

ÖFFENTLICHE INFORMATIONSTECHNOLOGIE: ABGRENZUNG UND HANDLUNGSFELDER

Jens Fromm, Petra Hoepner, Mike Weber, Christian Welzel



IMPRESSUM

Autoren:

Jens Fromm, Petra Hoepner, Mike Weber, Christian Welzel

Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3436-7173
Telefax: +49-30-3436-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

ISBN: 978-3-9816025-0-0

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet
diese Publikation in der Deutschen Nationalbibliografie;
detaillierte bibliografische Daten sind im
Internet über <http://dnb.d-nb.de> abrufbar.
1. Auflage Juni 2013

Dieses Werk steht unter einer Creative Commons
Namensnennung 3.0 Unported (CC BY 3.0) Lizenz.
Es ist erlaubt, das Werk bzw. den Inhalt zu vervielfältigen,
zu verbreiten und öffentlich zugänglich zu machen,
Abwandlungen und Bearbeitungen des Werkes bzw.
Inhaltes anzufertigen sowie das Werk kommerziell zu nutzen.
Bedingung für die Nutzung ist die Angabe der
Namen der Autoren sowie des Herausgebers.

VORWORT

Ob für die smarte Stadt mit ihren intelligenten Stromnetzen und Gebäuden, für eine reibungslose Produktion und Logistik, für effektive Mobilität und Kommunikation jederzeit und überall – moderne Informationstechnik nimmt in nahezu allen Zukunftsfeldern wichtige Querschnittsfunktionen wahr und treibt die gesellschaftlich notwendigen Innovationen.

Ungeachtet dieser übergreifenden Anforderungen werden Forschungs- und Entwicklungsvorhaben der öffentlichen Hand weiterhin mit Bezug auf konkrete Einzelprobleme vergeben. So entstehen »Insellösungen«, die den Anforderungen an eine moderne, zukunftssichere und wirtschaftliche IT immer weniger gerecht werden. Insellösungen beeinträchtigen die dringend erforderliche Abstimmung von Steuerung und Konsolidierung der IT in Deutschland, zu der das Grundgesetz im Art. 91c explizit berechtigt. Insofern bedürfen Planungen und Beschaffungsvorhaben wie auch rechtliche Regelungen vertiefter Analysen der Gesamtinfrastruktur. Das schließt auch die Problem- und Erwartungslagen auf Seiten ihrer Nutzer mit ein.

Um dem gerecht zu werden, wird ein Konzept von öffentlicher IT benötigt, das mehr als die Hard- und Software von Behörden bezeichnet. Es schließt die Diskussion einer Vielzahl unterschiedlicher Einzelfragen ein: Beschränkt sich die Rolle der öffentlichen Hand auf die Bereitstellung der eigenen IT-Infrastruktur, kommt ihr eine Verantwortung für das Funktionieren der öffentlich zugänglichen Infrastrukturen zu oder muss sie diese sogar selbst anbieten und betreiben? Wie stark darf, wie stark soll Politik und Recht die auf Informationstechnologie basierenden Interaktionen beeinflussen und reglementieren? Welche Rollen und Funktionen erfüllt die öffentliche Hand bei der Bereitstellung und Verarbeitung von Daten?

Ziel dieses Whitepapers ist es, diese und andere Forschungsfragen aufzuwerfen und die dringend erforderliche Diskussion anzustoßen und zu strukturieren.

Die Diskussion und die mit ihr verbunden tiefgreifenden Herausforderungen bedürfen einer langfristigen Begleitung durch eine kompetente, neutrale und stark vernetzte Einrichtung. Das Kompetenzzentrum Öffentliche IT von Fraunhofer FOKUS hat

sich zum Ziel gesetzt, mit einem interdisziplinären Ansatz an der Erforschung und Entwicklung der öffentlichen IT zu arbeiten. Aktuelle Forschungsgebiete und die Expertise von Fraunhofer FOKUS bilden dafür eine Basis. Gesellschaftliche Aspekte werden dabei als integraler Bestandteil informationstechnischer Themen verstanden.

Wir freuen uns auf die dringend notwendige Diskussion.

Berlin im Juni 2013



Jens Fromm

UNTER ÖFFENTLICHER IT VERSTEHT MAN
INFORMATIONSTECHNOLOGIEN, DIE IN EINEM ÖFFENTLICHEN
RAUM DURCH DIE GESAMTGESELLSCHAFTLICHE
RELEVANZ UNTER BESONDERER BERÜCKSICHTIGUNG
DER STAATLICHEN VERANTWORTUNG STEHEN.

INHALTSVERZEICHNIS

Vorwort	3
Inhaltsverzeichnis	4
1 Öffentliche IT – eine Eingrenzung	5
1.1 Öffentlicher Raum	5
1.2 Begriffliche Annäherung an öffentliche IT	5
1.3 Schaffung und Gewährleistung öffentlicher Räume	6
1.4 Eingrenzung und Entgrenzung des Begriffs öffentliche IT	7
2 Anforderungen an die öffentliche Hand	8
2.1 Infrastrukturbereitstellung und -betrieb	8
2.2 Anspruchsvolle Bedarfe	9
2.3 Selbstregulierung im Schatten des Gesetzes	10
3 Beispielhafte Handlungsfelder	13
3.1 Open Government	13
3.2 Smart Energy	13
3.3 Mobilität und intelligente Verkehrs- und Transportsysteme	14
3.4 Vertrauenswürdige Identitäten	15
4 Zusammenfassende Thesen	17

1. ÖFFENTLICHE IT – EINE EINGRENZUNG

Informationstechnologien (IT) spielen im öffentlichen Leben eine wachsende Rolle. Nicht nur öffentliche und privatwirtschaftliche Leistungserstellung, auch die Lebenswelten der Bürgerinnen und Bürger werden durch die vermehrte Verwendung von Informationstechnologien nachhaltig beeinflusst. Welche Rolle der öffentlichen Hand in diesem Zusammenhang zukommt, ist eine nicht abschließend geklärte und in der kurzen Technologiesgeschichte durchaus unterschiedlich beantwortete Frage. Bevor sich dieser Frage gewidmet werden kann, bietet dieses Kapitel zunächst eine Auseinandersetzung mit dem Konzept von »öffentlicher IT«.

