Kompetenzzentrum
Öffentliche IT

KOMPETENZZENTRUM ÖFFENTLICHE INFORMATIONSTECHNOLOGIE

Jens Fromm, Marit Hansen, Gerrit Hornung, Philipp Müller, Kay Ruge, Helga Springeneer

MENSCHEN IN DER DIGITALEN GESELLSCHAFT

in Kooperation mit:
INITIATIVE D21

Fraunhofer FOKUS

IMPRESSUM

Autoren:
Jens Fromm, Marit Hansen, Gerrit Hornung,
Philipp Müller, Kay Ruge, Helga Springeneer

Gestaltung:
Reiko Kammer

Herausgeber:
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3463-7173
Telefax: +49-30-3463-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

1. Auflage Mai 2014

Die veröffentlichten Artikel geben die Meinungen der
Autorinnen und Autoren wieder und repräsentieren nicht
notwendigerweise die Position des Herausgebers.

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

Wir reden nicht mehr über das Ob. Wir reden nur noch über das Wie.

Darüber allerdings müssen wir reden. Und viele Vorurteile über Bord werfen. Wir haben es mit unserer Beteiligungsplattform LiquidFriesland gezeigt: Es geht nicht allein um Technik. Es geht darum, diese Technik kreativ in Organisation und Kommunikation einzubinden, einen Kulturwandel in Verwaltungen zu Transparenz und Open Government zu begleiten, auch ganz geerdet für mehr Breitbandanschlüsse zu sorgen. Diese Schritte alle gleichzeitig zu unternehmen und sich immer gewahr zu sein, was im Mittelpunkt steht: Nicht das Projekt. Nicht die Strategie. Nicht die Software. Sondern der Mensch.

Sven Ambrosy
Landrat des Landkreises Friesland

DEUTSCHER LANDKREISTAG

INITIATIVE D21

Kompetenzzentrum Öffentliche IT

ULD

UNIVERSITÄT PASSAU

verbraucherzentrale Bundesverband

INHALTSVERZEICHNIS

	Vorwort	3
	Inhaltsverzeichnis	5
1.	**Eine offene Bürgergesellschaft**	**6**
2.	**Der Bürger im Zentrum der digitalen Gesellschaft**	**8**
3.	**Der Verbraucher in der digitalen Welt**	**10**
4.	**Herausforderungen für den selbstbestimmten Bürger**	**12**
5.	**IT-Grundversorgung als staatliche Aufgabe**	**14**
6.	**Öffentlicher Raum 2.0: IT im Wandel**	**16**

1. EINE OFFENE BÜRGERGESELLSCHAFT

Im Jahr 2014 ist die Idee, dass die Informationsgesellschaft auf einer anderen sozio-strukturellen Logik basiert als die durch Max Weber und Frederick Winslow Taylor beschriebene Massengesellschaft des 20. Jahrhunderts, allgemein akzeptiert. Und das sollte nach über 50 Jahren Diskussion über die Begrifflichkeit »Informationsgesellschaft« auch so sein.

Wenn es aber um die konkrete Ausgestaltung geht, herrscht noch keine Einigkeit. Politik, Verwaltung, Unternehmen, Universitäten und die Zivilgesellschaft haben in den letzten zehn Jahren oft aneinander vorbeigeredet, wenn es um die Themen E-Government, Digitalisierung, Netzwerkgesellschaft und das Internet als gesamtgesellschaftliches Phänomen ging. Es fehlt immer noch ein Verständnis für das Zusammenspiel zwischen der strukturellen Logik und den Gestaltungsräumen, die wir in der Informationsgesellschaft haben.

Dabei ist die grundsätzliche Logik nicht besonders kompliziert.

- Die Fähigkeit Daten zu erheben und zu verarbeiten erlaubt uns unsere Welt anders zu verstehen und zu steuern – Datafizierung.
- Die Fähigkeit Systeme miteinander zu vernetzen, erlaubt uns, anders zu organisieren und zu kollaborieren – Vernetzung.
- Die Perspektiv-Verschiebung von Aufgabe zu Prozessen erlaubt uns anders über das Erreichen von Wirkung nachzudenken – Prozess- und Architekturdenken.

