere. Der medienbruchfreie Datenaustausch zwischen allen in vernetzten Prozessen Beteiligten ist hier eine zentrale Herausforderung. Nicht die digitale Nachverfolgung eines gedruckten Bescheides, sondern digitale Bescheide eröffnen Potenziale. Im Gegensatz zur industriellen stützt sich die öffentliche Leistungserstellung vorrangig auf das Internet der Dienste. Hierin lassen sich etwa Dienste zur Arbeitsunterstützung nutzen, die eine teilautomatisierte Vorprüfung erlauben und dabei die Kosten für einzelne Verwaltungsleistungen deutlich senken.

Jenseits der Kernverwaltungen finden sich auch für das Internet der Dinge Anwendungsfelder im öffentlichen Sektor. So werden im Rahmen der Arbeiten zu Smart Cities Szenarien zu Energie, Gesundheit und Verkehr untersucht. Auch für Feuerwehr, Zivil- und Katastrophenschutz, bei denen technische Hilfsmittel traditionell von großer Bedeutung sind, bieten intelligent vernetzte Objekte beträchtliche Potenziale. Ein in diesem Themenfeld oft zitiertes Beispiel ist die Einrichtung eines Tsunamifrühwarnsystems, das die von bereits existierenden Bojen erfassten Wellenbewegungen entsprechend auswertet. Intelligente Vernetzung, Datenanalyse und Informationsverbreitung erlauben die Einrichtung eines solchen Systems mit überschaubarem Aufwand. Eine zeitnahe Reaktion auf Bedrohungssituationen wird damit realistisch – möglicherweise aber auch eine Massenpanik aufgrund einer Fehldiagnose.

In der Zusammenschau bergen die Konzepte der Verwaltung 4.0 somit ein beträchtliches Potenzial für ein Modernisierungsprogramm des öffentlichen Sektors. Es zeichnen sich zahlreiche Anwendungsfelder ab wie beispielsweise medienbruchfreie Prozesse durch webbasierte Dienste, proaktives Verwaltungshandeln, etwa Erinnerung an abgelaufene oder gar automatisierte Zustellung neuer Ausweisdokumente, automatisierte Beeinträchtigungsmeldungen bei Schäden von Straßen und anderen Infrastrukturen, umfassende Lageberichte von Großveranstaltungen oder bei Rettungseinsätzen, Datenfundierung durch Verbindung von bestehenden und neuen Datenquellen sowie Entscheidungsunterstützung und (Teil-)Automatisierung von Prozessen.

Anwendungsfelder für die Verwaltung 4.0 sind etwa die automatisierte Zustellung neuer Ausweisdokumente oder selbsttätige Meldungen bei Schäden von Straßen und anderen Infrastrukturen.

Die sich vage abzeichnenden Entwicklungen werfen grundsätzliche Fragen nach Datenschutz, gesellschaftlicher Akzeptanz und politischer Legitimität, der faktischen Macht von Algorithmen und IT-Sicherheit auf. Kann die De-Anonymisierung auch bei der Verknüpfung von Datenbeständen nachweislich verhindert werden? Welche politische und möglicherweise rechtliche Verantwortung für Entscheidungsabläufe und ihre Folgen entsteht durch zunehmend intelligent agierende Systeme? Wird politische Verantwortung gegebenenfalls durch algorithmische Legitimation verdrängt? Je gravierender die Entscheidungsfolgen sind, desto kritischer werden Fragen der IT-Sicherheit.

Sicherheitslücken, aber auch schwer absehbare Folgen aus der Verfügbarkeit neuer Funktionen in Anwendungsfeldern wie der Sozialverwaltung oder der inneren Sicherheit bieten Anknüpfungspunkte für Ängste und Dystopien hinsichtlich Kontrollverlusts und Totalüberwachung.

6.2 TECHNOLOGISCHE SICHT

Technischer Fortschritt bildet die Grundlage für neue Anwendungen. Intelligente Objekte, große Datenmengen und unbegrenzte Ressourcen charakterisieren aktuelle Entwicklungen. Allerdings wachsen damit auch die Angriffsmöglichkeiten.

6.2.1 Internet der Dinge

Im Internet der Dinge werden viele unterschiedliche Objekte durch Sensoren, Aktuatoren und Vernetzung an IT-Systeme gekoppelt.

Das Internet ermöglicht neuartige Kommunikationsformen zwischen Menschen – Gleiches wiederholt sich nun mit Gegenständen. [Trendthema Internet der Dinge] Im Zusammenhang mit Beobachtbarkeit, Datenproduktion, Steuerungsmöglichkeiten und Selbstorganisation eröffnen sich neue Kommunikationsmöglichkeiten, die hinsichtlich technischer Anforderungen und gesellschaftlicher Wirkungen die informationstechnische Revolution durch das Internet noch übertreffen können. Der weit gefasste Begriff »Internet der Dinge«, »Internet of Things« im Englischen, beschreibt dieses Phänomen.

Objekte werden durch Sensoren, Aktuatoren und Vernetzung an IT-Systeme gekoppelt. Ziel ist dabei der direkte Zugriff auf das physische System selbst oder der indirekte Zugriff auf eine digitale Repräsentation des Systems. Einsatzmöglichkeiten finden sich in allen Bereichen wie etwa Industrie, Verkehr und Umwelt. An der Schnittstelle zwischen der realen Welt und der IT kommen verschiedene Konzepte zum Einsatz. Funktionsumfang und eingesetzte Technologie können hierbei unterschiedlich sein. Produkte werden mit vergleichsweise preiswerten RFID-Chips ausgestattet, die eine automatische Erfassung einzelner Daten an bestimmten Punkten der Produktions- und Logistikkette ermöglichen. Wird eine über die Erfassung hinausgehende Kommunikation mit einem Objekt notwendig, so kann auch ein einfacher Netzanschluss integriert werden. Die sich aus der automatisierten Verfolgung von Produkten ergebenden Möglichkeiten haben zu einem anfänglichen Fokus auf Optimierungsfragen in der Logistik geführt. Das Nachvollziehen von Wertschöpfungs- und Lieferketten kann darüber hinaus beispielsweise auch wesentlich zur Kontrolle der Einhaltung von Öko- und Sozialstandards beitragen. Komplexere Sensoren, die etwa zur Steuerung im Rahmen der Heimautomatisierung dienen (Stichwort: Kühlschrank im Internet), verfügen über einen permanenten Netzzugang. Neben der reinen Erfassung von Objekten werden in den verschiedenen Anwendungsbereichen Steuerungsketten und automatisierte Interaktionen zwischen Systemen ermöglicht.

Durch neue, automatisierte Interaktionsformen zwischen realer Welt und IT-Systemen vergrößern sich allerdings auch die Angriffsfläche und die Angriffstiefe von Infrastrukturen. Fragen zu Sicherheit und Privatsphäre, Überwachung und Kontrolle,

Datenhoheit und -lebensdauer prägen die Relevanz öffentlicher IT. Zudem stellen sich analog zur Gewährleistung des Internetzugangs (vgl. 4.1.3) Fragen nach möglicher Unterversorgung mit der notwendigen Technik. Bereitstellung und Betrieb der technischen Basis für die Digitalisierung privater und insbesondere öffentlicher Räume könnten durch das Trittbrettfahrerproblem bei der Erstellung öffentlicher Güter beeinträchtigt werden.

6.2.2 Big Data

Neue technische Lösungen zur verteilten Verarbeitung immer größerer Datenmengen wecken neue Hoffnungen. Seit 2011 versucht die Industrie, diese neuen Möglichkeiten unter dem Sammelbegriff Big Data zu beschreiben. [Gartner 2011]

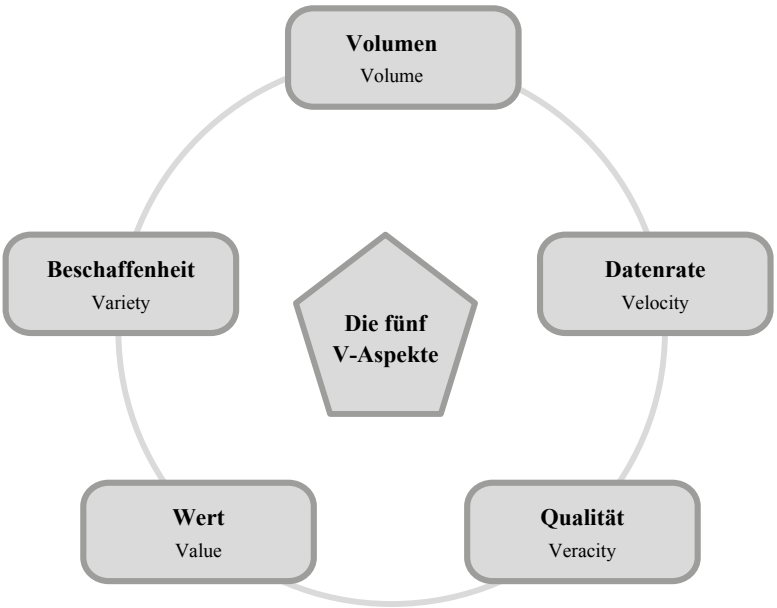

Abb. 12: Eigenschaften von Big Data (fünf V-Aspekte)

Big Data bezeichnet Methoden und Technologien für die hochskalierbare Erfassung, Aufbereitung, Speicherung und Analyse strukturierter und unstrukturierter Daten. [White Paper Big Data] Diese können helfen, die Planung, Steuerung und Optimierung von Prozessen in Wirtschaft, Verwaltung und Zivilgesellschaft zu verbessern. Aus Bereichen wie Wirtschaftsförderung, Energiewende, Sozialhilfe, Bildung, Verkehr oder öffentlicher Sicherheit liegen Ergebnisse für den erfolgreichen Einsatz von Big Data vor. [Bitkom 2012a] Beispielsweise versteht man unter Predictive Policing – in der einschlägigen Literatur mit »vorhersagende Polizeiarbeit« übersetzt – die auf Big Data basierende Datenanalyse zur Wahrscheinlichkeitsschätzung zukünftiger

Straftaten, um eine möglichst konkrete Unterstützung für die polizeiliche Einsatzplanung zu erhalten. Ausgewertet werden detaillierte Lagebilder, aktuelle Ereignisse, allgemein zugängliche Daten und auch Sensordaten. [Trendthema Vorhersagende Polizeiarbeit] Die Analysen basieren auf kriminologischen Theorien, die zur Erklärung bestimmter Muster herangezogen werden. Kern einer Vielzahl solcher kriminologischen Theorien ist die Annahme, dass aus vorliegenden Straftaten auf die Wahrscheinlichkeit zukünftiger Verbrechen geschlossen werden kann.

Big Data bezeichnet Methoden und Technologien für die hochskalierbare Erfassung, Aufbereitung, Speicherung und Analyse strukturierter und unstrukturierter Daten.

Der Einsatz von Big-Data-Technologien ist jedoch auch mit einer Vielzahl von Risiken verbunden, die sich aus missbräuchlicher Nutzung, fehlenden rechtlichen Rahmenbedingungen und unzulässigen Schlussfolgerungen aus dem generierten Wissen ergeben. Das Zusammenführen personenbezogener und personenbeziehbarer Daten aus verschiedenen Quellen und deren Auswertung widerspricht häufig den Prinzipien der Zweckbindung und Datensparsamkeit. Der Bürger muss als Individuum durch Anonymisierung und Pseudonymisierung seiner Daten davor geschützt werden, zum gläsernen Menschen zu werden. Auch seine Identität, Privatsphäre und Reputation müssen gegen Manipulation durch Dritte geschützt werden. Dieses Aufgabenfeld zählt zu den Kernelementen des staatlichen Gestaltungsanspruchs an die Digitalisierung.

Aus Online-Shops sind uns die Auswirkungen der Auswertungen von Verhaltensmustern in Form personalisierter Werbung gut bekannt. Die von den Betreibern zu eigenen Zwecken genutzten und im Extremfall ohne Kenntnis der Betroffenen veröffentlichten Personenprofile können Risiken und Gefahren verursachen. Daher muss sichergestellt werden, dass der Einsatz von Big Data nicht nur unter technischen Gesichtspunkten diskutiert wird, sondern auch unter Einbeziehung rechtlicher und ethischer Aspekte. [Davis und Patterson 2012] Öffentliche IT muss sich neben den technischen Entwicklungen auch mit folgenden Fragen beschäftigen: Welche Rechte bezüglich ihrer Identität und ihrer Daten besitzen Bürger im Zeitalter von Big Data? Wie können sie ihre digitale Identität und Reputation im Netz schützen? Wer darf welche Daten über Dritte ins Netz stellen, die dann allgemein für Big-Data-Analysen und speziell zur Definition des digitalen Ichs Verwendung finden? Wie kann Datenschutz gewährleistet werden, ohne die Potenziale von Big Data zu stark einzuschränken?