1.1 ÖFFENTLICHER RAUM

Die Auseinandersetzung mit öffentlicher IT geht von der Betrachtung des öffentlichen Raumes und der diesen konstituierenden gesellschaftlichen Teilsystemen aus (vgl. Abbildung 1). Die Konzeption des öffentlichen Raumes orientiert sich dabei weniger an geographischen Räumen oder an Eigentumsverhältnissen von Infrastrukturen, sondern berücksichtigt vielmehr öffentliche Funktionen und staatliche Verantwortung. Die höchstrichterliche Feststellung, dass etwa Flughäfen als öffentliche Räume zu verstehen sind und dort entsprechend Grundrechte unmittelbar Anwendung finden, spiegelt diese Sichtweise.¹

Eine solche Betrachtung unterscheidet in starker Vereinfachung nur die gesellschaftlichen Subsysteme der Wirtschaft, der öffentlichen Hand sowie der Zivilgesellschaft. Diese gesellschaftlichen Subsysteme lassen sich als auf sich selbst bezogene Kommunikationssysteme verstehen. Die Subsystemgrenzen ergeben sich dabei aus der Referenz, auf die sich die jeweilige Kommunikation bezieht. In Anlehnung an Luhmann² ließe sich beispielsweise konstatieren, dass die öffentliche Hand auf Rechtmäßigkeit und Gemeinwohl rekurriert. Diese beispielhafte Referenz zeigt bereits, dass sich Kommunikationen nicht vollständig eindeutig voneinander abgrenzen lassen. Gleiches gilt für die diese Subsysteme vornehmlich konstituierenden Akteursgruppen. Dessen ungeachtet lassen sich spezifische, gegen andere Subsysteme abgeschlossene Informationsbestände ausfindig machen. Staatsgeheimnisse, intellektuelle Eigentumsrechte und Privatheit mögen als Schlagworte zur Veranschaulichung dienen. Charakteristisch und für zeitgemäße Wertschöpfungsketten bedeutsamer werden jedoch geteilte Informationen, die den geschlossenen Bereich der jeweiligen

Einheit verlassen. Diese geteilten Informationen konstituieren den öffentlichen Raum. Der öffentliche Raum wird hier als virtueller Raum gefasst, der durch geteilte Informationen, also durch Formen von gesellschaftlich relevanter Kommunikation entsteht.

1.2 BEGRIFFLICHE ANNÄHERUNG AN ÖFFENTLICHE IT

Eine begriffliche Annäherung kann am ersten Teil des Begriffs-paares ansetzen. »Öffentlich« bedeutet zunächst, dass das dadurch Bezeichnete prinzipiell frei zugänglich ist. 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 öffentlich mit staatlich, respektive quasistaatlich assoziiert. Im Gegensatz dazu betonen anglo-amerikanische Sprachgewohnheiten eher die private und privatwirtschaftliche Seite. »Going public« bezeichnet dort einen Börsengang und eben keine politische Kampagne.

»Öffentlich bezeichnet eine möglichst leichte Zugänglichkeit für möglichst breite Kreise Interessierter.«

»Öffentlich« bewegt sich demnach auch 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 es 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 für möglichst breite Kreise Interessierter aus.

Im Gegensatz zu öffentlicher IT lässt sich private IT demnach durch die Anwendung von Informationstechnologie in einem abgegrenzten und dadurch privaten Raum charakterisieren.

Abbildung 1: Öffentlicher Raum und ihn konstituierende gesellschaftliche Subsysteme



Das Bild eines nicht verbundenen Privatrechners verdeutlicht unmittelbar den beträchtlichen Wandel, der sich hier vollzogen hat. Die große Mehrzahl der privaten Haushalte ist breitbandig an das Internet angebunden.³ 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 Datenübermittlung von Personen erwarten. Dabei bedeutet schon die Anbindung eines zuvor isoliert betriebenen Rechners an das Internet zum Zweck des rein passiven Seitenaufrufs einen Eingriff in diesen öffentlichen Raum. Für die Optimierung eines Webangebots gezählt, hat dieser Seitenaufwurf Auswirkungen auf spätere Onlineangebote.

Ähnlich lässt sich für die staatliche IT argumentieren. Wenn ein Aspekt von E-Government die Verlängerung zuvor verwaltungsinterner Prozessketten nach außen ist, dann beeinflussen organisationsinterne Abläufe bei zunehmendem Einsatz von E-Government ihre Umwelt. Dabei gilt es festzuhalten, dass die zunehmende Verschmelzung von staatlicher IT und öffentlichem Raum eben nicht aus der sprachlichen Analogie zwischen staatlich und öffentlich erwächst. Vielmehr bietet staatliche Informationstechnologie zur privaten vergleichbare Möglichkeiten der Abschottung. Staatlich bezeichnet in diesem Sinne tendenziell einen Gegenpol zu öffentlich und nicht dessen Spezialfall. Bezogen auf Informationstechnologie muss also eine Differenz im Verständnis zu anderen Definitionen von öffentlich konstatiert werden.

Informationstechnologie 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, so dass sich der Unterschied zwischen Systemen der Informations- und der Kommunikationstechnologie weiter verringert. Die

wachsende Durchdringung anderer Technologiefelder führt dabei zu einem steten Bedeutungszuwachs der Informationstechnologien. So lässt sich eine weitgehende Konvergenz zwischen Informations- und Kommunikationstechnologien bereits heute 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 weiter entwickelt. Immer mehr Bereiche aus Wirtschaft und Gesellschaft greifen auf Informationstechnologien zurück. IT kommt damit wie kaum einer anderen Technologie eine Querschnittsfunktion zu, die insbesondere für die Generierung von Innovationen von überragender Bedeutung ist. Zudem erweist sich öffentliche IT als zunehmend bedeutsamer Träger gesellschaftlich relevanter Kommunikation.

1.3 SCHAFFUNG UND GEWÄHRLEISTUNG ÖFFENTLICHER RÄUME

Die überragende Bedeutung digitaler IT-Netzinfrastrukturen für Wirtschaft und gesellschaftliche Teilhabe macht aus ihr eine als kritisch angesehene Infrastruktur. Ein Ausfall des Kommunikationsnetzes beispielsweise kann mit volkswirtschaftlichen, politischen und persönlichen Schäden verbunden sein, die durchaus mit denen eines Ausfalls des Stromnetzes vergleichbar sind. Die Gewährleistung des Funktionierens solcher Infrastrukturen selbst wird damit als Staatsaufgabe wahrgenommen, die es durch geeignete technische und organisatorische Unterstützung 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 jedem Fall wird der Staat in der Verantwortung gesehen zu gewährleisten, dass die Infrastruktur betrieben und für alle Interessierten in geeigneter Weise nutzbar gemacht wird.

AN DIE ÖFFENTLICHE HAND WIRD DIE ANFORDERUNG
GERICHTET, IT-GESTÜTZTE ÖFFENTLICHE RÄUME ZU
SCHAFFEN, ZU SCHÜTZEN UND IHR
GESAMTGESELLSCHAFTLICHES
FUNKTIONIEREN SICHERZUSTELLEN.

Die staatliche Verantwortung für das Funktionieren öffentlicher, digitaler Räume wird von vielen Seiten betont. So sieht beispielsweise auch der Bitkom den »Staat als Gestalter der digitalen Welt«⁴ in der Pflicht und bewertet damit die Chancen für eine rein marktwirtschaftliche Selbstorganisation als gering. Der Ruf eines Branchenverbandes nach mehr Staat fügt sich in die lange Tradition der Diskussion um die Art der Leistungserstellung für Bereiche öffentlicher Daseinsvorsorge. In historischer Perspektive unterlag beispielsweise die Art der Leistungserstellung in der Elektrizitätswirtschaft beträchtlichen Schwankungen.⁵ Dem initialen Aufbau der Stromversorgung durch privatwirtschaftliche Akteure folgte eine Phase der faktischen Verstaatlichung und Kommunalisierung. Diese im Zuge der europäischen Marktliberalisierungen aufgebrochenen Strukturen scheinen sich aktuell auf lokaler Ebene erneut in Richtung Rekommunalisierung zu verändern. Die Gewährleistungsverantwortung des Staates für die Bereitstellung dieser Dienstleistung von allgemeinem öffentlichen Interesse erwies sich in diesem Prozess als ein Treiber für die große Bedeutung der öffentlichen Einflussnahme.