Grundsätzlich kann man annehmen, dass diese drei Megatrends die Gestaltungskompetenz eher dezentralisieren als zentralisieren und die Unterscheidung zwischen Produzent und Konsument relativieren. D.h., die für Politik und Verwaltung epistemologisch relevanteste Einheit, um diese Transformation zu denken, sind »die Bürger« und/oder allgemeiner gesprochen die »Nutzer«.

Das Potenzial von Organisationen, die durch n-zu-n-Beziehungen strukturiert sind, ist so groß, dass zu erwarten ist, dass sowohl Unternehmen und Verwaltungen als auch zivilgesellschaftliche Gruppen fundamental anders geführt werden. Dies geschieht allerdings nicht automatisch, sondern muss strategisch angegangen werden. Verkürzt geht es darum, dass man Offenheit gezielt einsetzt. Ein Thema wie Offenheit und Transparenz ist plötzlich auf der Tagesordnung und Verfassungsänderungen stehen somit an. Die Ersetzung des Amtsgeheimnisses durch eine aktive Veröffentlichungspflicht erscheint in vielen Ländern als ein weiterer Schritt zu »mehr Demokratie«. Die Grundidee von Offenheit hat strategisches Potenzial, ist allerdings auch jenseits der Transparenzdebatte relevant. Denn Offenheit als Mittel ermöglicht neue strategische Ansätze, neue Organisationsformen und neue Formen der Führung. Wir sehen das heute bei Open Data, Open Access, OpenStreetMap, Open Science oder Open Government, implizit auch bei Themen wie Big Data, Cybersecurity, Bring-Your-Own-Technology (BYOT) und Cloud-Computing. Es ist heutzutage wichtiger denn je, dass sich Entscheider in Organisationen (Management/Politik) mit diesen Fragen auseinandersetzen um die Potenziale, die ein strategischer Einsatz von Offenheit mit sich bringt, zu realisieren. Nur wenn wir Offenheit als Mittel einsetzen, werden wir es schaffen unsere Organisationen und Gesellschaften im 21. Jahrhundert erfolgreich zu führen.

Wir müssen in den nächsten Jahren erreichen, dass sich EntscheiderInnen in den wichtigen Institutionen unserer Gesellschaft auf diese Situationslogik der Informationsgesellschaft einlassen und lernen, diese strategisch zu nutzen. D.h. wir brauchen neue Management-Ansätze für die bürgerzentrierte Gesellschaft. Wir müssen die strukturelle Logik »Wie funktioniert die Welt?«, Organisation »Wie organisieren wir kollektives Handeln?« und Strategie, wie können wir gestalten?« wieder miteinander in Einklang bekommen. Das gab es und gibt es immer wieder in der Geschichte der Menschheit. Machiavelli hat das für das 16. Jahrhundert beschrieben, Martin Luther brachte den Buchdruck und das emanzipatorische Denken der Renaissance zueinander und startete damit eine globale Revolution. Ähnliches erleben wir heute.

Dabei geht es um Fragen der strukturellen Logik »Warum sind Bürger die relevante Analyseeinheit in der Netzwerkgesellschaft?« und um strategische Fragen »Wie können Bürger intelligent an politischen und verwaltungstechnischen Prozessen beteiligt werden?«, sowohl auf der demokratisch-legitimatorischen Ebene wie auch in der profanen Verwaltungsarbeit.

Burberry und die öffentliche Verwaltung

Es geht dabei nicht um ein technisches, eher um ein logisches Verständnis. Strategie muss in der Netzwerkgesellschaft unter den »Bedingungen der Möglichkeit« einer technologisch mediatisierten Welt gedacht und gehandelt werden. Angela Ahrendts, die CEO von Burberry, hat uns das seit 2006 in der ursprünglich nicht digitalisierten Mode-Industrie gezeigt, als sie ihren Chief Technology Officer auf die gleiche Stufe wie ihren Chief Creative Officer gestellt hat, indem sie die Kommunikation mit den Kunden von 1-zu-n in den klassischen Medien zu n-zu-n in den sozialen Medien umgestellt hat und indem sie das digitale Erleben auf der Website mit dem taktil-analogen Einkaufserlebnis in ihren Läden verknüpft hat: Nutzer-orientierung par excellence! Ähnliches geschieht gerade in der ehemals »menschelnden« und papierbasierten Welt der Politik und Verwaltung. Wichtig ist, dass auch dort die Angela Ahrendts die Verantwortung übernehmen.