6.2.3 Cloud-Computing

Mit Cloud-Computing wird das aktuelle IT-Paradigma bezeichnet, IT-Leistungen nicht mehr vor Ort auf der Hardware des Nutzers zu erbringen, sondern über das Netz (Inter- oder Intranet) anzubieten. Immer mehr Daten und Anwendungen wandern vom eigenen Endgerät und von betrieblichen Rechenzentren »in die Wolke«. [Trendthema Cloud-Computing]

Cloud-Computing ist – wie jede andere Technologie – aus vorhergehenden Entwicklungen erwachsen. Auf technischer Ebene besteht sein innovativer Charakter zunächst in der umfassenden Automatisierung der Diensterbringung: Die Bereitstel-

lung, der Betrieb und das Management komplexer Anwendungen können ohne das Zutun menschlicher Administratoren für eine hohe Anzahl von Kunden erfolgen. Die Cloud wird damit – wie das Internet im Bereich Datenübertragung – zum umfassenden Instrument der Datenspeicherung und -verarbeitung. [Expertise Cloud-Fahrplan]

Der Zugang zu einer Cloud erfolgt netzwerkbasiert über das Internet oder aber über ein dediziertes Netzwerk, sodass Dienste der Cloud auf verschiedenen Endgeräten verwendet werden können. Die Nutzer sind in der Lage, selbstständig Dienste und Ressourcen anzufordern. Diese werden »elastisch« zur Verfügung gestellt, das heißt, ein Benutzer erhält innerhalb kurzer Zeit adäquate Ressourcen entsprechend seinem augenblicklichen Bedarf. Für den Nutzer stehen dadurch meistens scheinbar unbeschränkte Ressourcen zur Verfügung. Die Ressourcen des Anbieters sind in Pools konsolidiert, was eine parallele Diensterbringung für mehrere Mandanten (Kunden) erlaubt. Dabei werden die Ressourcen der einzelnen Mandanten einschließlich der Daten und Prozesse auf sichere Weise voneinander getrennt.

Die Cloud bestimmt längst das digitale Leben von Bürgern und Unternehmen und schafft dabei digitale öffentliche Räume: Soziale Netzwerke werden auf der Basis von Cloud-Infrastrukturen realisiert – Facebook ist ohne Cloud nicht denkbar. Als Cloud-Klienten genutzte mobile Endgeräte werden als Erweiterung des Büros und Online-Speicher als zuverlässige Alternative zur externen Festplatte oder zum USB-Stick angesehen. Viele Unternehmen – auch aus dem KMU-Segment – nutzen Cloud-Angebote, um Investitionen und operative Kosten für ihre IT zu reduzieren. [KPMG und Bitkom 2013]

Immer mehr Daten und Anwendungen wandern »in die Wolke«. Für den Nutzer stehen dadurch meistens scheinbar unbeschränkte Ressourcen zur Verfügung.

Angesichts fast täglicher Meldungen über Sicherheitslecks bei großen IT-Diensteanbietern stellt sich jedoch die Frage: Wie sicher ist die Cloud eigentlich? Diese Frage ist nicht pauschal zu beantworten: Ein Angriff auf einen großen Dienstleister mag nur deshalb durchgeführt worden sein, weil dieser Anbieter ein großes Ziel darstellt. Und wie wurde der Angriff überhaupt durchgeführt? Wurden wirklich kritische Komponenten einer Cloud direkt angegriffen oder beruht der Angriff auf Social Engineering (zum Beispiel Ergaunern von Passwörtern durch Telefonanruf), das mit der unterliegenden Technik nichts zu tun hat? Sicherheit ist immer das Ergebnis einer Vielzahl technischer Mechanismen und organisatorischer Maßnahmen. Moderne Cloud-Infrastrukturen implementieren solche Mechanismen; ihre Herstellerfirmen verstehen es als Marktvorteil, für zeitgerechte Sicherheitsupdates zu sorgen. Integrierte Monitoring- und Analysefunktionen vereinfachen das Aufspüren von Angriffen. Schließlich ist der Betreiber einer Cloud eher in der Lage, ein dediziertes Expertenteam für Sicherheitsfragen zu finanzieren als eine kleine IT-Abteilung, in der jeder Mitarbeiter multiple Aufgaben hat.

Neben der IT-Sicherheit wird der Datenschutz ebenfalls oft hinterfragt, da es kaum nachvollziehbar ist, wo sich die eigenen Daten befinden. Welche Datenschutzgesetze kommen zur Anwendung? Werden alle Daten gelöscht, wenn der Anbieter gewechselt wird? Kann man dem Cloud-Diensteanbieter wirklich vertrauen?

Gerade große Cloud-Infrastrukturen erlangen durch ihre umfangreichen Speicherungs- und Verarbeitungsfunktionen auch eine strategische Relevanz für das öffentliche Leben, nicht zuletzt deshalb, weil Abhängigkeiten entstehen, wenn immer mehr

Dienstleistungen aller Art aus der Cloud in Anspruch genommen werden. Eigene Infrastrukturen, Dienste und eigenes Personal werden nicht mehr vorgehalten. Potenzielle umfangreiche Cloud-Ausfälle werfen Fragen der Notfallversorgung nicht nur für Betriebe, sondern langfristig auch für die Funktionsfähigkeit der Gesellschaft auf.

6.2.4 Safety und Security

Sicherheit bezeichnet einen von Risiken und Gefahren freien Zustand von Menschen, Objekten oder Systemen. Um eine angemessene Sicherheit zu erreichen, ist es erforderlich, ein vorhandenes Risiko zu vermeiden, zu reduzieren, auf Dritte zu übertragen oder auch zu akzeptieren (siehe [BSI IT-Grundschutz 4.5 Risikostrategien wählen]). Aufgrund der heutigen technologischen Dynamik ist Sicherheit jedoch kein fixer Zustand, sondern erfordert eine kontinuierliche Überprüfung und Anpassung. Relevante Informationen müssen ständig aktualisiert, analysiert und adäquate Maßnahmen eingeleitet werden.

Die englische Sprache bietet mit den Begriffen Safety und Security eine Differenzierung der komplexen Thematik Sicherheit. [White Paper Safety und Security] Ihren Ursprung hatte die Betrachtung der funktionalen Sicherheit (engl. Safety) bereits zu Zeiten rein mechanischer Systeme, die in geschlossenen Umgebungen (zum Beispiel industriellen Steuerungssystemen) beziehungsweise als geschlossene Einheiten (zum Beispiel Fahrzeuge) ohne Verbindung nach außen operierten. Durch die zunehmende Vernetzung jeglicher Systeme mit Informationstechnik wird diese Isolierung von der Außenwelt jedoch immer mehr aufgeweicht. Heute ist das Hauptziel von Safety der Schutz der Umgebung vor dem Fehlverhalten des Systems. Im Fokus steht die Unversehrtheit von Mensch und Umwelt. Sichere Systeme müssen sich konform zu ihrer – korrekten – Spezifikation verhalten und eine hohe Zuverlässigkeit und Fehlersicherheit gewährleisten.

Safety – Das System soll die Umgebung nicht schädigen.

Security – Die Umgebung soll das System nicht schädigen.

In der Informationstechnik stehen die technische Verarbeitung, Lagerung und Übertragung von Daten im Vordergrund. Das Hauptziel von Security ist daher der Schutz der (IT-)Systeme und der gespeicherten Daten vor unerwünschten Einwirkungen aus der Umgebung. Ebenfalls relevant sind Aspekte der Kommunikationstechnik, vornehmlich der sichere Austausch von Daten.

Sicherheit ist von der Größe und Komplexität der IT-Systeme abhängig. Mit der Anzahl der Komponenten eines Systems steigt die Wahrscheinlichkeit von Fehlern und Schwachstellen. Wie sich diese auswirken, hängt dabei stark vom konkreten System und seiner Einsatzumgebung ab. Gerade in einem sehr komplexen System kann es Zustände geben, die sich nur schwer vorhersagen und überprüfen lassen, und an die daher vorher niemand gedacht hat. Derartige Zustände können im Ausnahmefall und auch bei einer vorangegangenen Risikobetrachtung zu einem Versagen des Systems und seiner Schutzmechanismen oder zu unangemessenen Gegenmaßnahmen führen.

Mit der fortschreitenden Digitalisierung und Vernetzung unserer Gesellschaft ist die Trennung von Safety- und Security-Aspekten bereits heute nicht mehr zeitgemäß.

Das Beispiel Verkehr verdeutlicht, wie beide Aspekte zusammenhängen: Moderne Fahrzeuge integrieren dutzende elektronische Steuereinheiten für Unterhaltungselektronik, Assistenzsysteme, schlüssellose Einstiegssysteme oder Anti-Diebstahleinheiten, die uns schützen, aber fahrzeugintern sowie nach außen auch unzählige neue Schnittstellen aufweisen (vgl. 6.1.4). Welche Gefahren diese zunehmende Komplexität und deutlich vergrößerte Angriffsfläche mit sich bringen, zeigen die beiden folgenden Fälle: Eine Sicherheitslücke in einem verbauten Mobilfunkmodul zur Vernetzung von Fahrzeugen mit dem Automobilhersteller hätten Angreifer ausnutzen können, um die Türen der betroffenen Fahrzeuge zu öffnen. [o. A. 2015] Und bereits im Juli 2014 war es Studierenden im Rahmen eines Sicherheitswettbewerbs gelungen, die Sicherheitsmechanismen eines Elektroautos zu überwinden. Der Angriff erlaubte es ihnen, bei voller Fahrt per Funk die Türen und das Sonnendach zu öffnen sowie die Hupe und das Licht zu betätigen. Als Angriffspunkt diente das schlüssellose Einstiegssystem in Verbindung mit der mobilen App des Herstellers. [o. A. 2014]

Die wachsende Vernetzung und Entgrenzung von Systemen mit immer mehr Angriffsvektoren kann daher dazu führen, dass bereits kleine Störungen in Teilsystemen ein unvorhersehbares Verhalten und letztlich gravierende Probleme für das Gesamtsystem bewirken. Wie also kann Sicherheit in Zukunft gewährleistet werden? Perimeter-Sicherheit, das heißt, der Schutz durch Abgrenzung wie zum Beispiel durch Firewalls, funktioniert in vielen Systemen und Anwendungen nicht mehr. Ein Lösungsansatz für diese zunehmend bedeutsame Herausforderung für unsere Gesellschaft ist die Verbesserung der Fähigkeit von Systemen, mit widrigen Ereignissen umgehen zu können (Resilienz). Bedingt durch die steigende Popularität des Forschungsthemas Resilienz existieren zahlreiche Begriffsdefinitionen. Diese lassen sich zusammenfassen als »die Fähigkeit, tatsächlich oder potenziell widrige Ereignisse abzuwehren, sich darauf vorzubereiten, sie einzukalkulieren, sie zu verkraften, sich davon zu erholen und sich ihnen immer erfolgreicher anzupassen« [acatech 2014]. Immer wieder muss die Frage gestellt werden, wie man sich auf Katastrophen vorbereiten kann. Wie können Gefahren verhindert werden? Welche Schutzsysteme sind sinnvoll? Wie kann die essenzielle Funktionsfähigkeit von Infrastrukturen, Systemen und Anwendungen gewährleistet werden? Wie kann ein System selbstständig aus Ereignissen lernen, um zukünftig besser gegen Bedrohungen gerüstet zu sein? Wie können sich Systeme selbstständig an veränderte Bedingungen anpassen?

Mit der fortschreitenden Digitalisierung und Vernetzung unserer Gesellschaft ist die Trennung von Safety- und Security-Aspekten bereits heute nicht mehr zeitgemäß.

Ein Lösungsansatz für diese Herausforderung für unsere Gesellschaft ist die Verbesserung der Fähigkeit von Systemen, mit widrigen Ereignissen umgehen zu können (Resilienz).

So beträchtlich der Bedarf an Sicherheit ausfällt, so häufig wird eine Unterversorgung mit Sicherheitslösungen konstatiert. Während sich der Frage nach hinreichenden Vorkehrungen für jeden Einzelnen prinzipiell mit Risikoabschätzungen und versicherungsmathematischen Erwägungen begegnen lässt, stellt die Sicherheit öffentlicher digitaler Raume und Infrastrukturen ein klassisches öffentliches Gut dar. Dementsprechend ausgeprägt zeigt sich in diesem Feld staatlicher Handlungsbedarf.

6.3 GESELLSCHAFTLICHE SICHT

Informationstechnik verändert unsere Gesellschaft. Neue Formen der Mitwirkung von Bürgern entstehen ebenso wie Debatten über digitalpolitische Themen und deren Auswirkungen.

6.3.1 Digitale Teilhabe

Die fortschreitende Digitalisierung persönlicher Lebenswelten bietet zunehmend neue und erweiterte Möglichkeiten demokratischer Beteiligung beziehungsweise Partizipation. So entstehen digitale öffentliche Räume, die der politischen Willensbildung dienen. Dafür stehen eine Reihe neuer Verfahren und Möglichkeiten zur Verfügung, die mit den weitgehend synonym verwendeten Stichwörtern E-Partizipation, digitale Teilhabe und elektronische Bürgerbeteiligung bezeichnet werden. [Expertise Digitale Teilhabe] In allen Begriffen wird bereits deutlich, dass das »Teilen« eine wesentliche Eigenschaft des Konzepts darstellt. Die Verfahren werden auf allen politischen Ebenen angewendet, angefangen bei Bürgerhaushalten auf kommunaler Ebene über Landes- und Bundesangebote wie E-Petitionen bis hin zu Online-Konsultationen der EU. Alle politischen Entscheidungen durchlaufen einen Prozess wie den in Abbildung 9 dargestellten Policy-Cycle. Da Beteiligungsaktivitäten zum Ziel haben, Entscheidungen zu beeinflussen, ist die Bereitschaft seitens offizieller Amts- und Mandatsträger, den Entscheidungsprozess für Austausch- und Mitwirkungsprozesse zu öffnen, Grundvoraussetzung.