»Öffentliche IT erweist sich als zunehmend bedeutsamer Träger gesellschaftlich relevanter Kommunikation.«

Der sich inzwischen abzeichnende Trend eines stärkeren staatlichen Engagements für öffentliche IT-Infrastruktur speist sich aus drei Legitimationsquellen: (1) aus der wachsenden Bedeutung für Wirtschaft und Gesellschaft, (2) aus der Übertragung gesellschaftlicher Phänomene auf virtuelle Räume samt des sich daraus ergebenden Regulierungsbedarfs und (3) aus der Notwendigkeit smarterer (effizienter, interoperabler, intelligenter, skalierbarer) öffentlicher Netze (Kommunikation, Strom, etc.). Aus diesem Dreiklang ergibt sich eine der Gewährleistungsverantwortung analoge Anforderung, die von verschiedenen

gesellschaftlichen Gruppen an den Staat und an die öffentliche Hand insgesamt herangetragen wird, IT-gestützte öffentliche Räume zu schaffen, zu schützen und ihr gesamtgesellschaftliches Funktionieren sicherzustellen. Auf welche konkreten Bereiche sich eine solche Gewährleistungsverantwortung in welcher Intensität erstreckt, erstrecken sollte und zukünftig erstrecken wird, sind offene, empirisch und normativ zu beantwortende Fragen.

1.4 EINGRENZUNG UND ENTGRENZUNG DES BEGRIFFS ÖFFENTLICHE IT

Die Überlegungen erlauben eine Eingrenzung des Begriffs öffentliche IT anhand von vier Merkmalen. Für die Begriffsfassung ist es wesentlich, ob:

- (1) ein öffentliches, also prinzipiell zugängliches, IT-gestütztes Kommunikationsnetz zu Grunde liegt oder IT-Systeme von staatlichen, kommunalen oder anderen öffentlichen Einrichtungen involviert sind;
- (2) Dienstleistungen von allgemeinem öffentlichen Interesse (Daseinsvorsorge) angeboten werden;
- (3) reale Lebenswelten gespiegelt oder substituiert werden;
- (4) mögliche Regulierungserfordernisse (Datenschutz, ggf. auch Strafrecht) zu diskutieren sind.

Die Eingrenzung unterliegt dabei einer fortlaufenden Veränderung durch lebhaftere gesellschaftliche Diskurse. Die Bedeutung der Merkmale, die Relation der Merkmale untereinander und sogar die Merkmale selbst unterliegen so einem steten Wandel. Die Eingrenzung kann absehbar nur temporär sein und wird durch gesellschaftliche Entwicklungen immer wieder auf ein Neues entgrenzt.

2. ANFORDERUNGEN AN DIE ÖFFENTLICHE HAND

So vielfältig die Ausprägungen öffentlicher IT sind, so mannigfaltige Anforderungen lassen sich an sie richten. Diese Anforderungen sind in hohem Maße von der spezifischen Domäne abhängig. Hier werden generelle Anforderungen identifiziert, die quer zu den einzelnen Handlungsfeldern liegen und entsprechend für die Themenstellung als konstitutiv gelten können. Die Anforderungen werden an die öffentliche Hand gerichtet. 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.

2.1 INFRASTRUKTURBEREITSTELLUNG UND -BETRIEB

Allen hier herangezogenen Sichtweisen auf öffentliche IT ist gemein, dass sie eine vernetzte Infrastruktur für Datenspeicherung und -verarbeitung voraussetzen. Unabhängig von der auf ihr aufsetzenden Komplexität bedarf es zunächst einer solchen Infrastruktur.

Weite Teile der öffentlich zugänglichen IT-Netzinfrastrukturen 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 führten zu einer Dominanz privatwirtschaftlicher Bereitstellung. Dies hat sich sowohl national als auch global für die Verbindung von Metropolen bewährt, wie die kurzen Innovationszyklen in der digital vermittelten Kommunikation eindrucksvoll zeigen. Es kommt hierbei jedoch zu beträchtlichen internationalen und interregionalen Ungleichgewichten. So ermöglichen dichte globale Kommunikationsnetze zwischen den industriellen Ballungszentren einen intensiven Datenaustausch bei gleichzeitiger Konkurrenz konvergierender Übertragungstechnologien vor Ort, während sowohl ganze Staaten als auch dünn besiedelte ländliche Räume in Deutschland nicht von breitbandigen Zugängen profitieren können.

Der Bedeutungszuwachs des breitbandigen Netzzugangs, der jüngst etwa durch das Grundsatzurteil des BGH zum Schadensersatzanspruch bei dessen Ausfall unterstrichen wurde,⁶ legt eine Verantwortung der öffentlichen Hand für das Funktionieren

nahe, wie sie in 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 jedoch staatlichen und kommunalen Handlungsbedarf auf, 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.⁷ Erst ein Zweckverband zum Aufbau eines breitbandigen Kommunikationsnetzes konnte durch Selbstverpflichtung der Kommunen und bei Anpassung der technischen Lösungen die Versorgung sicherstellen. Die Versorgung 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. 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, umfasst aber auch eine Versorgungsaufgabe für die Breitbandversorgung.⁸ Diese Auflage besagt, dass zunächst schlechter versorgte Gemeinden mit Breitbandzugängen versorgt werden müssen, bevor auch der für Mobilfunkprovider technisch und wirtschaftlich interessante 800-MHz-Bereich in Ballungsgebieten freizügig genutzt werden kann. Interessant ist dabei, dass die Breitbandversorgung technologieneutral betrachtet wird. Die anzuschließenden Gemeinden, also insbesondere unterversorgte Kleingemeinden, können durch kabelgebundene Lösungen versorgt werden.

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 Kommunikati-

DIE STAATLICHE UND KOMMUNALE ROLLE
BEI DER GEWÄHRLEISTUNG DER
BREITBANDVERSORGUNG GEHT ÜBER DIE
BEREITSTELLUNG FINANZIELLER
MITTEL HINAUS.

onsnetzen berührt demnach Fragen der Gleichheit der Lebensverhältnisse und entscheidet über die Verteilung von Lebenschancen und gesellschaftlicher Teilhabe mit. Für deren Nutzung ist der technische Zugang eine notwendige, nicht jedoch hinreichende Bedingung. Als Analogie lässt sich hier die Verfügbarkeit eines Girokontos für jedermann heranziehen, die durch die staatliche Stützung des Bankensektors alleine noch nicht gewährleistet werden kann. Bezogen auf öffentliche IT bedarf es zur Sicherstellung gesellschaftlicher Teilhabe nicht nur des Zugangs zur Infrastruktur, sondern zugleich darauf aufsetzender Dienste sowie der entsprechenden Kompetenzen. In diesem Sinne tangiert der Ausbau breitbandiger Netzinfrastruktur zugleich regionalökonomische, demographische und bildungspolitische Aspekte.