Ein ganzheitlicher Ansatz im Management von E-Government-Projekten

Im Prinzip ist das einfach, aber eben nicht trivial. Wir brauchen einen ganzheitlichen Ansatz, der das Potenzial digitaler Netzwerktechnologien hebt. Wir müssen Vernetzung, Datafizierung und Prozess-/Architekturdenken zusammenbringen und damit etwas kombinieren, was in der von und durch Max Weber gedachten Verwaltung nicht möglich war: die Industrialisierung der Systeme im Hintergrund durch Integration und Standardisierung einerseits und andererseits die Fokussierung auf Interaktivität und Agilität durch eine Individualisierung der Nutzererfahrung, durch die Konzentation auf Intuitivität im Zusammenspiel mit Bürgern und Nutzern. D.h., wir müssen zwei Dinge kombinieren, die nur selten gemeinsam gedacht werden.

Um ein bürgerzentriertes, aber effizientes E-Government für die digitale Netzwerkgesellschaft umzusetzen, brauchen wir also drei Dinge:

- EntscheiderInnen, die die Logik der digitalen Netzwerkgesellschaft grundsätzlich internalisiert haben und ihre Gestaltungsräume zu nutzen wissen.
- Prozess-Architekten digitaler Staatlichkeit, die Industrialisierung, Interaktivität und Agilität gleichzeitig in Prozesse umsetzen können.
- Eine Organisationskultur, die Offenheit, also intelligentes Schnittstellenmanagement, zelebriert.

Nur wenn wir es schaffen eine digitale Staatlichkeit zu etablieren, die Standardisierung und Integration lebt, aber agil mit Ausnahmen umgehen kann, die Daten nutzt, aber auch Daten sicher schützt, die offen ist, aber diese Offenheit auch intelligent absichert, werden wir im Wettbewerb bestehen und dem Selbstverständnis unserer Gesellschaft entsprechen. Das ist nicht trivial, aber machbar. Wir müssen es angehen.

Dr. Philipp Müller
Initiative D21

Dr. Philipp S. Müller verantwortet den Bereich Public Affairs bei CSC und unterrichtet an der Business School (SMBS) der Universität Salzburg.

2. DER BÜRGER IM ZENTRUM DER DIGITALEN GESELLSCHAFT

Die digitale Durchdringung nahezu aller Lebensbereiche ist mittlerweile Allgemeingut. Das Internet ist aus dem Alltag vieler Menschen nicht mehr wegzudenken. Insofern kommt auch dem Verhältnis Kommune – Bürger, das in einer gesamtstaatlichen Betrachtung das engste ist, sowie den diesbezüglichen Auswirkungen und Herausforderungen große Bedeutung zu.

1. These: Digitalisierung in Stadt und Land erfordert Breitband überall

Unabhängig von allen denkbaren oder wünschenswerten Verheißungen der Digitalisierung ist es zwingende Grundvoraussetzung, dass zunächst die digitale Infrastruktur bereitsteht, um überhaupt Teil der digitalen Gesellschaft sein zu können. Nach wie vor besteht hier ein großes Defizit hinsichtlich des flächendeckenden Ausbaus moderner und zukunftssicherer Breitbandnetze. Zahlreiche Studien bestätigen gerade hinsichtlich der Breitbandversorgung die deutlich fehlende Anbindung des ländlichen Raumes, insbesondere bei Bandbreiten von 16 MBit/s und 50 MBit/s. Hier weist Deutschland im europäischen Vergleich einen deutlichen Nachholbedarf auf, der auch verstärkte staatliche institutionelle Förderungen zwingend erforderlich macht. Angesichts dieses Defizits sind bereits jetzt zahlreiche Landkreise gemeinsam mit dem kreisangehörigen Raum selbst in Vorleistung getreten, um diese wichtige Infrastruktur von der Schaffung eigener Gesellschaften bis hin zum Betrieb von Netzen, zu schaffen. Hierin manifestiert sich der Anspruch gleichwertige Lebensverhältnisse bereitzustellen und Bürgerinnen und Bürgern auch im ländlichen Raum gleiche Lebenschancen zu ermöglichen.