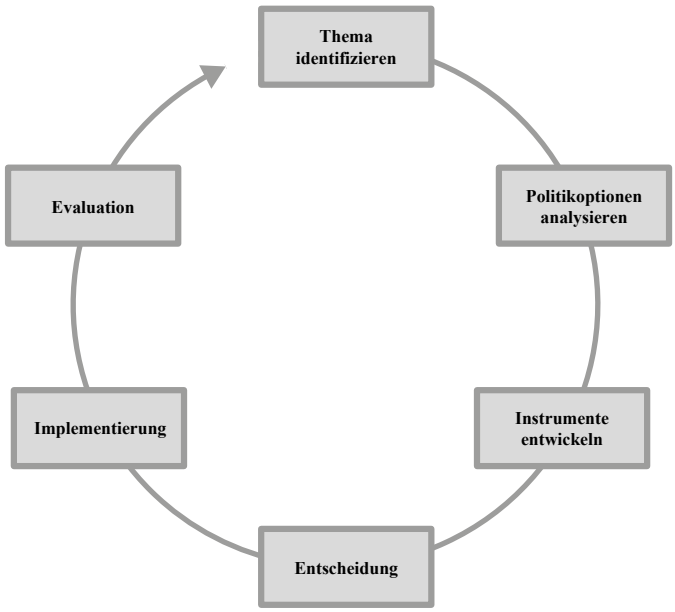

Abb. 13: Policy-Cycle für politische Entscheidungsprozesse nach [Bridgman und Davis 2003]

Die Unterstützung von Beteiligungsprozessen besteht aus unterschiedlichen technischen Elementen. Untersucht man mehrere Partizipationsvorhaben, so lassen sich häufig wiederkehrende Bestandteile identifizieren. Unterschieden werden können beispielsweise Werkzeuge, Bausteine und Verfahren:

- *Werkzeuge:* Als Werkzeuge werden in diesem Zusammenhang Softwarelösungen bezeichnet, die auch oder nur für Beteiligungsprozesse eingesetzt werden können. Werkzeuge haben oft einen Anwendungsschwerpunkt (zum Beispiel Informationsverbreitung oder gemeinsames Bearbeiten von Dokumenten). Beispiele sind Weblogs, Wikis, Umfrage- und Abstimmungssoftware oder Liquid-Democracy-Werkzeuge. Umfassende Übersichten und Beschreibungen wurden bereits von diversen Autoren erstellt, stellvertretend seien hier [Bächle 2006] oder [Geiger et al. 2013] genannt.
- *Bausteine:* Unter Bausteinen werden stark bis gar nicht strukturierte Methoden zur Beteiligung verstanden. Beispiele sind Umfragen oder unverbindliche Abstimmungen, gemeinsame Erarbeitung von Inhalten oder Kommentierung. Ausführlichere Übersichten sind zum Beispiel bei [Albrecht et al. 2008] zu finden.
- *Verfahren:* Als dritte Ebene innerhalb von Beteiligungsvorhaben lassen sich die Verfahrensweisen festmachen. Darunter werden hier einfache bis komplexe Abläufe zur Beteiligung verstanden. Zur Umsetzung von Verfahren werden häufig mehrere Bausteine und Werkzeuge in Kombination eingesetzt. Beispiele sind Bürgerhaushalte, Bürgerdialoge und Bürgergutachten. Diese Vorhaben können über analoge und digitale Phasen innerhalb eines Verfahrens verfügen. Eine umfangreiche Übersicht bieten beispielsweise [Nanz und Fritsche 2012].

Ein systematischer Überblick über die verschiedenen Elemente, einschließlich diverser Beispiele und Erfolgsfaktoren und -kriterien von Teilhabeprozessen, findet sich in der [Expertise Digitale Teilhabe].

Mit der Digitalisierung entstehen auch neue Formen demokratischer Beteiligung beziehungsweise Partizipation, allerdings mit dem Risiko, dass nicht jeder diese wahrnehmen kann.

Digitale Teilhabe bietet die Möglichkeit, viele Probleme der herkömmlichen Beteiligung auszugleichen oder abzuschwächen (zum Beispiel bessere Möglichkeit zum Diskurs, Beteiligung in der Fläche, zeitversetzte Beteiligung). Jedoch ergeben sich auch Risiken. Eine direktere Einbindung von Bürgern in Sachentscheidungen führt nicht zu einer gleichmäßigen Beteiligung. Vielmehr können sich hier diejenigen besser durchsetzen, die zum Beispiel besser für ihre Interessen mobilisieren können.

Verstärken digitale Beteiligungsformate den digitalen Graben? Während für die analoge Beteiligung bereits ein Ungleichgewicht zuungunsten von Personengruppen mit geringerer Bildung und geringeren finanziellen Ressourcen feststellbar ist, tritt bei der digitalen Partizipation die Herausforderung der technischen Affinität hinzu. Teilnehmende benötigen Zugang zur notwendigen Informationstechnik sowie ein Mindestmaß an Verständnis für die Nutzung entsprechender Plattformen.

Werden zu hohe Erwartungen geschürt, beispielsweise dass gemeldete Probleme sofort bearbeitet werden? Wird eine Erwartung geweckt, die nicht bedient werden kann (oder soll), so führt diese Pseudo-Beteiligung zu einem Glaubwürdigkeitsverlust der Beteiligenden.

Zudem gilt es, einen angemessenen Umgang mit digitalen Identitäten zu finden. Sind Anonymität (beispielsweise bei Wahlen) und Pseudonymität (beispielsweise in Foren) nutzerfreundlich realisierbar und je nach Teilhabeanwendung einfach wechselbar? Können aufgrund von Teilhabeaktivitäten zu viele personenbezogene Daten korreliert werden, um Personenprofile zu erstellen und etwa für politische Zwecke auszunutzen?

6.3.2 Bürgerschaftliches Engagement

Gemeinwohlorientiertes Engagement übernimmt Aufgaben, die sich Staat und Wirtschaft nicht leisten können, wollen, sollen oder dürfen. Ungeachtet der Frage nach Verantwortung und Zuständigkeiten ist die Ausübung bürgerschaftlichen Engagements also ein wichtiger Bestandteil unserer Gesellschaft, der dank der Gestaltung der Zivilgesellschaft wesentlich zum Gemeinwohl beiträgt. Fakt ist, dass in verschiedenen Bereichen viele Menschen gemeinnützige Arbeit leisten und damit direkt oder indirekt anderen Menschen helfen. Diese Engagierten weiter zu motivieren und den Zugang zu bürgerschaftlichem Engagement zu erleichtern und zu verbessern – hierbei kann IT unterstützen. [White Paper Bürgerschaftliches Engagement]

Bei digitalem bürgerschaftlichen Engagement übernimmt ein vernetztes System eine Schlüsselrolle bei Akquise, Vermittlung oder Ausübung

Digital wird Engagement, wenn ein System, das über Computer, mobile Endgeräte oder andere Zugänge erreichbar ist, eine Schlüsselrolle in den Bereichen Akquise, Vermittlung von Aktivitäten oder Ausübung des Engagements übernimmt. Digitales bürgerschaftliches Engagement ist also zunächst nichts originär Neues, sondern bezieht die Möglichkeiten, aber auch Herausforderungen der Digitalisierung ein. Digitale Funktionen können das bürgerschaftliche Engagement unterstützen oder auch Inhalt des Engagements sein.

Der Umfang unterstützender Funktionen variiert von der reinen Informationsbereitstellung (Websites, Newsletter, Apps) über kommunikative Dienstleistungen zwischen Organisationsmitgliedern und auch mit anderen Engagierten (soziale Netzwerke) bis hin zur Vermittlung von Engagement und Ressourcen (Ehrenamts- und Engagementbörsen). Eine Übersicht über die digitalen Unterstützungsbausteine mit kurz beschriebenen Beispielen findet man im [White Paper Bürgerschaftliches Engagement].

Engagement kann auch vollständig im Digitalen stattfinden. Das vielleicht bekannteste Beispiel digitaler Mitarbeit ist die Web-Enzyklopädie Wikipedia[6], auf der Artikel zu diversen Themenbereichen von Engagierten in digitalen Medien zusammengetragen, überprüft und einer breiten Öffentlichkeit kostenfrei zur Verfügung gestellt werden.

Zugang zu jeder Zeit und flexible Wahrnehmung der Beteiligung werden beim gesellschaftlichen Engagement zunehmend gewünscht und auch erwartet. Micro-Engagement für kleinteilige Einsätze spiegelt die Bedürfnisse eines wachsenden Anteils der Engagierten wider. Die Flexibilisierung reicht so weit, dass Elemente aus

[6] Die hohe Sichtbarkeit zeigt sich auch in Zahlen: Wikipedia belegt aktuell den siebenten Platz der weltweit meistbesuchten Websites (Stand 2015), verfügt über 37 Millionen Artikel in über 300 Sprachen und über 2 Millionen angemeldete Nutzer (Stand 2016). Vgl. Wikipedia; de.wikipedia.org/wiki/Wikipedia

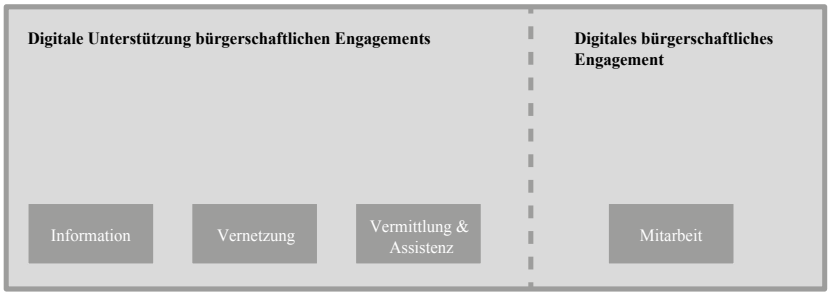

Abb. 14: Digitale Bausteine bürgerschaftlichen Engagements

Spielen herangezogen werden, wenn beispielsweise Engagierte für die Verschlagwortung und Kategorisierung von digitalisierten Objekten Punkte erhalten, die in Bestenlisten verglichen werden. Eine solche als Gamification [Trendthema Gamification] bezeichnete Motivation zur Beteiligung findet aktuell in verschiedensten Anwendungsfeldern Beachtung. Wird die Arbeit an eine Gruppe Engagierter ausgelagert, die auf dieselben Ressourcen zugreifen kann, wird dies als Crowdsourcing bezeichnet.

Im Hinblick auf kleinteiligere Formen des Engagements stellt sich die Frage, ob die Koordination des Einzelengagements überproportional zum Nutzen erschwert wird. Bedeutet der Einsatz von IT für die Organisationen schließlich sogar einen Mehraufwand ohne konkreten Nutzen? Nehmen zukünftig ortsgebundene und langfristige Einsätze ab, da man sich minimal engagiert, mitunter nur durch Mausklicks? Verursacht mangelnde Souveränität im Umgang mit digitalen Medien auch den Ausschluss von Mitarbeitern oder Engagierten? Und müssen aus diesem Grunde Doppelstrukturen aufrechterhalten werden, wenn beispielsweise die Mitgliedszeitschrift sowohl auf dem Postweg versandt wird, als auch in einer für den Online-Versand optimierten Form erstellt werden muss? Sich deshalb weniger intensiv auf die Digitalisierung einzulassen, führt jedoch zum faktischen Ausschluss von digital Interessierten.

Möglicherweise liegt ein wesentlicher Lösungsansatz für die Bewältigung der Mehrarbeit gerade in der Aktivierung digitalen bürgerschaftlichen Engagements. Im Rahmen dessen werden nicht nur angepasste Softwarelösungen entwickelt. Die organisationsbezogene Anpassung könnte ein spannendes Betätigungsfeld für technikaffine Interessierte sein, die sich von anderen Aufgaben möglicherweise weniger angesprochen fühlen. In jedem Fall sollte den Herausforderungen frühzeitig begegnet werden, um die Potenziale der Digitalisierung für bürgerschaftliches Engagement ausschöpfen zu können.

Zugang zu jeder Zeit und flexible Wahrnehmung der Beteiligung werden beim gesellschaftlichen Engagement zunehmend gewünscht und auch erwartet.

6.3.3 Verschlüsselung

Sicherheitsbehörden diskutieren nach Sicherheitsvorfällen wie »Nine Eleven« oder den Datenlecks durch Edward Snowden wiederholt eine Regelung für die Verschlüsselung, die ein legales Entschlüsseln ermöglicht. [Schulzki-Haddouti 2015] Die Argu-

mente für beziehungsweise wider Verschlüsselung ändern sich dabei nicht wesentlich. Für Verschlüsselung sprechen der Schutz der Privatsphäre, wie beispielsweise bei der privaten Kommunikation mit dem Arzt oder beim Online-Banking, die Wahrung von Geschäftsgeheimnissen und Urheberrechten in der Wirtschaft, die vertrauliche behördliche Kommunikation oder der Datenschutz in der Cloud. Gegen Verschlüsselung spricht die notwendige Bekämpfung von Terrorismus und Kriminalität durch die Strafverfolgungs- und Sicherheitsbehörden.

Um mit diesem Zwiespalt umzugehen, hat der Staat verschiedene Optionen: (1) Verbot von Verschlüsselungstechnik, (2) Ermöglichen von staatlichen Eingriffen in die Verschlüsselung oder (3) keine Kryptoregulierung.

Ein totales Verschlüsselungsverbot (Option 1) widerspricht unserer Kultur, die unter anderem mit dem Recht auf informationelle Selbstbestimmung den Datenschutz und die Privatsphäre respektiert. Auch eine Schwächung der Verschlüsselungstechnik, beispielsweise durch das Verbot von starken Schlüsseln oder von Verschlüsselung für bestimmte Software-Anwendungen, hindert keinen Kriminellen an seinen Taten. Es gibt viele andere Möglichkeiten, geheime Botschaften zu versenden: Steganografie erlaubt das Verstecken von Daten in Bildern, Absprachen können in Geheimsprachen stattfinden oder verbotene Kommunikation wird in andere Länder ohne diesbezügliche Gesetzgebung verlagert.