2.2 ANSPRUCHSVOLLE BEDARFE

Ungeachtet der Dominanz privatwirtschaftlicher Leistungserstellung halten Staat, Kommunen und andere öffentliche Einrichtungen eine Vielzahl von IT-Infrastrukturbausteinen und Diensten vor. Einigen dieser Bausteine der IT von öffentlichen Einrichtungen kommt mitunter eine gewichtige Funktion für die Entwicklung und Verbreitung von Innovationen zu. Beispielsweise ist hier an die phasenweise beträchtliche Bedeutung der Wissenschaft für heute alltägliche Internetstandards zu denken, die etwa die Entstehung des World Wide Webs ermöglichten. Aus solchen Mechanismen ergeben sich mindestens drei Aspekte, die hier Berücksichtigung finden müssen: Effektivität

»Ungeachtet der Dominanz privatwirtschaftlicher Leistungserstellung halten öffentliche Einrichtungen eine Vielzahl von IT-Infrastrukturbausteinen und Diensten vor.«

und Effizienz des Betriebs eigener Kommunikationsnetze und Dienste, die sich daraus ergebende Notwendigkeit der ebenen- und bereichsübergreifenden Zusammenarbeit sowie der Rolle der öffentlichen Hand als direkter und indirekter Impulsgeber für die Entstehung und Verbreitung von Innovationen.

Die Frage nach effektiven und effizienten öffentlichen Kommunikationsnetzen und Diensten verweist auf einschlägige E-Government-Diskussionen. Öffentliche Einrichtungen verfügen oftmals über ausgereifte IT-Lösungen, die für ein spezifisches Anforderungsprofil entwickelt wurden, das sich aus ihrer öffentlichen Aufgabenstellung ergibt. Zu denken ist hier beispielsweise an die IT-Systeme der Sozialversicherungsträger, bei denen gleich eine Vielzahl von überaus anspruchsvollen Anforderungen kumuliert: enorme Datenmengen, die rechtssicher über große Zeiträume gespeichert und bearbeitet werden müssen und an die höchste Anforderungen hinsichtlich Datensicherheit, Datenintegrität und Datenschutz gerichtet werden. Diese IT-Systeme wurden oftmals maßgeschneidert für die spezifischen Bedarfe der jeweiligen Einrichtung 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 der öffentlichen Hand für die öffentliche IT nutzbar gemacht werden, kommt es gerade auf diese Öffnung an. Dabei birgt die Öffnung prinzipiell Effizienzpotenziale, die es schon aufgrund des Wirtschaftlichkeitsgrundsatzes im Haushaltsrecht zu heben 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 beeinflussen. Solche etwa kommunale Einzellösungen stehen nicht nur dem durch Cloud-Infrastrukturen ermöglichten Trend zur Industrialisierung der IT-Branche entgegen, sie verweisen 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 wird es beispielsweise Aufgabe des Projektes Föderales Informationsmanagement (FIM)⁹ sein, 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. Wie umfänglich die zu koordinierenden Infrastrukturelemente sind, verdeutlicht die Diskussion über den Schutz kritischer Infrastrukturen.¹⁰ 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 einer intensiven Zusammenarbeit, Abstimmung und Information unterschiedlichster Akteursgruppen. Wirtschaft und Verwaltung müssen ebenso Berücksichtigung finden wie Wissenschaft und Forschung, die Öffentlichkeit (Bevölkerung, Medien) und internationale und supranationale Einrichtungen. Die intensive Kooperation muss also 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 Informationstechnologie staatlicher, kommunaler und anderer öffentlicher Einrichtungen führt zum dritten hier zu behandelnden Aspekt. Zur Erfüllung der anspruchsvollen öffentlichen Aufgaben muss der Staat sicherstellen, dass die erforderliche IT zur Verfügung steht. Die aktive Beeinflussung bestehender Infrastrukturen, die Förderung nationaler IT-Forschung und der Einkauf zeitgemä-

»Die intensive Kooperation von Wirtschaft, Verwaltung, Wissenschaft und Zivilgesellschaft muss über Gebietskörperschafts- und Zuständigkeitsgrenzen hinweg aufgebaut und gepflegt werden.«

ßer 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 öffentlicher Dienstleistungen und der gleichzeitig großen Bedeutung öffentlicher Einrichtungen für die IT-Branche ergeben sich vielfältige Gestaltungsmöglichkeiten. Oftmals tritt der Staat als »Lead User«¹¹ auf, der anspruchsvolle Lösungen als Erster zum Einsatz bringen muss oder aufgrund politischer Programmatiken einen solchen Einsatz anstrebt. In der Summe ergeben sich dadurch in der Informationstechnologie Gestaltungsmöglichkeiten für die öffentliche Hand, wie sie in kaum einem anderen Technologiefeld und seiner korrespondierenden Branche gegeben sind. Aus dieser Gestaltungsmacht folgt zugleich eine Verantwortung der öffentlichen Hand.

2.3 SELBSTREGULIERUNG IM SCHATTEN DES GESETZES

Die ersten beiden Unterkapitel orientieren sich an Anforderungen, die an öffentliche Einrichtungen gerichtet werden können. Diesen kommt zwar eine wichtige Funktion bei der Behandlung des Phänomens öffentliche IT zu, insgesamt dominiert allerdings die privatwirtschaftlich betriebene IT, die dabei öffentliche Funktionen wahrnimmt. Dies erhöht die Anforderungen an die Regulierung, lassen sich gesellschaftliche Vorstellungen doch nicht ohne Weiteres in einer gegebenen privatwirtschaftlichen IT-Infrastruktur implementieren.

IN DER IT ERGEBEN SICH FÜR DIE
ÖFFENTLICHE HAND VIELFÄLTIGE
GESTALTUNGSMÖGLICHKEITEN, DIE ES
STRATEGISCH ZU NUTZEN GILT.

Die umfänglichen Regulierungsbedarfe beginnen bei der Regelung grundlegender Fragestellungen des gemeinsamen Miteinanders, die sich von denjenigen in der Alltagswelt durch die Art der Vermittlung, oftmals jedoch nicht substantiell unterscheiden. Das Austarieren von Anonymität und Identifizierbarkeit im digitalen Raum liefert hierfür ein aktuelles 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. Hierzu müssen geeignete technische Lösungen entwickelt und vorgehalten werden.

Wie in den 14 Thesen zur Netzpolitik¹² festgehalten, geht es bei der Regulierung in erster Linie um die Schärfung des Bewusstseins für gemeinsame Werte. Auf einem solchen Fundus gemeinsam geteilter Werte gründet jedes Gemeinwesen. Diese mögen durch die vermehrt digitale Abbildung erweiterungs- und partiell anpassungsbedürftig sein, letztlich bilden jedoch auch in digitalen Netzwerken solche gemeinsamen Handlungsnormen die Basis für das soziale Miteinander, die gegenseitigen Respekt und Rücksichtnahme einfordern. Eines solchen Umgangs bedarf es im persönlichen, im politischen und im wirtschaftlichen Bereich. Die Stärkung von Selbstbestimmung und Eigenverantwortung stößt dann an ihre Grenzen, wenn Freiheitsrechte Dritter berührt werden und ein fairer Interessenausgleich zwischen den Beteiligten nicht erfolgen kann. Erst dann greift die für die Bedarfe digitaler Welten angepasste Rechtsordnung, wobei es möglicherweise bewährter oder auch tiefgreifender Eingriffsrechte bedarf.