2. These: Mitmachen erfordert entsprechende Kenntnis bei Bürgern

Ein zweiter Aspekt der Ermöglichung betrifft die Medienkompetenz bzw. die Befähigung zur Teilnahme am digitalen Austausch. Auch hier kommt den Kommunen unter dem oftmals abstrakt als gesellschaftliche Teilhabe bezeichneten Gesichtspunkt eine wichtige Unterstützungsfunktion zu. Damit soll nicht in Abrede gestellt werden, dass es primär Aufgabe jedes Einzelnen ist, sich die digitalen Kompetenzen selbst oder im Austausch mit anderen anzueignen. Diese Selbstverpflichtung gilt im Bereich der Digitalisierung ein Leben lang. Darüber hinaus sind aber ergänzend insbesondere Schulen und andere Bildungseinrichtungen, wie die Volkshochschulen, die alle regelmäßig in kommunaler Trägerschaft stehen, aufgefordert Angebote für die Wissensaneignung oder Vertiefung zu schaffen.

3. These: Der Staat muss Datenschutz und sicheren Datenaustausch gewährleisten

Jenseits der zuvor dargestellten Grundvoraussetzungen im Bereich digitaler Infrastruktur und der Befähigung zum digitalen Austausch besteht ein weites Feld kommunaler Möglichkeiten Interaktion der Bürger zu befördern bzw. auch die Einbeziehung der Bürgerschaft zu ermöglichen. Dabei geht es vorrangig darum, Verwaltungsleistungen mit spürbaren Mehrwerten anzubieten und freiwillige Angebote zu schaffen. Nur ausnahmsweise kommen bspw. im Katastrophenfall, wie zuletzt bei dem Sommerhochwasser an Donau und Elbe, auch regulatorische Beeinflussungen der Interaktion von Bürgern in Betracht.

Hinsichtlich der Schaffung sinnvoller digitaler Angebote steht die rechtssichere, datenschutzkonforme, medienbruchfreie Abwicklung von Verwaltungsverfahren im Fokus. Es muss endlich gelingen einfache, für jedermann praktikable Wege für einen solchen Austausch zu etablieren. Elektronische Bestellungen im Bereich des E-Commerce oder Reservierungen von Bahnfahrten und Flügen bis hin zum Online-Banking sind Beleg für die elektronische Abwicklung auch komplexer und sensibler Bereiche. Insofern stellen immer mehr verwirklichte Bürgerserviceportale auf kommunaler Ebene, die eine Authentifizierung, die Abwicklung von Verwaltungsfachverfahren bis hin zur elektronischen Bezahlung ermöglichen, eine Perspektive dar. Um eine zumindest landesweite Abwicklung von Verwaltungsverfahren unterschiedlicher Verwaltungsträger zu ermöglichen sind Verknüpfungen mit entsprechend landesweit geltenden Bürgerkonten zu befördern.