Zivilgesellschaft, Wirtschaft, aber auch der Staat sind auf vertrauliche Kommunikation im digitalen Raum angewiesen. Jede Schwächung von Verschlüsselung betrifft daher alle Gesellschaftsbereiche.

Das zwangsweise Hinterlegen von privaten Schlüsseln (Option 2) bei einem vertrauenswürdigen Dritten (zum Beispiel Datennotar, Polizei, Bank) würde dem Staat die Möglichkeit eröffnen, durch eine Kombination aus organisatorischen, technischen und juristischen Maßnahmen diese Schlüssel legal zur Entschlüsselung zu nutzen. Die Gefahr, dass diese Schlüsselpools von Kriminellen oder Geheimdiensten kompromittiert werden, wäre allerdings sehr hoch. Andere Varianten, um staatliche Zugriffe zu ermöglichen, sind die Beeinflussung der Standardisierung der Verschlüsselungsalgorithmen oder der Schlüsselgenerierung, das Ausnutzen von bestehenden Sicherheitslücken oder der zwangsweise Einbau von Hintertüren in Verschlüsselungssoftware oder -hardware. Aber wie soll hier gewährleistet werden, dass nur der eigene Staat diese Lücken nutzen kann?

Ohne Kryptoregulierung (Option 3) muss der Staat andere Möglichkeiten der Kriminalitätsbekämpfung nutzen und diese sogar verbessern, um seine Bürger zu schützen.

Generell lässt sich zusammenfassen, dass eine Schwächung von Verschlüsselung alle Gesellschaftsbereiche betrifft. Zivilgesellschaft, Wirtschaft, aber auch der Staat sind auf vertrauliche Kommunikation im digitalen Raum angewiesen. Die Optionen 1 und 2 sind daher eher auszuschließen. Eine Studie des Ausschusses für Technikfolgenabschätzung des EU-Parlaments (Science and Technology Options Assessment, STOA) zeigt unter anderem, dass EU-Bürger Online-Privatsphäre sogar noch viel zu wenig nutzten. [Europäisches Parlament 2014] Das ist sicherlich auch dadurch bedingt, dass Verschlüsselung trotz geeigneter Werkzeuge noch zu kompliziert ist. Schon die Anzahl an unterschiedlichen Werkzeugen für die Verschlüsselung von Festplatten, Speicherbereichen im Smartphone, Dokumenten, E-Mails, in sozialen Netzwerken

und für Telefonie, Nachrichten- oder Datenübermittlung wirkt eher abschreckend. Zusätzlich muss man noch die privaten Entschlüsselungsschlüssel sicher für eine lange Zeit ablegen und sollte diese auch nicht verlieren.
Aber gerade weil heutzutage die Unsicherheit im Internet zunimmt, stellen sich Fragen: Wie kann der Staat seine Bürger und Unternehmen zum sicheren Handeln ertüchtigen? Wie kann Kryptografie so verwendet werden, dass Integrität und Vertraulichkeit von legalen Daten und Kommunikation gewährleistet, aber gleichzeitig Terrorismus und Kriminalität nicht begünstigt werden?

7.

HANDLUNGSRÄUME

Die Auseinandersetzung mit öffentlicher IT hat eine Vielzahl von Herausforderungen und Handlungsfeldern aufgezeigt. Immer wiederkehrende Handlungsräume werden daher im Folgenden vorgestellt.

7.1 FRÜHZEITIGE IDENTIFIKATION RELEVANTER TRENDS

Ein Trend bezeichnet eine gerichtete Entwicklung einer Technologie oder eines Phänomens in einer Gesellschaft. Lässt sich ein solcher Trend in die Zukunft fortschreiben, lassen sich daraus Anforderungen, Herausforderungen und Möglichkeiten für die Zukunft ableiten. Eine Analyse der Trendwirkungen erlaubt so die Identifikation zukünftiger Handlungsfelder und bietet Entscheidungsunterstützung bei der Frage, wie sich schon heute den Herausforderungen von morgen begegnen lässt.

Grundlage der Folgenabschätzung bildet die Identifikation relevanter Trends und ihre angemessene Fortschreibung. In einigen Anwendungsfeldern erlaubt die Trägheit der Prozesse, ihre vielfältige gesellschaftliche Einbettung und die sich daraus ergebende Robustheit sowie die ausgezeichnete Datenbasis zum Status quo sehr genaue Voraussagen. Demografische Projektionen erlauben beispielsweise sehr exakte Schätzungen der natürlichen Bevölkerungsentwicklung über Jahrzehnte. Die Digitalisierung markiert in dieser Hinsicht den Gegenpol. Veränderungen sind hier oft sprunghaft, ergeben sich durch schnell entstehende Technologien oder auch nur durch die Rekombination von Altbekanntem und werden durch Begriffskonjunkturen begleitet, die nach Durchlaufen eines Hype-Zyklus ohne nennenswerte Wirkungen bleiben.

Zukunftsbezogene Aussagen können die Entscheidungsgrundlage erweitern und mehr Zeit für notwendiges Handeln schaffen.

Trendforschung zur Digitalisierung erweist sich somit gleichermaßen als besonders herausfordernd wie auch außerordentlich wichtig. Wenn disruptive Veränderungen ganze Branchen in wenigen Jahren auf den Kopf stellen und geschätzte Fertigkeiten und Kompetenzen wertlos machen können, muss eine wirksame Digitalpolitik vorausschauend agieren und für mögliche Zukünfte gewappnet sein. Neben der Identifikation relevanter Trends und ihrer Extrapolation in die Zukunft kommt der Betrachtung möglicher Folgen daher eine große Bedeutung zu. Dazu gilt es, Möglichkeitsräume wahrscheinlicher Entwicklungslinien zu erkennen und zu beschreiben, welche für die öffentliche IT und damit für die Gesellschaft insgesamt mit großen Veränderungen verbunden sein können. [ÖFIT-Trendschau] Die Erkenntnisse über mögliche Ausgestaltungen und Wirkungen in der Zukunft helfen auch bei der Entscheidungsfindung für grundlegende gesellschaftliche Fragen und potenzielle neue Regulierungsbedarfe in der Gegenwart.

7.2 E-GOVERNMENT ALS TEILBEREICH ÖFFENTLICHER IT

Die Bestandsaufnahme zum E-Government in Deutschland bietet ein ernüchterndes Bild. Zwar kommt innerhalb der Verwaltung diverse IT-Unterstützung zum Einsatz, doch in der Regel bleibt Bürgern der Weg zum Amt nicht erspart. [White Paper E-Government]

Soll ein wirksames E-Government geschaffen werden, ist politischer Wille auf allen Ebenen erforderlich, um es durchgängig an den Bedürfnissen der Bürger auszurichten. Dies muss mit neuen gesetzlichen Verbindlichkeiten untermauert werden, beispielsweise einem Recht des Bürgers auf vollständig digitalisierte Verwaltungsleistungen. Dabei gilt es, Kompetenzstreitigkeiten zu überwinden, um gemeinsame und einheitliche Lösungen realisieren zu können. Hierfür müssen übergreifende Gremien etabliert werden, die eine gemeinsame Koordinierung und Steuerung des Gesamtvorhabens übernehmen.

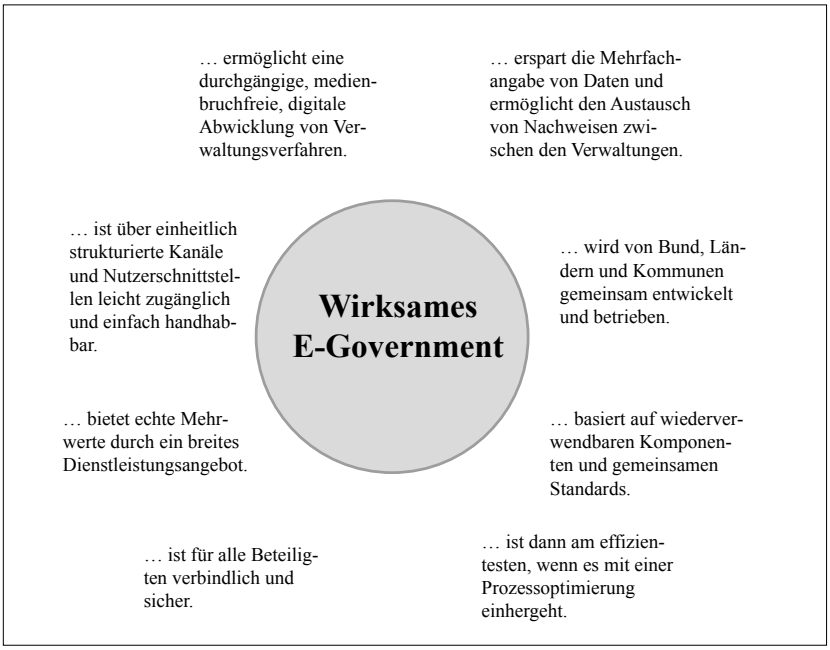

Abb. 15: Eckpunkte eines wirksamen E-Governments

Über die Ausgestaltung eines wirksamen E-Governments herrscht dabei weitgehende Einigkeit. Die elektronische Abwicklung muss zur Regel werden (Digital-by-Default). Für Verwaltungsleistungen muss das Prinzip des Vorrangs der digitalen Verfahrensabwicklung gelten. Die zur Beschreibung eines Sachverhalts oder einer Person dienenden Daten sollten nur einmal erfasst und bei Bedarf auch von anderen Behörden

benutzt werden (Once-only). Für die Verwaltung heißt das, erforderliche Nachweise, die an anderer Stelle innerhalb der Verwaltung vorliegen, nach Zustimmung der Betroffenen automatisiert einzuholen sowie nicht zustimmungsbedürftige Daten generell wiederzuverwenden.

7.3 MEDIENKOMPETENZ UND DIGITALE BILDUNG

Die breite Nutzung von IT verändert nachhaltig die Lebensgewohnheiten der Bürger. Hierfür müssen Nutzer aller Altersgruppen in die Lage versetzt werden, selbstständig absehen zu können, welche Auswirkungen ihr Handeln im digitalen Raum hat. Sie müssen verstehen, welche Prozesse ablaufen und welche Konsequenzen diese haben können. Nicht zuletzt müssen auch die Bürger selbst neue Verhaltensmuster für den Umgang im und mit dem digitalen öffentlichen Raum entwickeln. Technische Hintergründe sollten so weit verstanden werden, dass Bürger sich bewusst für oder gegen die Nutzung einer Anwendung oder eines Dienstes entscheiden können.

Medienkompetenz wird zunehmend auch zu einem Wirtschaftsfaktor und hat Einfluss auf die gesellschaftliche Entwicklung. Viele Unternehmen erwarten heute bereits, dass Arbeitnehmer ein gewisses Grundverständnis im Umgang mit Informationstechnik haben. Durch die beschriebenen qualitativen Veränderungen von Diensten und Anwendungen hat der Einsatz allgegenwärtiger IT-Komponenten weitergehende Konsequenzen als nur die zusätzliche mobile Nutzung bekannter Anwendungen. Die Fähigkeit des Einzelnen zur gezielten Informationsbewertung wird immer wichtiger, ebenso wie eine gesellschaftliche Auseinandersetzung mit der Erzeugung, Verarbeitung und Nutzung von Daten.

Nutzer aller Altersgruppen müssen selbstständig absehen können, welche Auswirkungen ihr Handeln im digitalen Raum hat.

Was sich für die Bürger individuell konstatieren lässt, kann auf Organisationen als Ganzes übertragen werden. Behörden sind heute im Bereich IT oftmals von externer Beratungsexpertise abhängig. Diese Expertise ist nicht nur ein erheblicher Kostenfaktor, viel relevanter ist die damit verbundene Abhängigkeit. Es muss daher im eigenen Interesse der Verwaltung sein, technische Beurteilungskompetenz zu erhalten oder aufzubauen. Das bedeutet auch, eine durchgängige Qualifikation der Mitarbeiterinnen und Mitarbeiter sicherzustellen. Kompetenzaufbau und -erhalt in einem hochdynamischen Umfeld betreffen also Individuen und Organisationen in Wirtschaft, Zivilgesellschaft und öffentlichem Sektor gleichermaßen.

Um die allgemeine Medienkompetenz zu steigern, ist in erster Linie der Staat gefordert, die entsprechenden Bildungsmöglichkeiten anzubieten. Aber auch Autodidaktik verspricht, durch die motivationsfördernde Wirkung selbstbestimmten Lernens eine zunehmend größere Bedeutung zu erlangen. [Trendthema Autodidaktik] In der Frage der Veränderung von Lehrmaterialien durch die Digitalisierung spiegeln sich viele Aspekte, die für die Digitalisierung der Gesellschaft insgesamt leitend sind. Die mögliche Allverfügbarkeit nahezu beliebig kombinierbarer Informationen macht den wesentlichen Unterschied zu Bildungsprogrammen im öffentlich-rechtlichen Regionalfernsehen der Vergangenheit aus. Digitale Lernmaterialien lassen sich grundsätzlich individualisiert zusammenstellen. Die Produktion solcher Materialien wird zudem

immer einfacher. Bereits mit preiswerten technischen Mitteln lassen sich Inhalte – auch multimedial – aufbereiten. Diese Möglichkeiten treffen auf eine große Gruppe von Beschäftigten in Bildung und Forschung, die schon von Berufs wegen einen beträchtlichen Bedarf an solchen Materialien haben. Austauschplattformen von Lehrmaterialien für Schulklassen erfreuen sich entsprechend wachsender Beliebtheit. Galt Autodidaktik bisher eher als Randerscheinung, könnte die selbstverständliche Nutzung digitaler Lernmaterialien mittelfristig die formale Bildung durch Elemente der autodidaktischen Aneignung erheblich ergänzen. Welche Potenziale dies wiederum hinsichtlich sozialer Chancengleichheit birgt, bleibt abzuwarten.