Angesichts der Komplexität der Fragestellungen dürfen die Möglichkeiten staatlicher Intervention nicht überschätzt werden. Vielmehr müssen die Grenzen des Tolerierbaren und die Notwendigkeiten staatlicher Eingriffe immer wieder neu bestimmt werden. So bietet die staatliche Regulierung von Trägern ebenso wünschenswerter, wie noch fehlender oder bis dato ungenutzter Funktionen nicht notwendig die effektivste

Form der Intervention. Insbesondere hinsichtlich Effizienzkriterien kann die gesetzliche Rahmung mit Nachteilen für die Beteiligten. Die Komplexität der Rahmenbedingungen spricht dafür, dass es sich um ein klassisches Anwendungsgebiet von Mechanismen der Selbstregulierung handelt. Vergleichbar mit technischen Fragestellungen verfügen die in digitalen Räumen aktiven Akteure über einen mitunter beträchtlichen Wissensvorsprung gegenüber Regulierern. Bei technischen Fragestellungen wird diesen Wissensasymmetrien durch die strukturierte Selbstregulierung unter Hinzuziehung des jeweils relevanten Sachverstandes begegnet. Erst wenn diese etwa in Normungsorganisationen geleistete Arbeit nicht die gesellschaftlich gewünschten Ergebnisse zeitigt, greift die staatliche Regulierung ein. Alleine die Möglichkeit der staatlichen Intervention, die im Zweifel für die Beteiligten mit Nachteilen und in diesem Sinne mit gesamtgesellschaftlichen Ineffizienzen verbunden ist, wirkt auf die an der Selbstregulierung beteiligten Akteure disziplinierend.

Kulturell geprägte Unterschiede in der Abgrenzung, welche Bereiche einer direkten staatlichen Kontrolle unterliegen müssen und welche Bereiche für eher weiche Formen der Kontextsteuerung und Selbstregulierung zugänglich sind, bleiben dabei bestehen. Die Notwendigkeit zur internationalen Koordination steigert so die Komplexität der Bestimmung von Regulierungsanforderungen und unterstreicht die Bedeutung von Subsidiarität und Selbstregulierung. Welche Form der Selbstregulierung angemessen ist, hängt auch von dem konkreten Regulierungsbedarf ab. Zwischen marktformiger Selbststeuerung und direkter staatlicher Intervention spannt sich ein

»Selbstregulierung kann nur funktionieren, wenn sie nicht alternativlos ist – und dazu braucht der Staat umfassende Fachkenntnisse.«

DAS KONZEPT DER ÖFFENTLICHEN IT BEDARF
EINER SCHÄRFUNG DES BEWUSSTSEINS FÜR
GEMEINSAME WERTE IM VIRTUELLEN
ÖFFENTLICHEN RAUM.

breites Spektrum auf, in dem von den Regulierten getragene Agenturen eine mögliche Form der Institutionalisierung markieren.

Selbstregulierung im »Schatten des Gesetzes«¹³ bietet somit das Potenzial, die durch die Digitalisierung sozialer Beziehungen neu entstandenen Regelungsbedarfe zu decken. Dies bedeutet jedoch keinesfalls die Untätigkeit des Staates. Jenseits der Rahmgebungsfunktion und der bereits angeführten Notwendigkeit zur Entwicklung und Bereitstellung neuer Technologien muss die direkte Regulierung und ordnungsrechtliche Umsetzung eine realistische, wenn auch nach Möglichkeit nicht wahrzunehmende Option bleiben. Um glaubhaft zu machen, die Regulierung in nahezu beliebige Detailtiefen staatlich ausführen zu können, bedarf es neben eingehender inter- und supranationaler Zusammenarbeit insbesondere einer hinreichenden Expertise, um die Wissensasymmetrien zwischen Regulierer und Regulierten nicht zu groß werden zu lassen. Selbstregulierung kann nur funktionieren, wenn sie nicht alternativlos ist – und dazu braucht der Staat umfassende Fachkenntnisse.

3. BEISPIELHAFTE HANDLUNGSFELDER

Zur Veranschaulichung werden hier einige Handlungsfelder aufgezeigt, die für Fragen öffentlicher IT von besonderer Relevanz sind. Die Breite der Thematik bringt es mit sich, dass die Handlungsfelder 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 Felder – sondern skizzieren vielmehr relevante Einzelaspekte. Die Auswahl der hier dargestellten Handlungsfelder richtet sich am Kriterium aus, eine möglichst breite Repräsentanz des öffentlichen Raumes zu gewährleisten (vgl. Abbildung 2). Gewählt wurde je ein Themenbereich, der sich an der Grenze zwischen zwei gesellschaftlichen Subsystemen bewegt sowie der übergreifend relevante Aspekt vertrauenswürdiger Identitäten.

3.1 OPEN GOVERNMENT

Mit sozialer Software und dem Web 2.0 wurden neue Wege für die menschliche Kommunikation und die Zusammenarbeit im Internet beschritten. Soziale Netzwerke entstanden, die private Kontakte in einer neuen Dimension erlauben. Die Nutzung dieser neuen Technologien von Politik und Verwaltung führt zu den Leitgedanken des Open Government:¹⁴

- Transparenz: Offenheit staatlichen und kommunalen Handelns;
- Partizipation: Mitwirkung von Bürgern und Wirtschaft bei staatlichen und kommunalen Entscheidungsprozessen;
- Kooperation: Zusammenarbeit von staatlichen und kommunalen Stellen mit Bürgern und Wirtschaft.

Von den Leitgedanken des Open Government wird bisher vor allem die Forderung nach Transparenz realisiert, indem staatliche Stellen offene Daten zur Weiterverwendung durch Dritte strukturiert bereitstellen.¹⁵

»Durch Open Government können neue öffentliche Räume etwa im Bereich der politischen Partizipation geschaffen werden.«

Beispiele hierfür sind:

- GovData (govdata.de): Datenportal für Deutschland mit zentralem Zugang zu Verwaltungsdaten aus Bund, Ländern und Kommunen;
- GovApps (govapps.de): Apps mit regionalem Bezug und Anzeige der Datenschutzzeigenschaften einer App anhand von Symbolen;
- Berlin Open Data (daten.berlin.de): Berliner Open-Data-Portal;
- Datenportal der Europäischen Kommission (open-data.europa.eu);
- Hamburgisches Transparenzgesetz: umfassendes Informationsrecht mit Auskunfts- und Veröffentlichungspflicht.