4. These: Kommunen fördern (digitale) Beteiligung der Bürger

Im Bereich der Partizipation und Einbindung der Bürgerschaft in die Gestaltung des Gemeinwesens nehmen die Kommunen bereits jetzt vielfach eine Vorreiterrolle ein. Maßgebliche Bemühungen im Handlungsfeld Open Government basieren auf kommunalen Erfahrungen. Einen umfassenden, und, soweit ersichtlich, bisher deutschlandweit einmaligen Weg der Bürgerbeteiligung geht bspw. der Landkreis Friesland. An »Liquid Friesland« können sich alle Kreisbewohner beteiligen, die über einen Internetzugang verfügen. Ermöglicht wird das Einbringen eigener Vorlagen oder die Diskussion von Vorhaben, die im Kreistag erörtert werden. Jenseits derartig umfassender Beteiligungsmöglichkeiten sind insbesondere die frühzeitige Mitwirkung bei einzelnen (bspw. städtebaulichen) Vorhaben, die Schaffung von Erörterungsmöglichkeiten hinsichtlich denkbarer Alternativen und eine ggf. auch moderierte Diskussion über die zukünftige Entwicklung einer Gebietskörperschaft, sei es auf gemeindlicher, sei es auf kreislicher Ebene, sinnvolle Fortentwicklungen. Niederschwellig die Verantwortung der Bürger für ihr Gemeinwesen stärkend sind auch kommunale Angebote gefragt, auf Infrastrukturprobleme hinzuweisen, wie dies bspw. in Brandenburg für zahlreiche Kommunen mit dem Märker Brandenburg realisiert worden ist.

Im Bereich der Sicherheit – im Zusammenhang mit Warnungen vor Katastrophen jedweder Art – kommen aus kommunaler Sicht neben den klassischen Instrumenten wie Sirenen zukünftig auch mobile Endgeräte der Bürgerinnen und Bürger in Betracht. Ein ergänzendes Warnsystem in diesem Sinne bietet bspw. das in zahlreichen Landkreisen und Städten bereits zum Einsatz gebrachte System KATWARN, das in Abstimmung mit den zuständigen Katastrophenschutzbehörden Warnmeldungen verfasst und ortsgenau auf die gefährdeten Postleitzahlenbereiche abstimmt. Über eine zunächst angestrebte, grundsätzlich freiwillige Beteiligung an einem solchen System mittels einer SMS-Anmeldung hinaus erscheint es angesichts der zunehmenden Verbreitung mobiler Endgeräte sinnvoll, auch Rechtsgrundlagen dergestalt zu schaffen, ggf. zwingend unmittelbar Warnungen auf derartige mobile Endgeräte versenden zu können. Dies ermöglichte auch in einem anderen Zusammenhang eine Lösung: Beim Sommerhochwasser 2013 haben sich – organisiert über soziale Netzwerke – freiwillige Helfer eigeninitiativ an ihnen sinnvoll erscheinende Stellen zur Deichsicherung begeben, was sich weder im Hinblick auf die konkrete Hochwassergefährdungslage, noch auf die Koordinierung der Helfer durch die zuständigen Katastrophenschutzbehörden als sinnvoll erwiesen hat. Auch in derartigen Fällen sollte der Staat künftig handlungsfähig sein.

Dr. Kay Ruge
Deutscher Landkreistag

Dr. Kay Ruge studierte Rechtswissenschaften an der Christian-Albrechts-Universität zu Kiel und an der University of Surrey in England (1991-1996).

Seit 2003 ist er beim Deutschen Landkreistag tätig. Als Beigeordneter ist er dort für Verfassungs- und Europafragen sowie Neue Medien zuständig.

3. DER VERBRAUCHER IN DER DIGITALEN WELT

In der digitalen Welt zahlen Verbraucher mit einer Währung, die sie nicht kennen und die sie nicht sehen: mit ihren Daten. Ohne Anpassung der gesetzlichen Regelungen und einer digitalen Marktaufsicht kann das auf Dauer nicht gut gehen.