7.4 MOBILE NUTZUNG VON IT ALS NORMALFALL

Mit den aktuellen Möglichkeiten der mobilen Nutzung von Diensten und Anwendungen können die Bürger nahezu immer vernetzt und online sein. Digitale Mobilität entwickelt sich zu einem Leitbild der Gesellschaft, die uneingeschränkte Kommunikation fordert und jederzeit überall auf Informationen zugreifen will. Dies bedeutet, dass alle notwendigen Infrastrukturkomponenten, das heißt, Endgeräte, Netzzugänge, Netze und Anwendungen, die mobile Nutzung sinnvoll unterstützen müssen. Nur in ihrer Kombination schaffen sie die Möglichkeit für digitale Mobilität.

Neben der Ausweitung der Nutzung von IT ergeben sich auch qualitative Veränderungen: Die enge Bindung von Nutzer und Mobilgerät ermöglicht zunehmend spontane oder automatisierte Leistungsangebote in immer mehr Situationen. Dabei erfolgen eine Dynamisierung und Individualisierung, die weit über die reine Präsentation des Angebots hinaus reichen. Die Personalisierung der Endgeräte ermöglicht wiederum die Gestaltung neuer personalisierter Anwendungen, sodass es zu Rückkopplungen zwischen Nutzung und Dienst kommt.

Digitale Mobilität ist im heutigen Alltag, ja in der derzeitigen Kultur, nicht mehr wegzudenken.

Digitale Mobilität ist im heutigen Alltag, ja in der derzeitigen Kultur, nicht mehr wegzudenken. Zu vielfältig, praktisch und allgegenwärtig sind ihre Möglichkeiten – und fast täglich kommen neue Dienste hinzu. Um diese effektiv nutzen zu können, müssen Voraussetzungen geschaffen werden: Eine der wichtigen gesamtgesellschaftlichen Aufgaben der kommenden Jahre wird es sein, die Unterstützung der digitalen Mobilität so auszugestalten, dass sie optimal auf die jeweiligen Bedürfnisse der Nutzer, die kollektiven Bedürfnisse der Wirtschaft und die umfassenden Bedürfnisse der Gesellschaft abgestimmt werden kann.

7.5 NETZE, NETZE, NETZE

Ein entscheidender Standard für die Zukunft des Internets ist das Internetprotokoll Version 6 (IPv6). Nach mehr als 20 Jahren Entwicklung und Vorbereitung ist der Zeitpunkt gekommen, die Migration von der alten Version 4 (IPv4) auf IPv6 zügig voranzutreiben. Dies schafft eine Grundlage zur Unterstützung von neuartigen Anwendun-

gen und damit die Voraussetzung für weitere Innovationen auf Basis des Internets. IPv6 ermöglicht dabei auch neue Ansätze für den Betrieb und das Management der Netze selbst, hin zu einer dynamischeren Konfiguration und mehr Sicherheit.

IPv6 ist mehr als »IPv4 mit langen Adressen« – es ist ein moderner System-Baukasten für Netze.

Zunehmende Kommunikationsrelationen und eine Vielzahl von Endgeräten und Anwendungen erfordern ein automatisiertes und dynamisches Netzwerkmanagement. Die Automatisierung erhöht die Leistungsfähigkeit von Netzen und verhindert Fehler in komplexen Konfigurationen. Das Ziel ist, komplexe Netze über allgemein verständliche, überschaubare Regeln zu steuern, die auch den Nachweis eines korrekten Betriebs ermöglichen.

Die stetig steigende Nachfrage nach drahtloser Kommunikation erfordert eine andauernde Optimierung der Ausnutzung des nur begrenzt verfügbaren Frequenzspektrums. Technologisch sich abzeichnende oder bereits verfügbare Verfahren zur optimalen Nutzung bedürfen internationaler Abstimmung, lokaler Infrastrukturen und eines adäquaten Ordnungsrahmens.

7.6 STANDARDISIERUNG ALS GRUNDLAGE FÜR INNOVATION UND DYNAMIK

Um interoperable Lösungen zu erreichen, sind standardisierte Schnittstellen, Protokolle oder Technologien erforderlich. Das Verwenden von Standards ist dabei genauso wichtig wie die aktive Teilnahme an der Standardisierung, um eigene Interessen einbringen zu können und dabei beispielsweise die positiven Ergebnisse geförderter Projekte formal zu etablieren.

Normen und Standards bieten ein hohes Maß an Investitionssicherheit, wenn und solange sie für das Einsatzumfeld angemessen sind. Das sehr dynamische Einsatzumfeld IT kann häufige Anpassungen erforderlich machen, wenn die Normen und Standards nicht von vornherein eine große und vorausschauende Flexibilität besitzen, was jedoch wiederum zu einer hohen Komplexität führen kann.

Um technologische Innovationen und Weiterentwicklungen des Marktes im Bereich öffentlicher IT nicht durch zu restriktive Festlegungen zu behindern, sollten Standards bevorzugt werden, die einheitliche Anforderungen festlegen, statt bestimmte Lösungen zur Erfüllung der Anforderungen festzuschreiben. Dies bedeutet, dass es in der Regel ausreicht, funktionale und organisatorische Komponenten eines IT-Systems zu identifizieren und deren jeweilige Schnittstellen zu anderen Komponenten sowie geeignete Qualitäts- und Sicherheitsanforderungen festzulegen. Die konkrete interne Umsetzung der Funktionen einer Komponente kann hingegen dem Hersteller überlassen werden. [White Paper Standardisierung]

Ein generelles Problem von Standardisierungsprozessen ist deren Dauer von der Entstehung eines Bedarfs über die Initiierung eines Normungs- beziehungsweise Standardisierungsvorhabens bis zur Veröffentlichung und gegebenenfalls Verbindlichmachung eines Standards. Bei internationalen Normen sind 3 – 5 Jahre von der Initiierung bis zur Veröffentlichung durchaus keine Ausnahme, auch wenn mittlerweile kürzere Fristen angestrebt werden. [Expertise IT-Standardisierung] Die Zeit bis zur Umset-

zung kommt noch hinzu. Im schnelllebigen IT-Bereich besteht damit die Gefahr, dass Standards nicht zur Verfügung stehen, wenn sie gebraucht werden, und von der technologischen Entwicklung bereits überholt sind, wenn sie erscheinen.

Normung, Standardisierung und insbesondere die Verbindlichmachung von Normen und Standards müssen sich auf den notwendigen Umfang beschränken. Eine Überregulierung wirkt auch bei diesem Instrument innovationshemmend und verursacht vermeidbare Kosten, wenn sachlich unnötige Anforderungen festgeschrieben werden.

7.7 DIGITALE SOUVERÄNITÄT

Das Internet ist in seiner technischen Struktur zunächst unabhängig von politischen Strukturen wie Staaten und bildet einen eigenen virtuellen Raum. Darüber angebotene Dienste sind grundsätzlich international angelegt und werden weltweit nachgefragt. Kommunikationspfade orientieren sich nur an Staatsgrenzen, wenn dies explizit verlangt wird. Angebotene Dienste können prinzipiell von jedem Zugangspunkt des Internets genutzt werden, es sei denn, dies wird durch Filterung aktiv verhindert. Aus Datenschutzgründen wurden zeitweise Überlegungen zur gezielten Wahl von Kommunikationspfaden angestellt.

Auch wenn national angemessene Regelungen zum Beispiel zur Blockierung illegaler Inhalte gefunden werden, bleiben diese durch die Internationalität des Internets eventuell wirkungslos oder stellen sogar einen Wettbewerbsnachteil dar. Beispielsweise wird eine Blockierung deutscher Quellen zu einer vermehrten Nutzung ausländischer Quellen derselben Inhalte führen.

Auch wenn der Nutzen einer Nationalisierung des Internets begrenzt ist, gibt es dennoch Maßnahmen, die sinnvoll staatlich unterstützt werden sollten. Dazu gehören zum Beispiel Maßnahmen zur Erhaltung beziehungsweise Wiedererlangung nationaler digitaler Souveränität. Bitkom beschreibt »Digitale Souveränität« als die Fähigkeit zu selbstbestimmtem Handeln und Entscheiden im digitalen Raum. [Bitkom 2015] In Abgrenzung zu Fremdbestimmung und Autarkie umfasst digitale Souveränität die angemessene Leistungs- und Handlungsfähigkeit von Unternehmen, Staat sowie Bürgern innerhalb der existierenden digitalen Welt.

Selbstbestimmtheit und Entscheidungsfreiheit erfordern allerdings einige Grundlagen: [Bundesministerium für Wirtschaft und Energie 2015]

- Digitale Bildung für alle und technische Spitzenkompetenz, um Innovationen zu ermöglichen und Abhängigkeiten zu vermeiden.
- Technische Komponenten, die standardisierte Schnittstellen und Protokolle unterstützen, um Alternativlösungen jederzeit zu ermöglichen.
- Bewertung und Nachweisbarkeit der Sicherheit der Hard- und Software sowie vertrauenswürdige Akteure.
- Angemessener Schutz von geistigem Eigentum, Daten und Systemen.
- Forschungs- und Entwicklungsarbeit, um neue Trends und Technologien zu erkennen, zu gestalten und anzuwenden.

Die Stärkung digitaler Souveränität ist für die zukünftige Entwicklung und Anwendung öffentlicher IT eine wesentliche Voraussetzung. Dies gilt in allgemeiner Form für jeden Einzelnen und in spezieller, erweiterter Ausprägung für IT-Verantwortliche und -Zuständige der öffentlichen Hand.

7.8 SPANNUNGSFELD SICHERHEIT VS. NUTZERFREUNDLICHKEIT

Sicherheit darf nicht primär vom Benutzer beziehungsweise der Benutzung abhängen.

Um Informationssicherheit zu gewährleisten, werden meist Anforderungen an die Fähigkeiten der Nutzer gestellt, wie beispielsweise Passwortregeln, Patch-Verhalten oder Installationsanweisungen. Ebenso wie ein Schutz vor Fehlbedienung in IT-fernen Bereichen längst Standard ist, so müssen zukünftig auch IT-nahe Produkte und Systeme eine sichere Benutzung garantieren. Auch wenn eine Sensibilisierung und Befähigung der Menschen für Sicherheitsaspekte weiter gefördert werden muss, sollte die Hauptverantwortung für Sicherheit von den Herstellern und Betreibern nicht auf den Endnutzer abgewälzt werden dürfen.

Ein Mehr an Sicherheit bedeutet zumeist Einbußen beim Nutzungskomfort und umgekehrt. Daher muss für jeden Anwendungsfall ein angemessener Kompromiss zwischen beiden Aspekten gefunden werden. Der Zusammenhang zwischen Sicherheit und Usability wird von Yee so dargestellt: »Sicherheit schränkt den Zugriff auf Operationen ein, die unerwünschte Ergebnisse haben, während Usability den Zugang zu Operationen verbessert, die erwünschte Ergebnisse haben. Ein Konflikt entsteht erst dann, wenn Informationen fehlen, die entscheiden lassen, ob ein bestimmtes Ergebnis erwünscht war.« [Yee 2004] Diese Entscheidung ist komplizierter, wenn beispielsweise Fehlermeldungen nicht verständlich sind oder die Funktionalität zu umfassend ist. Eine Möglichkeit wäre die Reduzierung von Funktionalität, um Sicherheit und Nutzerfreundlichkeit besser miteinander zu harmonisieren. In jedem Fall richten Sicherheitstools höchste Anforderungen an ihre eigene Usability.

7.9 EUROPÄISCH DENKEN

In den Mitgliedstaaten der EU entstehen viele, oftmals unterschiedliche Lösungen für die verschiedenen Anwendungsdomänen. Interoperabilität wird dann nachträglich in EU-Großprojekten (beispielsweise STORK, e-SENS) geschaffen. Diese Projekte dienen häufig auch als Input für die europäische Standardisierung und Regulierung.

Daher ist das Engagement Deutschlands in europäischen Projekten, Standardisierungsgremien und EU-Gesetzgebungsprozessen wesentlich, um rechtzeitig EU-interoperable Lösungen zu schaffen.

Auch wenn gute nationale Lösungen entstehen, werden diese oft nicht von anderen EU-Ländern übernommen. Dies kann zeitliche, organisatorische, lizenzrechtliche, sprachliche oder auch technische Gründe haben. Intensiver Wissens- und Informati-

onsaustauch mit europäischen Partnern und frühzeitige (auch bilaterale) grenzüberschreitende Teststellungen können europäische Interoperabilität beschleunigen und unterstützen.

7.10 DIGITALE GOVERNANCE

Aus der zunehmenden Bedeutung von Informationstechnologie und der durch sie bewirkten Digitalisierung und Vernetzung ergeben sich sowohl erheblich wachsende als auch grundsätzlich neuartige Herausforderungen für die öffentliche Hand. Insbesondere gilt es, den Prozess der digitalen Transformation von Gesellschaft, Wirtschaft, Verwaltung und Politik der Rolle des Staates entsprechend adäquat zu begleiten und mitzugestalten. Über das IT-Management von E-Government-Lösungen hinaus ist hierzu eine umfassendere IT-Governance – also eine strategisch-politische Gestaltung und Führung des IT-Einsatzes – in der Verwaltung und für öffentliche IT unabdingbar.