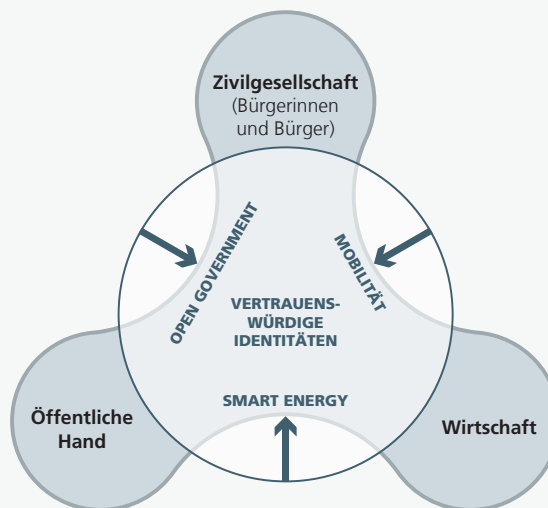
Durch die EU-Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors aus dem Jahr 2003¹⁶ (»PSI-Richtlinie«)¹⁷ wurde der allgemeine Rechtsrahmen auf europäischer Ebene festgelegt und im Jahr 2006 in Deutschland mit dem Informationsweiterverwendungsgesetz umgesetzt. Ein politisches und administratives Handeln im Sinne von Open Government verlangt jedoch mehr als offene Daten. Mit Bürgerorientierung und Teilhabe sollen gesellschaftliche Bedürfnisse und Anforderungen erkannt und Lösungen gefunden werden. Neue verwaltungs- und organisationsübergreifende Prozessketten müssen auf Basis öffentlicher IT entstehen und in die vorhandenen Abläufe integriert werden. So können durch Open Government neue öffentliche Räume etwa im Bereich der politischen Partizipation geschaffen werden.

3.2 SMART ENERGY

Die durch die Energiewende politisch priorisierten Veränderungen in der Energieversorgung erfordern neuartige Systeme zum dezentralen Erzeugen, Verteilen, Speichern und zur effizienten Verwendung von Energie. Die Einführung sogenannter Smart-Meter-Systeme zur Messung und Übermittlung des Verbrauchs hat bereits begonnen. Bis zum Jahr 2020 sollen laut einer EU-Richtlinie¹⁸ mindestens 80 % des EU-Marktes mit solchen Geräten ausgestattet werden.

Von der Stromproduktion bis zum Endgerät sollen langfristig alle relevanten Netzknoten in ein intelligentes Stromnetz (Smart Grid) integriert werden. Smart Meter erfassen die dafür benötigten Messdaten über Verbrauch und Produktion. Die Werte

Abbildung 2: Verortung der betrachteten Handlungsfelder im öffentlichen Raum



werden über verschiedene Kommunikationsschnittstellen zur weiteren Verarbeitung bereitgestellt. Diese Systeme sind ein erster Schritt zu identitätsbasierten Messsystemen für Verbrauchsdaten im Haushalt von Gas, Wasser, Elektrizität und Fernwärme. Gemeinsam sind diesen Systemen Herausforderungen an eine sichere Infrastruktur, personalisierte Objekte, Schutz persönlicher Daten sowie Anwendungen, die die Objekte des häuslichen Umfelds verbinden. Die Technische Richtlinie des BSI »Smart Energy«¹⁹ beschreibt die Anforderungen an die Funktionalität, Interoperabilität und Sicherheit, die die Einzelkomponenten in einem Smart-Meter-System erfüllen müssen sowie die Anforderungen zur Prüfung dieser Eigenschaften.

Beispiele für neue Dienste basierend auf intelligenten Netzen sind:

- IT-basiertes Energiesparen, zum Beispiel Elektrofahrzeuge dann laden zu lassen, wenn gerade viel Energie zur Verfügung steht oder Verbrauchsgeräte zu bestimmten Tageszeiten einzuschalten;
- Variable Stromtarife für ein Zusammenspiel zwischen Angebot und Nachfrage, d.h. Lastspitzen ebenso wie zu geringe Verbräuche steuern;
- Kostentransparenz für Verbraucher.

Smart Meter sind ein Baustein für die Stadt der Zukunft (Smart City),²⁰ in der Technologien und neue Verbünde zusammenwir-

»Die gesellschaftlichen Anforderungen an die zukünftige Energieversorgung erfordern neuartige Systeme zum dezentralen Erzeugen, Verteilen, Speichern und zur effizienten Verwendung von Energie.«

ken. Die Möglichkeiten, Umgebungs-, Last- oder Zustandsinformationen zu erfassen, bedarfsgerecht zu analysieren, auszuwerten und zeitnah zur Verfügung zu stellen, erlauben es, Nutzungssituationen transparent zu gestalten und so die Infrastrukturen effizienter zu nutzen. Erforderlich sind dafür unter anderem der Ausbau von Sensornetzen, Maschine-zu-Maschine (M2M) Kommunikationsnetze und Mobilkommunikation. Energie, Raum, Geld und Zeit sollen in Smart Cities basierend auf aktuellen Bedürfnissen dynamisch eingesetzt werden, um die Ressourceneffizienz nachhaltig zu steigern. Daher sind die IT-Infrastrukturen der Smarten City sinnvoll vernetzt, um Daten über Status, Nachfragen und Kapazitäten untereinander auszutauschen und nutzen zu können. Interoperabilität dieser verschiedenen Infrastrukturen ist eine wesentliche Voraussetzung hierfür.

3.3 MOBILITÄT UND INTELLIGENTE VERKEHRS- UND TRANSPORTSYSTEME

Sicher, umweltverträglich und effizient sollen die Verkehrs- und Transportsysteme in Zukunft funktionieren, um den Herausforderungen an Mobilität gerecht zu werden. In der EU-Richtlinie 2010/40/EU²¹ 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«.

Die Forschung und Entwicklung befasst sich in diesem Umfeld mit vielfältigen technischen Neuerungen, die auf IT basieren, innerhalb des Fahrzeugs, zwischen Fahrzeugen, zwischen Fahrzeugen und der Verkehrsinfrastruktur und zwischen Verkehrs- und anderen Infrastrukturen.

DIE IT-INFRASTRUKTUREN DER SMARTEN

CITY SIND SINNVOLL VERNETZT –

INTEROPERABILITÄT DIESER VERSCHIEDENEN

INFRASTRUKTUREN IST EINE WESENTLICHE

VORAUSSETZUNG HIERFÜR.

»Verkehrsinfrastrukturen müssen mit anderen Informationsverbänden zusammenwirken, weshalb übergreifende Standards und Architekturen erforderlich sind.«

Beispiele hierfür sind:

- Neuartige Mobilitätskonzepte mit der smarten Verknüpfung unterschiedlicher Verkehrsträger und neuer Nutzungsformen (z.B. Kurzzeit-Carsharing), wie sie aktuell im Rahmen der Initiative »Schaufenster Elektromobilität« entwickelt werden;
- Schaltung einer »grünen Welle« bei Bedarf für Einsatzfahrzeuge von Krankenhaus, Polizei oder Feuerwehr;
- E-Call-System (emergency call oder automatischer Notruf), das im Falle eines Autounfalls automatisch vom auslösenden Airbagsensor über das Mobilfunknetz die örtlich zuständige Notrufstelle informiert;
- Erkennung und Steuerung von flexiblen Umweltzonen entsprechend der aktuellen Schadstoffbelastung.