Die Digitalisierung des Alltags

Ohne vertiefende technische Vorkenntnisse kann der Nutzer selbst eigene Beiträge publizieren, Nachrichtenartikel kommentieren, einen eigenen Blog führen, Erfahrungen zum Hausarzt in einem Forum weitergeben, sich politisch beteiligen, das günstigste Hotel suchen etc. Der Berg an persönlichen Daten wächst stetig. Aber den größeren Anteil machen nicht die Daten aus, die Verbraucher selbst eingeben, sondern die, die automatisch im Hintergrund über sie generiert werden. Menschen werfen »digitale Schatten«. Smartphones, Überwachungskameras, vernetzte Autos oder smarte Stromzähler erzeugen ständig Daten. Aus diesen Daten lassen sich viele wertvolle Erkenntnisse gewinnen. Im Gesundheitswesen können Grippewellen genauer vorhergesagt und neue Therapien für die Bekämpfung von Krebs entwickelt werden. Auch neue Dienste für Verbraucher, wie die vernetzte Verkehrsplanung, sind denkbar. Wenn das Smartphone nicht nur den nächstgelegenen Carsharing-Standort anzeigt, sondern zusätzlich auch die optimale Verbindung mit öffentlichen Verkehrsmitteln und Leihfahrrädern mit einschließt, dann können die verschiedenen Verkehrsmittel je nach Bedarf gewählt und miteinander kombiniert werden.

Algorithmen bestimmen das digitale Leben

Neben diesen Vorteilen nehmen gleichzeitig aber auch die Risiken für die Persönlichkeitsrechte der Verbraucher immer weiter zu. Unternehmen verfügen bereits heute über eine Unmenge an Daten der Verbraucher: Name, Wohnort, Kreditkartendaten, Einkaufsverhalten, Bewegungsdaten u. v. m. Webdienste sammeln nicht nur Informationen über ihre Kunden, sondern auch über deren Freunde und Bekannte. Durch Cloud-Computing und Big-Data-Analyse werden die Datenberge immer größer und der Zugriff auf die persönlichen Daten der Verbraucher sowie ihre Auswertung immer leichter. Niemand würde zum Bäcker gehen und sagen: Guten Tag, ich heiße Max Müller, bin 46 Jahre alt, verheiratet, Jurist, wiege manchmal 74 Kilo und bin über die Jakob-Müller-Straße hierher gelangt. Im Internet funktioniert es aber genauso. Die Backwarenverkäuferin interessiert das lediglich, wie viele Brötchen man haben will. Für Anbieter im Internet sind persönliche Daten ein begehrtes Gut. Auf Basis der erstellten Profile können Algorithmen heute nicht nur entscheiden, welche Werbung Verbraucher zu sehen bekommen, sondern auch, welchen Preis sie für den neuen Bestseller zahlen sollen, welcher Versicherungstarif am besten zu ihnen passt, ob sie einen Studienplatz erhalten oder mutmaßlich in den nächsten Wochen eine Straftat begehen werden.

Doch nicht nur Unternehmen sind an den Daten der Verbraucher interessiert. Auch Staaten wollen immer mehr Daten ihrer Bürger erfassen. Durch die Digitalisierung ist es einfacher geworden. Sie müssen die Bürger nicht mehr selbst aufwendig überwachen, indem sie Internetleitungen und Telefone anzapfen. Vielmehr verschaffen sie sich Zugriff auf die gewaltigen Datenberge, die die Internetwirtschaft in den letzten Jahren angehäuft hat. Die Grenzen zwischen privatem und staatlichem Sammeln von Daten, zwischen Verbraucherschutz und Bürgerrechten verschwimmen immer mehr.

Die technischen Systeme und Geschäftsprozesse im digitalen Zeitalter sind heute zu komplex, als dass sie von den meisten Verbrauchern durchschaut werden könnten. Sie können nicht mehr überblicken, wo auf der Welt ihre Daten gespeichert sind, welche Wege sie gehen, wer auf die Daten zugreift und mit welchen anderen Datenbeständen sie verknüpft werden. Zudem wissen Verbraucher nicht, welchen Wert ihre Daten haben. Sie zahlen mit ihren Daten, wissen aber nicht, wie viel und an wen.