Im Hinblick auf Wirtschaft und Gesellschaft insgesamt ist selbst dies nicht hinreichend, sondern darüber hinaus eine strategisch-politische Gestaltung und Führung im Sinne einer »Digitalen Governance« erforderlich. [Diskussionspapier Digitale Governance] Ein wesentliches Element einer guten Governance besteht darin, ihre Einzelmaßnahmen in den Kontext einer übergreifenden Strategie zu stellen und aufeinander abzustimmen. Hierzu sind zusätzlich strategische Ziele zu formulieren, Kriterien für das Erreichen dieser Ziele zu definieren und die Zielerreichung zu kontrollieren.

8.

GESAMTÜBERSICHT

In Kapitel 6 wurden drei Perspektiven identifiziert, um das Konzept der öffentlichen IT zu fassen: die technologische Sicht, die anwendungsspezifische Sicht und die gesellschaftliche Sicht. Wie stellen sich die identifizierten Handlungsräume aus diesen Perspektiven dar beziehungsweise was muss konkret getan werden, um die Handlungsräume auszufüllen?

In der nachfolgenden Gesamtübersicht werden die Handlungsräume aus den verschiedenen Perspektiven beleuchtet. Dabei ergeben sich für die technologische und die anwendungsspezifische beziehungsweise für die anwendungsspezifische und die gesellschaftliche Perspektive mitunter analoge Ansprüche und Erfordernisse, sodass sie in Einzelfällen nicht trennscharf voneinander abzugrenzen sind.

Handlungsräume	**Technologische Sicht**	**Anwendungsspezifische Sicht**	**Gesellschaftliche Sicht**
Trenderkennung	Forschungsgeschehen und Entwicklung intensiv beobachten und durch Förderung gezielt Impulse setzen	Innovationsförderliche Bedingungen schaffen, z. B. Inkubatoren, Testbeds, Wettbewerbsrecht; Marktdurchdringung bei der Trenderkennung berücksichtigen	Gesellschaftliche und politische Technikfolgenabschätzung frühzeitig durchführen
E-Government	Sichere, interoperable E-Government-Lösungen schaffen	Anwendungen konsequent an Nutzen und Nutzern orientieren	Teilhabe ermöglichen und Erleichterungen für Bürger sowie Unternehmen schaffen
Medienkompetenz	Durch die Gestaltung von Technologien und Anwendungen möglichst breiten Bevölkerungsschichten den Zugang zur digitalen Welt ermöglichen, z. B. durch Barrierefreiheit, Responsivität, altersgerechte Angebote im Hard- wie Softwarebereich		Persönliche und organisationale Medien- und IT-Kompetenz aufbauen und erhalten, u. a. durch Bildungsangebote wie Medienkunde als Schulfach
Digitale Mobilität	Flächendeckend für vielfältigen Netzzugang sorgen, auch über öffentliche WLAN-Netze und Innovationen wie 5G	Anwendungen bereitstellen, die auch mobil und über verschiedene Geräte und Geräteklassen hinweg nahtlos nutzbar sind	Gesellschaftliches Bedürfnis nach Mobilität und die entsprechende gesellschaftliche Entwicklung unterstützen

Netze	Für den kontinuierlichen, bedarfsgerechten Ausbau einer leistungsfähigen Netzinfrastruktur mit flächendeckend breitbandigem Zugang sorgen	Innovative Anwendungen unterstützen, die durch die Leistungsfähigkeit der Netze ein besseres Nutzererlebnis erreichen	Gesellschaftliche Teilhabe sicherstellen sowie Wettbewerb und Innovation fördern
Standardisierung	Aktiv an nationaler und internationaler Standardisierung beteiligen, etwa ISO, DIN, VDI/VDE, BSI, IETF	Standardkonforme Lösungen bevorzugen	Freie und offene Standards priorisieren
Digitale Souveränität	Nationale und europäische technologische und anwendungsspezifische Kompetenzen erhalten und ausbauen, z. B. Verschlüsselungshardware		Digitale Selbstbestimmung durch Medienkompetenz, vertrauenswürdige Infrastrukturen und angemessenen Schutz von Daten und geistigem Eigentum ermöglichen
Sicherheit vs. Nutzerfreundlichkeit	Sicherheit und Nutzerfreundlichkeit von Beginn an mitdenken (Safety und Security by Design, Usability)	Sicherheitsanwendungen möglichst nutzerfreundlich gestalten (z. B. Verschlüsselungsanwendungen)	Mindestvorgaben für Sicherheit und Nutzerfreundlichkeit schaffen
Europäische Lösungen	Den europäischen Markt mitdenken, z. B. durch gemeinsame Forschung und Entwicklung, die Berücksichtigung und ggf. Wiederverwendung bereits vorhandener Lösungen und die Nutzung europäischer Standards und Schnittstellen	Interoperabilität nationaler Lösungen sicherstellen und durch die Nutzung europäischer Standards und Schnittstellen für Mitbewerber öffnen, z. B. bei Smart Home Anwendungen	Deutsche Interessen in die europäische Harmonisierung verstärkt einbringen
Digitale Governance	Konzepte, Strategien und Vorgaben zur Mitgestaltung der digitalen Transformation aller Lebens- und Arbeitsbereiche entwickeln und umsetzen		

Abb. 16: Konkretisierung der Handlungsräume aus den verschiedenen Perspektiven

9.

GLOSSAR / BEGRIFFE

Aktuator, (Aktor)	Während Sensoren eine physikalische Größe in elektrischen Strom umwandeln, machen Aktoren oder Aktuatoren genau das Gegenteil und wandeln Strom oder Spannung in eine andere Energieform um, so beispielsweise in Schall, Druck, Temperatur, Bewegung, Drehmoment, Licht usw. (www.itwissen.info)
Ambient Assisted Living (AAL)	Technologische Lösungen, Konzepte, Dienstleistungen und technische Infrastrukturen, die das häusliche Umfeld mit Hilfsinstrumenten ausstatten.
Anonymisierung	Die Anonymisierung ist das Verändern personenbezogener Daten dahingehend, dass diese Daten nicht mehr einer Person zugeordnet werden können. (www.wikipedia.de)
Augmented Reality	Wiedergabe realer Szenen (speziell Video), die direkt um zum Beispiel erläuternde oder spielerische Elemente ergänzt sind.
Big Data	Methoden und Technologien für die umfangreiche Erfassung, Aufbereitung, Speicherung und Analyse strukturierter und unstrukturierter Daten.
Botnet, Botnetz	Mit Schadsoftware infizierte Computer, die von Kriminellen ferngesteuert und beispielsweise für Spam-Versand und für Attacken auf andere Computer missbraucht werden. (www.botfrei.de)
Bring Your Own Device (BYOD)	Nutzung privater Endgeräte in der IT-Infrastruktur von Unternehmen oder Organisationen.
Cloud-Computing	Cloud-Computing ist ein Modell, das es erlaubt, bei Bedarf jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (zum Beispiel Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können. (www.bsi.bund.de)
Cyber-physische Systeme	Systeme, bei denen informations- und softwaretechnische mit mechanischen beziehungsweise elektronischen Komponenten verbunden sind, wobei Datentransfer und -austausch sowie Kontrolle beziehungsweise Steuerung über eine Infrastruktur wie das Internet in Echtzeit erfolgen. (wirtschaftslexikon.gabler.de) Sie sind die Grundlage für das Internet der Dinge und dessen Anwendung in Industrie 4.0 oder auch Smart Cities.
Datenschutz	Die technischen Anforderungen für den Datenschutz sind Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit.
Digitale Governance	Strategisch-politische Gestaltung und Führung der Digitalisierung.

Digitale Gräben	Unterschiede in der Souveränität im Umgang mit digitalen Medien und ihrer Nutzung.
Digitale Identität	Jede mögliche Form von technisch abgebildeten Daten, die zu einer Person gehören [ULD 2007]. Neben Personen können auch Organisationen, Objekte oder Geschäftsprozesse identifiziert werden.
Digitale Mobilität	Die durch Technik unterstützte Bewegung in physischen und virtuellen Räumen.
Digitale Unversehrtheit	Übertragung des Grundrechts auf körperliche Unversehrtheit auf die digitale Welt.
Digitalisierung	Die zunehmende Vernetzung und Durchdringung von immer mehr Lebensbereichen mit IT.
Disruption	Disruptive Entwicklungen sind Innovationen, die bestehende Technologien oder Dienstleistungen, aber auch kulturelle Gepflogenheiten teilweise oder komplett zerstören und irreversible Veränderungen hervorrufen.
Filterblase	Effekt der Vorsortierung von Online-Inhalten durch Software auf Basis des Surfverhaltens und weiterer Merkmale wie Ort oder verwendetes Endgerät.
Hashfunktion, Hashwert	Hashfunktionen sind Komprimierungsfunktionen, die eine Nachricht beliebiger Länge auf eine Nachricht fester Länge (zum Beispiel 128 oder 164 Bits) – den Hashwert – verdichten. (www.secupedia.info)
Informations-technologie (IT)	Oberbegriff für alle mit der elektronischen Datenverarbeitung in Berührung stehenden Techniken (wirtschaftslexikon.gabler.de), je nach Kontext auch Technologie der Gewinnung, Speicherung und Verarbeitung von Informationen. (www.duden.de)
Internet der Dienste	Gesamtheit der Dienste, zum Beispiel zur Leistungserstellung oder Arbeitsunterstützung, die durch Datenaustausch zwischen den Beteiligten in vernetzten Prozessen elektronisch nutzbar und abwickelbar sind.
Internet der Dinge	Gesamtheit der digitalen Repräsentationen von Dingen, die durch Sensoren, Aktuatoren und Vernetzung an IT-Systeme gekoppelt sind.
IP	Internetprotokoll.
KMU	Abkürzung für kleine und mittlere Unternehmen.
Kritische Infrastruktur	Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. (www.kritis.bund.de)

Liquid Democracy	»Flüssige Demokratie«: Bezeichnung einer Demokratie, in der jeder die Möglichkeit hat, entweder am Entscheidungsprozess teilzunehmen oder seine Stimme zu delegieren. (definition.cs.de)
Nonliner	Menschen, die das Internet willentlich nicht nutzen.
Öffentliche IT	Öffentliche IT bezeichnet den gesellschaftspolitischen Gestaltungsanspruch an die Digitalisierung.
Öffentlicher Raum	Das Wesen des öffentlichen Raumes kennzeichnen Zugänglichkeit und gesellschaftliche Funktion.
Öffentliches Gut	Öffentliche Güter zeichnen sich durch Nicht-Ausschließbarkeit und Nicht-Rivalität im Konsum aus.
Open Data	Datenbestände, die maschinenlesbar sind und ohne Nutzungsbeschränkungen bereitgestellt werden.
Plattform	Bereitstellung einer einheitlichen Basis für die Entwicklung und/ oder Ausführung von Anwendungen und Diensten.
Privacy Divide	Differenz zwischen denjenigen Menschen, die ihre Privatheit schützen können, und jenen, die dies nicht können.
Pseudony-misierung	Bei der Pseudonymisierung wird der Name oder ein anderes Identifikations-merkmal einer Person durch ein Pseudonym (zumeist eine mehrstellige Buchstaben- oder Zahlenkombination, auch Code genannt) ersetzt, um die Identifizierung des Betroffenen auszuschließen oder wesentlich zu erschweren. (www.wikipedia.de)
Reale Virtualität	Beschreibt die Wirkung der digitalen Welt auf ihre Umgebung und ihr aktives Eingreifen, beispielsweise durch die Steuerung realer Gegenstände.
Resilienz	Die Fähigkeit, tatsächlich oder potenziell widrige Ereignisse abzuwehren, sich darauf vorzubereiten, sie einzukalkulieren, sie zu verkraften, sich davon zu erholen und sich ihnen immer erfolgreicher anzupassen. [acatech 2014]
Safety	Das System soll die Umgebung nicht schädigen.
Security	Die Umgebung soll das System nicht schädigen.
Security by Design	Berücksichtigung von Sicherheitsaspekten bereits bei Herstellung und Programmierung von Hard- und Softwarekomponenten, damit Sicherheit möglichst unabhängig von Nutzer und Benutzung wird.

Sensor	Siehe auch Aktuator. Für eine automatisierte Unterstützung von Personen und Prozessen sind hochwertige und vielfältige Informationen notwendig, die unter anderem durch technische »Sinnesorgane«, sogenannte Sensoren, erfasst werden können (beispielsweise zum Messen von Umwelt- und Verkehrsdaten).
Smart City	Konglomerat öffentlich verantworteter Informationstechnik zur Verknüpfung nahezu aller Bereiche der Daseinsvorsorge, um knappe Ressourcen nachhaltig zu nutzen.
Smart Energy	Systeme zur effizienten Verwendung und zum dezentralen Gewinnen, Erzeugen, Verteilen und Speichern von Energie.
Smart Grid	Intelligentes Stromnetz.
Smart Home	Vernetzung und Smartifizierung von Dingen im eigenen Zuhause.
Smart Meter	Geräte zur Erfassung und gegebenenfalls Übermittlung von Messdaten über Energieverbrauch und -produktion.
Smartifizierung	Anreicherung von Dingen jeglicher Art mit digitaler »Intelligenz«.

10.

LITERATURVERZEICHNIS

Publikationen und Trendthemen, die vom Kompetenzzentrum Öffentliche IT (ÖFIT) des Fraunhofer-Instituts für Offene Kommunikationssysteme (FOKUS) herausgegeben wurden, werden in zwei Tabellen aufgelistet. Danach folgen die bibliografischen Angaben der referenzierten externen Publikationen.