Kann die fahrzeuginterne IT-Kommunikation noch als privatwirtschaftliche IT eingeordnet werden, so ist die Grenze zu öffentlicher IT spätestens dann erkennbar, wenn das Fahrzeug mit externen Systemen wie anderen Fahrzeugen (Car-to-Car) oder mit Ampelanlagen oder Leitsystemen (Car-to-Infrastruktur) kommuniziert. Ebenfalls müssen Verkehrsinfrastrukturen mit anderen Informationsverbänden zusammenwirken, weshalb Standards und übergreifende Architekturkonzepte erforderlich sind. Beispielsweise sind Schnittstellen zum Identitätsmanagement sowohl für die Identitäten von Personen (etwa beim Einsatz des neuen Personalausweises) als auch für die Identitäten von Fahrzeugen bzw. Fahrzeugelementen nötig, um eine sichere Kommunikation zu gewährleisten. Privatheit und

Datenschutz sind sicherzustellen, um die nicht autorisierte Erstellung von Bewegungsprofilen zu verhindern.

Im Hinblick auf das grenzüberschreitende Zusammenwirken der neuen Dienste und Infrastrukturen sind Insellösungen zu vermeiden, indem Interoperabilität gewährleistet wird.

3.4 VERTRAUENSWÜRDIGE IDENTITÄTEN

Identitäten dienen der Erkennung von Personen und Objekten, bilden die Grundlage für die Zuordnung von Rechten, Werten und Nachweisen und unterstützen die Schaffung von sicheren, vertrauensvollen Beziehungen, die in neuen Identitätsverbänden angewendet werden. Was heute als »vernetzte Gesellschaft« wahrgenommen wird, ist erst der Anfang eines Transformationsprozesses, der sich in den nächsten Jahren massiv beschleunigen wird. Um vertrauenswürdige Identitäten in neuen Informationsverbänden zu nutzen, müssen eine Vielzahl von innovativen und interoperablen Technologien, Verfahren, Systemen und Infrastrukturen entwickelt und bereitgestellt werden.

In Deutschland wird die sichere Identität von Personen durch den neuen Personalausweis unterstützt. Der elektronische Identitätsnachweis bietet vielfältige Einsatzmöglichkeiten für elektronische Dienstleistungen von Verwaltung und Wirtschaft, die personen- bzw. ausweisbezogene Daten benötigen. Mit De-Mail kann eine vertrauenswürdige Kommunikation erfolgen, da sowohl die Identität der Kommunikationspartner als auch der Versand und der Eingang von De-Mails jederzeit zweifelsfrei nachgewiesen werden können.

WÄHREND IM ALLTAG EIN KOMPLEXES,
ABER VERTRAUTES WECHSELSPIEL VON
SICH-ZEIGEN UND SICH-VERBERGEN GESPIELT
WERDEN KANN, BEDARF ES IN DER
VIRTUELLEN WELT NEUER TECHNISCHER LÖSUNGEN.

Weitere Beispiele für den Einsatz von vertrauenswürdigen Identitäten sind:

- Verbund vom neuen Personalausweis mit mobilen Endgeräten;
- Vertrauenswürdige Identitätsattribute aus anderen Kontexten, z. B. Firmenzugehörigkeit, Bonität oder Vormundschaft;
- Identitäten (inkl. Altersverifikation) von Kindern und Jugendlichen für den Jugendschutz;
- Nichtpersonenbezogene Identitäten zum Beispiel Identitäten von Objekten und Diensten (Internet der Dinge, Internet der Dienste).

Auch in anderen EU-Mitgliedstaaten sind ab dem Jahr 2000 elektronische Identitätsnachweise eingeführt worden, die eine sichere Identifizierung und Authentisierung für elektronische Dienstleistungen unterstützen. Trotz europäischer Standardisierungsbemühungen wie der European Citizen Card sind die elektronischen Identitätsnachweise bislang nationale Insellösungen. Ein Rechtsrahmen für die grenzübergreifende Anerkennung und Interoperabilität sicherer elektronischer Identitäten ist daher zwingend erforderlich und wurde als Schlüsselaktion 3 in die Digitale Agenda²² aufgenommen. Als Ergebnis verschiedener Studien und Pilotprojekte²³ wie beispielsweise STORK, SPOCS und PEPPOL wurde am 4. Juni 2012 von der Europäischen Kommission der »Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt« veröffentlicht. Dieser bildet einen Rahmen für die sichere grenzüberschreitende Identifizierung, Authentisierung und für weitere Vertrauensdienste.

Identitäten benennen und charakterisieren aber nicht nur Personen, sondern auch Dinge, Ressourcen, Dienste und andere Objekte. Für die sichere Nutzung von Identitäten in öffentlicher IT ist die Authentizität der Identitätsdaten von entscheidender Bedeutung. Sind diese gefälscht, veraltet oder nicht nachweis-

bar, kann auch eine hochsichere Infrastruktur keine vertrauenswürdige Kommunikation erzeugen.

Eine der größten Herausforderungen des Identitätsmanagements für öffentliche IT ist es, 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 und Privatheit dagegen schränken die Verfügbarkeit hierzu erforderlicher Daten und Informationen ein. Während dies im Alltag durch ein komplexes, aber vertrautes Wechselspiel von Sich-Zeigen und Sich-Verbergen gewährleistet wird, bedarf es für funktionale Äquivalente in elektronischen Kommunikationssystemen hierzu neuer technischer Lösungen.

4. ZUSAMMENFASSENDE THESEN

Die Auseinandersetzung mit öffentlicher IT hat eine Vielzahl von Herausforderungen und Handlungsfeldern aufgezeigt. Abschließend werden die Ergebnisse in Form von pointierten Thesen entlang der drei Kapitel zusammengefasst.

Eingrenzung öffentlicher IT

- Öffentliche Räume konstituieren sich durch gesellschaftlich relevante Kommunikation. Das Internet ist hierfür das derzeit wohl bedeutendste Beispiel.
- Öffentliche IT bildet die Grundlage für virtuelle öffentliche Räume.
- Öffentliche Daten und IT-Infrastrukturen sind leicht zugänglich und können durch staatliche, privatwirtschaftliche oder private Stellen bereitgestellt werden.
- Teile der von Staat, Kommunen und anderen öffentlichen Einrichtungen betriebenen oder beauftragten IT-Infrastruktur bilden eine wesentliche Basis öffentlicher IT.

Anforderungen an die öffentliche Hand

- Bund, Ländern und Kommunen kommt eine Gewährleistungsverantwortung für öffentliche IT zu, die technische und wirtschaftliche Aspekte ebenso umfasst wie rechtspolitische, gesellschaftliche und kulturelle.
- Öffentliche IT erfordert und fördert eine ebenen- und anwendungsübergreifende Zusammenarbeit.
- Die öffentliche Hand sollte die Notwendigkeit und die Möglichkeit zur Beeinflussung der IT-Entwicklung als strategisches Instrument verstehen – und so vom Getriebenen zum Treiber werden.
- Die Gewährleistung einer effektiven und effizienten öffentlichen IT erfordert gerade bei Ausnutzung von Selbstregulierungskräften fundierte technische und fachliche Expertise.