ÖFIT-PUBLIKATIONEN (STAND 2016)

Kurztitel	**Originaltitel**	**Autoren, Jahr**
Expertise Online-Ausweisfunktion	3 Jahre Online-Ausweisfunktion – Lessons learned	Fromm, Jens; Hoepner, Petra; Pattberg, Jonas; Welzel, Christian (2013)
White Paper Big Data	Big Data – Ungehobene Schätze oder digitaler Albtraum	Eckert, Klaus-Peter; Henckel, Lutz; Hoepner, Petra (2014)
Expertise Cloud-Fahrplan	Cloud-Fahrplan für die öffentliche Verwaltung	Deussen, Peter H.; Eckert, Klaus-Peter; Hoepner, Petra; Hoffmann, Christian; Strick, Linda (2014)
Spezialedition Trendsonar	Das ÖFIT-Trendsonar der IT-Sicherheit	Opiela, Nicole; Hoepner, Petra; Weber, Mike (2016)
Diskussionspapier Digitale Bildung	Digitale Bildung – Ein Diskussionspapier	Opiela, Nicole; Weber, Mike (2016)
Diskussionspapier Digitale Governance	Digitale Governance – Ein Diskussionspapier	Stemmer, Michael (2016)
White Paper Digitale Mobilität	Digitale Mobilität – Dynamik im öffentlichen Raum	Schmoll, Carsten; Tiemann, Jens; Welzel, Christian (2014)
Expertise Digitale Teilhabe	Digitale Teilhabe	Klessmann, Jens; Löhe, Martin G.; Müller, Lena-Sophie (2014)
White Paper Bürgerschaftliches Engagement	Digitales bürgerschaftliches Engagement	Hinz, Ulrike; Wegener, Nora; Weber, Mike; Fromm, Jens (2014)

White Paper E-Governmentt	E-Government in Deutschland: Vom Abstieg zum Aufstieg	Fromm, Jens; Welzel, Christian; Nentwig, Lutz; Weber, Mike (2015)
White Paper Fortschrittliche Netze	Fortschrittliche Netze: Fundament für öffentliche Informationstechnologie	Fromm, Jens; Schmoll, Carsten; Tiemann, Jens; Weber, Mike (2013)
White Paper IT-Projekte	IT-Projekte: kleiner, feiner, überschaubarer	Gottschick, Jan; Hartenstein, Heiko (2015)
Expertise IT-Standardisierung	IT-Standardisierung in der öffentlichen Verwaltung	Stemmer, Michael; Goldacker, Gabriele (2015)
Diskussionspapier IT-Standardisierung	IT-Standardisierung in der öffentlichen Verwaltung – Ein Diskussionspapier	Stemmer, Michael; Goldacker, Gabriele (2014)
Spezialedition Digitale Gesellschaft	Menschen in der digitalen Gesellschaft	Fromm, Jens; Hansen, Marit; Hornung, Gerrit; Müller, Philipp; Ruge, Kay; Springeneer, Helga (2014)
White Paper Öffentliche Informationstechnologie	Öffentliche Informationstechnologie: Abgrenzung und Handlungsfelder	Fromm, Jens; Hoepner, Petra; Weber, Mike; Welzel, Christian (2013)
Tätigkeitsbericht	Öffentliche IT – Die ersten zwei Jahre	Kompetenzzentrum Öffentliche IT (2015)
White Paper Digitale Gesellschaft	ÖFIT-Atlas der Digitalisierung	Weigand, Florian; Bieker, Lisa; Gorny, Dominic; Weber, Mike (2015)
ÖFIT-Trendschau	ÖFIT-Trendschau: Innovationsfelder öffentlicher IT	Fromm, Jens; Gauch, Stephan; Kaiser, Tristan; Weber, Mike (2013)
Spezialedition Referenzmodell öffentliche IT	Referenzmodell öffentliche IT	Fromm, Jens; Hoepner, Petra; Welzel, Christian (2014)
White Paper Safety und Security	S^2: Safety und Security aus dem Blickwinkel der öffentlichen IT	Menz, Nadja; Hoepner, Petra; Tiemann, Jens; Koußen, Frank (2015)

White Paper Standardisierung	Standardisierung für die öffentliche IT	Stemmer, Michael; Goldacker, Gabriele (2014)
White Paper Internet-Modell	Vernetzung als Infrastruktur – Ein Internet-Modell	Tiemann, Jens; Goldacker, Gabriele (2015)
White Paper Vertrauenswürdige digitale Identität	Vertrauenswürdige digitale Identität: Baustein für öffentliche IT	Fromm, Jens; Welzel, Christian; Hoepner, Petra; Pattberg, Jonas (2013)

Alle herausgegeben vom Kompetenzzentrum Öffentliche IT, Fraunhofer FOKUS. Berlin.
Online verfügbar unter www.oeffentliche-it.de/publikationen.

ÖFIT-TRENDTHEMEN (STAND 2016)

3D-Drucker
5G
Ambient World
Autodidaktik
Autonomes Fahren
Blockchain
Cloud-Computing
Darknet
Daten-Philanthrop
Denkende Maschinen
Digitale Gräben
Digitale Mobilität
Digitale Unversehrtheit
Digitaler Nachlass
Digitaler Sport
Drohne
Gamification
Glokalisierung
Immersion
Indoor-Navigation
Industrie 4.0
Internet der Dinge
Kryptowährung
Massenmedien
Mensch-Maschine-Interaktion
Microservices
Mikroengagement
Mobile Money
No-Government
Peripherie
Post Privacy
Prosument
Security by Design
Selbstorganisation
Sichere Fahrzeugkommunikation
Stupsen
Usability
Verwaltung x.0
Vorhersagende Polizeiarbeit
Wearables
Werbeblocker

Autorinnen und Autoren der Gesamtausgabe: Mike Weber, Stephan Gauch, Faruch Amini, Tristan Kaiser, Jens Tiemann, Carsten Schmoll, Lutz Henckel, Gabriele Goldacker, Petra Hoepner, Nadja Menz, Maximilian Schmidt, Michael Stemmer, Florian Weigand, Christian Welzel, Jonas Pattberg, Nicole Opiela, Florian Friederici, Jan Gottschick, Jan Dennis Gumz, Valerie Albrecht, Jens Fromm

Alle erschienen in: Jens Fromm und Mike Weber (Hg.): ÖFIT-Trendschau: Öffentliche Informationstechnologie in der digitalisierten Gesellschaft. Berlin: Kompetenzzentrum Öffentliche IT. www.oeffentliche-it.de/trendschau/.

EXTERNE PUBLIKATIONEN

acatech (Hg.) (2011): Smart Cities. Deutsche Hochtechnologie für die Stadt der Zukunft. Aufgaben und Chancen. Deutsche Akademie der Technikwissenschaften. Online verfügbar unter www.acatech.de/de/publikationen/stellungnahmen/acatech/detail/artikel/smart-cities-deutsche-hochtechnologie-fuer-die-stadt-der-zukunft-1.html.

acatech (Hg.) (2014): »Resilience-by-Design«: Strategie für die technologischen Zukunftsthemen. Online verfügbar unter www.acatech.de/de/publikationen/stellungnahmen/acatech/detail/artikel/resilien-tech-resilience-by-design-strategie-fuer-die-technologischen-zukunftsthemen-1.html.

Albrecht, Steffen; Kohlrausch, Niels; Kubicek, Herbert; Lippa, Barbara; Märker, Oliver; Trénel, Matthias et al. (2008): E-Partizipation – Elektronische Beteiligung von Bevölkerung und Wirtschaft am E-Government. Studie im Auftrag des Bundesministeriums des Innern. Online verfügbar unter www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/studie_e_partizipation.html.

Arnold, Patrick (2009): Information und Wissen. Online verfügbar unter www.informatik.uni-leipzig.de/~graebe/Texte/Arnold-09.pdf.

Bächle, Michael (2006): Social Software. In: *Informatik Spektrum* 29 (2), S. 121–124. DOI: 10.1007/s00287-006-0063-2.

Bator, Francis M. (1958): The Anatomy of Market Failure. In: *The Quarterly Journal of Economics* 72 (3), S. 351-379. DOI: 10.2307/1882231.

Berger, Peter L.; Luckmann, Thomas (1972): Die gesellschaftliche Konstruktion der Wirklichkeit. Eine Theorie d. Wissenssoziologie. 3. Aufl. Frankfurt (am Main): S. Fischer (Conditio humana. Ergebnisse aus den Wissenschaften vom Menschen).

Betz, Andreas (2012): Breitbandversorgung im ländlichen Raum. Im Verbund zu schnellem Internet. Hg. v. Dataport (Dataport, 1/2012). Online verfügbar unter www.dataport.de/ueber-uns/publikationen/Seiten/Datareport-2012-1/2012-1-Breitband.aspx.

Beuth, Patrick (2014): Amazon Echo: Amazon hört immer zu. In: *ZEIT ONLINE*, 07.11.2014. Online verfügbar unter www.zeit.de/digital/internet/2014-11/amazon-echo-lautsprecher-spracheingaben, zuletzt geprüft am 31.08.2015.

Bitkom (Hg.) (2012a): Big Data im Praxiseinsatz – Szenarien, Beispiele, Effekte. Online verfügbar unter www.bitkom.org/Bitkom/Publikationen/Leitfaden-Big-Data-im-Praxiseinsatz-Szenarien-Beispiele-Effekte.html.

Bitkom (Hg.) (2012b): Der Staat als Gestalter der digitalen Welt – Industriepolitisches Grundsatzpapier. Online verfügbar unter www.bitkom.org/Bitkom/Publikationen/Der-Staat-als-Gestalter-der-digitalen-Welt-Industriepolitisches-Grundsatzpapier.html.

Bitkom (Hg.) (2015): Digitale Souveränität. Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa. Online verfügbar unter www.bitkom.org/Bitkom/Publikationen/Digitale-Souveraenitaet-Positionsbestimmung-und-erste-Handlungsempfehlungen-fuer-Deutschland-und-Europa.html.

Bock, Kirsten; Rost, Martin (2011): Privacy By Design und die Neuen Schutzziele. Grundsätze, Ziele und Anforderungen. In: *Datenschutz und Datensicherheit* – DuD 2011, Januar 2011 (1), S. 30–35.

BREKO (Hg.) (2016): BREKO Breitband Kompass 2016/2017, Bundesverband Breitbandkommunikation e.V. Online verfügbar unter www.brekoverband.de/fileadmin/user_upload/Breitbandkompass/BREKO_Breitband_Kompass_2016_2017.pdf.

Bridgman, Peter; Davis, Glyn (2003): What Use is a Policy Cycle? Plenty, if the Aim is Clear. In: *Australian Journal of Public Administration* 62 (3), S. 98–102. DOI: 10.1046/j.1467-8500.2003.00342.x.

Brühl, Kirsten; Pollozek, Silvan (2015), (Hg.: Zukunftsinstitut): Die neue Wir-Kultur.

BSI IT-Grundschutz 4.5 Risikostrategien wählen. Online verfügbar unter www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/Webkurs1004/4_RisikenAnalysieren/4_StrategienWaehlen/StrategienWaehlen_node.html.

BSI TR-03109, 18.03.2013: TR-03109 Technische Vorgaben für intelligente Messsysteme und deren sicherer Betrieb. Online verfügbar unter www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03109/index_htm.html.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hg.) (2014): Die Lage der IT-Sicherheit in Deutschland 2014. Online verfügbar unter www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.html.

Bundesgerichtshof (2013): Urteil des III. Zivilsenats vom 24.1.2013 – III ZR 98/12. Online verfügbar unter juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=df102f6662ffc98b64217a4b396fa79d&nr=63259&pos=0&anz=1.

Bundesministerium des Innern (Hg.) (2009): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Online verfügbar unter www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.html.

Bundesministerium für Bildung und Forschung (Hg.) (2015): Gesellschaftliche Herausforderungen – Horizont 2020. Online verfügbar unter www.horizont2020.de/einstieg-gesellschaftliche-herausforderungen.htm.

Bundesministerium für Wirtschaft und Energie (Hg.) (2015): Leitplanken Digitaler Souveränität. Papier der Fokusgruppe 1 zum Nationalen IT-Gipfel 2015. Online verfügbar unter www.bmwi.de/BMWi/Redaktion/PDF/IT-Gipfel/it-gipfel-2015-

leitplanken-digitaler-souveraenitaet,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf.

Bundesnetzagentur (26.11.2012): Bundesnetzagentur – Presse – Versorgungsauflage im 800-MHz-Bereich bundesweit erfüllt. Bonn. Online verfügbar unter www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2012/121126_Breitbandausbau-Erfuellt.html.

Bundesverfassungsgericht (2011): Bundesverfassungsgericht – Entscheidungen. Urteil des Ersten Senats vom 22. Februar 2011 – 1 BvR 699/06. Bundesverfassungsgericht; BVerfG. Online verfügbar unter www.bverfg.de/entscheidungen/rs20110222_1bvr069906.html.

Canzler, Weert; Knie, Andreas (2002): »New Mobility«? Mobilität und Verkehr als soziale Praxis. In: *Aus Politik und Zeitgeschichte. Beilage zur Wochenzeitung Das Parlament, B 45-46/2000,* 25.05.2002, S. 29–38. Online verfügbar unter www.bpb.de/apuz/25355/new-mobility-mobilitaet-und-verkehr-als-soziale-praxis.

Capurro, Rafael (2005): Zwischen Vertrauen und Angst. Über Stimmungen der Informationsgesellschaft. Deutsche Übersetzung von Susanne Ertelt und Klaus Kampst erschien in: D. Klumpp, H. Kubicek, A. Roßnagel, W. Schulz (Hrsg.): Informationelles Vertrauen für die Informationsgesellschaft. Berlin/Heidelberg: Springer 2008, 53-62. Online verfügbar unter www.capurro.de/vertrauen.html.

Davis, Kord; Patterson, Doug (2012): Ethics of big data. Sebastopol, CA: O'Reilly.

DIN ISO 26000, Januar 2011: Leitfaden zur gesellschaftlichen Verantwortung; Deutsche Norm.

DIN ISO 9001, Dezember 2008: Qualitätsmanagementsysteme – Anforderungen (ISO 9001:2008).

Dirscherl, Hans-Christian; Fogarty, Kevin (2016): Die spektakulärsten Fehlprognosen der IT-Geschichte. IDG Tech Media GmbH. Online verfügbar unter www.pcwelt.de/ratgeber/Die_spektakulaersten_Fehlprognosen_der_IT-Geschichte-6948150.html.

Duden: entgrenzen. Rechtschreibung, Bedeutung, Definition. Online verfügbar unter www.duden.de/rechtschreibung/entgrenzen.

Erbstößer, Anne-Caroline (2013): Smart City Berlin. Urbane Technologien für Metropolen. Hg. v. TSB Technologiestiftung Berlin. Online verfügbar unter www.technologiestiftung-berlin.de/fileadmin/daten/media/publikationen/140213_Studie_SmartCity.pdf.

Europäische Union (13.07.2009): Richtlinie 2009/72/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt und zur Aufhebung der Richtlinie 2003/54/EG. 2009/72/EG. Online

verfügbar unter eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:211:0055:0093:DE:PDF.

Europäische Union (07.07.2010): Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern. 2010/40/EU. Online verfügbar unter eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32010L0040&qid=1440591168935&from=EN.

Europäische Union (27.04.2016): Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). EU-DSGVO. Online verfügbar unter eur-lex.europa.eu/eli/reg/2016/679/oj.

Europäisches Parlament (2014): Science and Technology Options Assessment (STOA), Mass Surveillance. Part 1 and 2. Online verfügbar unter www.europarl.europa.eu/stoa/.

Even, Hans J. (2015): Marketing 2015: Hyperpersonalisierung auf allen Ebenen. Online verfügbar unter onlinemarketing.de/news/marketing-2015-hyperpersonalisierung-auf-allen-ebenen.

Frank, Detlef (1997): Mobilität Grundbedürfnis des Menschen. In: *Spektrum der Wissenschaft*. Online verfügbar unter www.spektrum.de/magazin/mobilitaet-grundbeduerfnis-des-menschen/823839.

Fraunhofer FOKUS (2015): Smart Cities. Center for Smart Cities. Online verfügbar unter www.ict-smart-cities-center.com/smart-cities/.

Fraunhofer Morgenstadt: Morgenstadt – City of the Future. Online verfügbar unter www.morgenstadt.de.

Fraunhofer-Institut für Integrierte Schaltungen IIS (Hg.) (2012): mp3 – Forschung, Entwicklung und Vermarktung in Deutschland. Online verfügbar unter www.mp3-history.com/content/dam/mp3history/de/documents/FraunhoferIIS_Produktbrosch%C3%BCre_mp3.pdf.

Fukuyama, Francis (1995): Trust. The social virtues and the creation of prosperity. New York: Free Press.

Gabler Wirtschaftslexikon: Definition Sharing Economy. Hg. v. Springer Gabler. Online verfügbar unter wirtschaftslexikon.gabler.de/Definition/sharing-economy.html.

Gartner (2011): Gartner Says Solving ›Big Data‹ Challenge Involves More Than Just Managing Volumes of Data. Online verfügbar unter www.gartner.com/newsroom/id/1731916.

Geiger, Christian; Lucke, Jörn von; Raffl, Celina; Große, Katharina; Ramsauer, Katharina; Jandeisek, Isabel (2013): Web 2.0 in bayerischen Kommunen. Hg. v. Innovationsstiftung Bayrische Kommune. Online verfügbar unter www.bay-innovationsstiftung.de/index.php?id=64.

Geschäftsstelle des UP KRITIS (Hg.) (2014): UP KRITIS: Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen. Grundlagen und Ziele. Online verfügbar unter www.kritis.bund.de/SubSites/Kritis/DE/Publikationen/UP_KRITIS_Fortschreibungsdokument.html.

Gesetzentwurf der Bundesregierung (2015): Entwurf eines Gesetzes zur Digitalisierung der Energiewende. Online verfügbar unter www.bmwi.de/BMWi/Redaktion/PDF/E/entwurf-eines-gesetzes-zur-digitalisierung-der-energiewende.

Horton, Graham (2015): Beispiele für Disruptive Innovation. Hg. v. Zephram. Online-verfügbar unter www.zephram.de/blog/innovation/disruptive-innovation-beispiele/.

ISO/IEC 25010, 01.03.2011: Systems and software engineering — Systems and software Quality Requirements and Evaluation, (SQuaRE) — System and software quality models, International Standard.

IT-Planungsrat – Föderales Informationsmanagement (2015). Aufbau eines föderalen Informationsmanagements. Online verfügbar unter www.it-planungsrat.de/DE/Projekte/Steuerungsprojekte/FIM/fim_node.html.

KPMG; Bitkom (Hg.) (2013): Cloud-Monitor 2013. Cloud-Computing in Deutschland – Status quo und Perspektiven. Studie. Online verfügbar unter www.bitkom.org/Bitkom/Publikationen/Cloud-Monitor-2013.html.

Lischka, Konrad (2011): Vorgefiltertes Web: Die ganze Welt ist meiner Meinung. In: *Spiegel Online,* 11.03.2011. Online verfügbar unter www.spiegel.de/netzwelt/web/vorgefiltertes-web-die-ganze-welt-ist-meiner-meinung-a-750111.html.

Lischka, Konrad (2014): Online-Fernseher: Der Spion in deinem Wohnzimmer. In: *Spiegel Online,* 25.01.2014. Online verfügbar unter www.spiegel.de/netzwelt/gadgets/labortest-online-fernseher-ueberwachen-nutzungsgewohnheiten-a-945488.html.

Luhmann, Niklas (2000): Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität. 4. Aufl. Stuttgart: Lucius und Lucius (UTB für Wissenschaft, 2185).

Maurer, Hermann; Balke, Tilo; Kappe, Frank; Kulathuramaiyer, Narayanan; Weber, Stefan; Zaka, Bilal (2007): Report on dangers and opportunities posed by large search engines, particularly Google. Graz University of Technology. Online verfügbar unter www.iicm.tugraz.at/iicm_papers/dangers_google.pdf.

Nanz, Patrizia; Fritsche, Miriam (2012): Handbuch Bürgerbeteiligung. Verfahren und Akteure, Chancen und Grenzen. Bonn: Bundeszentrale f. Politische Bildung

(Schriftenreihe der Bundeszentrale für politische Bildung, 1200). Online verfügbar unter www.bpb.de/shop/buecher/schriftenreihe/76038/handbuch-buergerbeteiligung.

O. A. (2014): Tesla Model S: Hacker-Attacke bei voller Fahrt. In: *Spiegel Online*, 23.07.2014. Online verfügbar unter www.spiegel.de/auto/aktuell/tesla-model-s-von-hackern-fremdgesteuert-a-982481.html.

O. A. (2015): Sicherheitslücke: 2,2 Millionen BMW konnten gehackt werden. In: *Spiegel Online,* 30.01.2015. Online verfügbar unter www.spiegel.de/auto/aktuell/adac-entdeckt-it-sicherheitsluecke-bei-bmw-connected-drive-a-1015819.html.

Otter, Nils; Weber, Mike (2012): Rekommunalisierung – ein Innovationstreiber im öffentlichen Sektor? In: Dennis Hilgers, Norbert Thom und Reinbert Schauer (Hg.): Public Management im Paradigmenwechsel. Staat und Verwaltung im Spannungsfeld von New Public Management, Open Government und bürokratischer Restauration. Linz: Trauner (Schriftenreihe Public & Nonprofit Management), S. 333–350.

Pariser, Eli (2012): Filter Bubble. Wie wir im Internet entmündigt werden. München: Hanser.

Rauterberg, Hanno (2014): Smart Home: Mein Zuhause ist fürsorglich und streng. In: *ZEIT ONLINE*, 31.12.2014. Online verfügbar unter www.zeit.de/2015/01/smart-home-wohnen-intelligentes-haus.

Schulz, Hajo (2015): Windows 10: Datensammelwut beherrschen. In: *heise online,* 07.08.2015. Online verfügbar unter www.heise.de/newsticker/meldung/Windows-10-Datensammelwut-beherrschen-2774941.html.

Schulzki-Haddouti, Christiane (2015): Crypto Wars 3.0: EU-Rat diskutiert Schlüsselhinterlegung. In: *heise online*, 21.01.2015. Online verfügbar
unter heise.de/-2524990.

Seemann, Michael (2014): Das Neue Spiel. Strategien für die Welt nach dem digitalen Kontrollverlust. Freiburg: orange press.

Statistisches Bundesamt (2016): Wirtschaftsrechnungen. Private Haushalte in der Informationsgesellschaft – Nutzung von Informations- und Kommunikationstechnologien 2015. Fachserie 15, Reihe 4. Wiesbaden. Online verfügbar unter www.destatis.de/DE/Publikationen/Thematisch/EinkommenKonsumLebensbedingungen/PrivateHaushalte/PrivateHaushalteIKT2150400157004.pdf?__blob=publicationFile.

Thomas, William Isaac (1928): The Methodology of Behavior Study. Chapter 13 in The Child in America: Behavior Problems and Programs. Hg. v. Alfred A. Knopf. New York. Online verfügbar unter https://brocku.ca/MeadProject/Thomas/Thomas_1928_13.html.

ULD (2007): Verkettung digitaler Identitäten. Projektnummer: PLI1563. Version 1.0. Hg. v. Marit Hansen. Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein. Kiel. Online verfügbar unter www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf.

VDI/VDE-IT (2011): Technologische und wirtschaftliche Perspektiven Deutschlands durch die Konvergenz der elektronischen Medien. Studie der VDI/VDE Innovation + Technik GmbH in Kooperation mit dem Institut für Gründung und Innovation der Universität Potsdam im Auftrag des Bundesministeriums für Wirtschaft und Technologie. Online verfügbar unter www.vdivde-it.de/publikationen/studien/.

von Hippel, Eric (1986): Lead users: a source of novel product concepts. In: *Management Science* 32 (7), S. 791–805. DOI: 10.1287/mnsc.32.7.791.

von Lucke, Jörn; Reinermann, Heinrich (2000): Speyerer Definition von Electronic Government. Online verfügbar unter 192.124.238.248/ruvii/SP-EGov.pdf.

Weitert, Christian (2014): Wettbewerbsimplikationen technologischen Wandels. Eine simulationsbasierte Untersuchung der Anpassungsfähigkeit von Unternehmen. Wiesbaden: Springer Gabler.

Wolfie, Christl (2015): Facebooks Datenauswertung: Verstecken kann sich niemand mehr. In: *Frankfurter Allgemeine Zeitung*, 28.04.2015. Online verfügbar unter www.faz.net/aktuell/feuilleton/debatten/ueberwachung/facebook-trackt-seine-nutzer-online-und-offline-13562350.html.

World Development Report 2016: Digital Dividends (2016): The World Bank. Yee, Ka-Ping (2004): Aligning security and usability. In: *IEEE Security & Privacy* 2 (5), S. 48–55. DOI: 10.1109/MSP.2004.64.

Zoche, Peter (2002): Virtuelle Mobilität: ein Phänomen mit physischen Konsequenzen? Zur Wirkung der Nutzung von Chat, Online-Banking und Online-Reiseangeboten auf das physische Mobilitätsverhalten. Berlin: Springer.

Zukunftsinstitut (Hg.) (2015): Megatrends. Online verfügbar unter www.zukunftsinstitut.de/dossier/megatrends/.

Zweck, Axel; Holtmannspötter, Dirk; Braun, Matthias; Hirt, Michael; Kimpeler, Simone; Warnke, Philine (2015): Gesellschaftliche Veränderungen 2030. Ergebnisband 1 zur Suchphase von BMBF-Foresight Zyklus II. Hg. v. Innovationsbegleitung und Innovationsberatung der VDI Technologiezentrum GmbH (Zukünftige Technologien, 100). Online verfügbar unter www.vditz.de/fileadmin/media/VDI_Band_100_C1.pdf.

Alle Links zuletzt aufgerufen am 9.11.2016

IMPRESSUM

Autoren:
Petra Hoepner, Mike Weber, Jens Tiemann, Christian Welzel, Gabriele Goldacker, Michael Stemmer, Florian Weigand, Jens Fromm, Nicole Opiela, Lutz Henckel

Gestaltung:
Reiko Kammer

Herausgeber:
Jens Fromm
Kompetenzzentrum Öffentliche IT (ÖFIT)
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin

Kontakt:
Dr. Mike Weber, Christian Welzel
Kompetenzzentrum Öffentliche IT
Telefon: +49-30-3463-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

1. Auflage Dezember 2016

ISBN: 978-3-9816025-4-8

Empfohlene Zitierweise:
Petra Hoepner et al. 2016: »Digitalisierung des Öffentlichen«
Hg. von Jens Fromm.
Berlin: Kompetenzzentrum Öffentliche IT
www.oeffentliche-it.de/publikationen

kre | 1612 (Grafiken: Fraunhofer FOKUS)