Aspekte der Handlungsfelder

- Die öffentliche Hand schafft durch die Öffnung ihrer Arbeit und die Bereitstellung des Zugangs zu IT-Infrastrukturen neue öffentliche Räume.
- Die ganzheitliche Ausrichtung öffentlicher IT fußt in technischer Hinsicht auf Interoperabilität und in organisatorisch-rechtlicher Hinsicht auf ebenen- sowie bereichsübergreifender Koordinierung.

- Öffentliche IT ist in vielfältiger Weise geeignet, gesellschaftliche Herausforderungen und Bedarfe zu adressieren.
- Der Staat kann in ausgewählten Bereichen eine Schlüsselposition für die Entwicklung funktionaler Äquivalente zu Mechanismen der Alltagswelt in virtuellen Räumen einnehmen.

Aus den Überlegungen ergibt sich die Notwendigkeit, öffentliche Informationstechnologie offen zu denken. Unter öffentlicher Informationstechnologie verstehen wir dabei Informationstechnologien, die in einem öffentlichen Raum durch die gesamtgesellschaftliche Relevanz unter besonderer Berücksichtigung der staatlichen Verantwortung stehen. Die Breite dieser Sichtweise offenbart sich in mannigfaltigen Spannungsfeldern: zwischen ressortspezifischen Sichten, disziplinären Vorgehensweisen und föderalen Ebenen; zwischen gesellschaftlichen Subsystemen wie Wirtschaft, Gesellschaft und öffentlicher Hand; zwischen visionärer Grundlagenforschung und konkreten Anwendungen; zwischen gesellschaftspolitisch und technisch; und insbesondere zwischen den mannigfaltigen Erwartungen, die ein immer größerer Teil der Gesellschaft als aktive Nutzer öffentlicher Informationstechnologien an diese richtet und zunehmend als Anforderungen formuliert. Diesen Prozess gilt es, am Gemeinwohl orientiert, proaktiv, neutral und kenntnisreich zu begleiten.



¹ BVerfG, 1 BvR 699/06 vom 22.2.2011, Absatz-Nr. (1 - 128); http://www.bverfg.de/entscheidungen/rs201110222_1bvr069906.html.

² Niklas Luhmann, Soziale Systeme, Grundriß einer allgemeinen Theorie, Frankfurt a.M.: Suhrkamp 1984.

³ Statistisches Bundesamt, Informationsgesellschaft in Deutschland, Ausgabe 2009; <https://www.destatis.de/DE/Publikationen/Thematisch/EinkommenKonsumLebensbedingungen/Querschnitt/Informationsgesellschaft1030701099004.pdf>.

⁴ Bitkom, Der Staat als Gestalter der digitalen Welt, Industriepolitische Grundsatzpapier, 2012; http://www.bitkom.org/files/documents/grundsatzpapier_062012.pdf.

⁵ Nils Otter und Mike Weber, Rekommunalisierung – ein Innovationstreiber im öffentlichen Sektor?; S. 333-350 in: Dennis Hilgers, Reinbert Schauer und Norbert Thom (Hrsg.): Staat und Verwaltung im Spannungsfeld von New Public Management, Open Government und bürokratischer Restauration, Linz: Trauner 2012.

⁶ Der Bundesgerichtshof, Az.: III ZR 98/12; <http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=7a782b47ebd960e7d06a8d3a8eba85de&n=63259&pos=0&anz=1>.

⁷ Andreas Betz, Breitbandversorgung im ländlichen Raum, Im Verbund zu schnellem Internet; S. 26-29 in: Datareport 1/2012; <http://www.dataport.de/ueber-uns/publikationen/Documents/Datareport-2012-1/Datareport-2012-1.pdf>.

⁸ Bundesnetzagentur, Versorgungsaufgabe im 800-MHz-Bereich bundesweit erfüllt; http://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2012/121126_BreitbandausbauErfuehlt.html.

⁹ Bundesministerium des Innern, FIM, E-Government mit Zukunft, Die einheitliche Basis für eine effiziente Verwaltung in Kommunen, Ländern und Bund, 2013; http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/Steuerungsprojekte/FIM_Brosch%C3%BCre.pdf.

¹⁰ Bundesministerium des Innern, Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS Strategie); <http://www.bmi.bund.de/cae/servlet/contentblob/544770/publicationFile/27031/kritis.pdf>.

¹¹ Eric von Hippel, Lead Users: A Source of Novel Product Concepts, 1986; S. 791-805 in: Management Science 32.

¹² Bundesministerium des Innern, 14 Thesen zu den Grundlagen einer gemeinsamen Netzpolitik der Zukunft; http://www.bmi.bund.de/cae/servlet/contentblob/1099988/publicationFile/88667/thesen_netzpolitik.pdf.

¹³ Renate Mayntz und Fritz W. Scharpf, Steuerung und Selbstorganisation in staatsnahen Sektoren; S. 9-38 in: ders. (Hrsg.): Gesellschaftliche Selbstregulierung und politische Steuerung, Frankfurt a.M.: Campus 1995; S. 29.

¹⁴ Matthias Kammer, Marie-Therese Huppertz und Horst Westerfeld (Hrsg.): ISPRAT White Paper, Vom Open Government zur Digitalen Agora - Die Zukunft offener Interaktionen und sozialer Netzwerke im Zusammenspiel von Politik, Verwaltung, Bürgern und Wirtschaft, 2010.

¹⁵ Fraunhofer FOKUS, Studie »Open Government Data Deutschland«, Eine Studie zu Open Government in Deutschland im Auftrag des Bundesministerium des Innern, Juli 2012; http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/ModerneVerwaltung/opengovernment.pdf.

¹⁶ Eine Änderung der PSI-Richtlinie wird derzeit im Europäischen Parlament diskutiert; http://ec.europa.eu/information_society/policy/psi/docs/pdfs/directive_proposal/2012/de.pdf.

¹⁷ Jörn von Lucke, Open Government – Öffnung von Staat und Verwaltung, Gutachten für die Deutsche Telekom AG zur T-City Friedrichshafen, Version vom 09.05.2010; http://www.zu.de/deutsch/lehrtstuehle/ticc/JvL-100509-Open_Government-V2.pdf.

¹⁸ 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; <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:211:0055:0093:DE:PDF>.

¹⁹ BSI, TR-03109 Smart Energy, Version 1.0 (Release Candidate), 21.12.2012; https://www.bsi.bund.de/DE/Themen/SmartMeter/TechnRichtlinie/TR_node.html.

²⁰ Fraunhofer FOKUS, Zentrum für Smart Cities; <https://www.ict-smart-cities-center.com/smart-cities>.

²¹ 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; <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:207:0001:0013:DE:PDF>.

²² Europäische Kommission, Eine Digitale Agenda für Europa, KOM(2010) 245 endgültig/2, 26.8.2010; <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=C OM:2010:0245:FIN:DE:PDF>.

²³ EU, eGovernment Large Scale Pilot Projects; <https://ec.europa.eu/digitalagenda/en/egovernment-large-scale-pilot-projects>.

GEFÖRDERT VOM



Bundesministerium
des Innern

KONTAKT

Jens Fromm
Leiter Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
jens.fromm@fokus.fraunhofer.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de
www.oeffentliche-it.de

ISBN: 978-3-9816025-0-0