Europa braucht ein Grundgesetz für das Netz

Trotz der vielfältigen Chancen, die die Digitalisierung bietet, dürfen die Persönlichkeitsrechte der Nutzer nicht auf der Stre-

cke bleiben. Es ist ein Grundrecht, dass der Einzelne selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen können muss. Eine zentrale politische Aufgabe ist es, dafür Sorge zu tragen, dass dieses Grundrecht gewahrt bleibt und wieder einen hohen Stellenwert erhält. Nur so wird sichergestellt, dass Verbraucher den technischen Systemen und den dahinter liegenden Geschäftsprozessen wieder vertrauen. Die Europäische Union strebt mit der EU-Datenschutz-Grundverordnung einen verbesserten, harmonisierten und modernen Datenschutz in Europa an. Die Bundesregierung muss daher eine Führungsrolle in Europa einnehmen und sich für ein hohes Datenschutzniveau in der Europäischen Union einsetzen. Für Unternehmen und den Staat muss es strenge Regeln geben, wie mit den Daten der Verbraucher und Bürger umgegangen werden darf. Klare Transparenzverpflichtungen, Einwilligungsregelungen und durchsetzbare Auskunfts- und Löschrechte sind ein Mindestmaß an Verbraucherdatenschutz, den es umzusetzen gilt.

Die Digitalisierung zu einem Chancenthema für Markt und Verbraucher machen

Auch die Wirtschaft muss ein größeres Interesse an einem starken Datenschutz entwickeln, denn nur so kann das Risiko verringert werden, dass Verbraucher sich den technischen Systemen und dahinter liegenden Geschäftsprozessen ausgeliefert fühlen. Der verantwortungsvolle Umgang mit den Daten der Nutzer, Offenheit und Transparenz bei der Erhebung und Verwertung sensibler Daten müssen die oberste Maxime für die Wirtschaft sein. Personenbezogene Daten dürfen nicht verwendet werden ohne Einwilligung der Betroffenen und ohne Zweckbindung. Die Betroffenen müssen mitbestimmen können, ob und in welcher Form ihre Daten erfasst, zusammengeführt und genutzt werden.

Viele Verbraucher wissen nicht, wie sie ihre Privatsphäre im Web schützen können. Sie brauchen Hilfe und einfache Anleitungen zum Selbstschutz. Und sie müssen sich darauf verlassen können, dass der digitale Markt eine Aufsicht hat; dass Marktverstöße erkannt und geahndet werden. Unabhängige Verbraucherverbände sind bereits jetzt schon elementare Erkenntnisquelle für vorhandenes Marktversagen und können bei einer besseren Ausstattung folglich auch einen wichtigen Beitrag zu einer systematischen Marktbeobachtung im Bereich der digitalen Welt beisteuern. Sie können aufzeigen, wo es Fehlentwicklungen gibt und Schaden droht. Diese Erkenntnisse sind elementar für Aufsichtsbehörden, Politik, Wirtschaft und Wissenschaft und tragen wesentlich zum Aufbau von Vertrauen in den Schutz von Daten und Privatsphäre bei.

Helga Springeneer
Verbraucherzentrale Bundesverband

Helga Springeneer arbeitet seit 2004 beim Verbraucherzentrale Bundesverband und ist seit 2013 Leiterin des Geschäftsbereichs Verbraucherpolitik und Mitglied der Geschäftsleitung. Sie studierte Rechtswissenschaften und Europäische und Internationale Wirtschaftsbeziehungen und war mit einem Schwerpunkt im Wirtschafts- und Zivilrecht als Rechtsanwältin tätig. Ihre Tätigkeit beim Hamburger Institut für Finanzdienstleistungen mit zahlreichen verbraucherbezogenen Projekten und Studien für die Europäische Kommission, für Bundesministerien und Verbände ebnete den Weg in die Verbraucherpolitik. Sie ist u. a. Mitglied der Association Internationale de Droit de la Consommation.

4. HERAUSFORDERUNGEN FÜR DEN SELBSTBESTIMMTEN BÜRGER

Die digitale Gesellschaft wird geprägt von Informationstechnik, die in immer mehr Lebensbereichen eine Rolle spielt. Ein Teil dieser Technik ist den Menschen üblicherweise bewusst, da sie aktiv damit umgehen, z. B. die Computer und Handys, mit deren Hilfe sie Informationen mit anderen Individuen oder mit Organisationen austauschen. Weniger im Bewusstsein verankert sind unterstützende Systeme, z. B. Sensorik im Auto oder im Haus. Das Wissen über die Verarbeitung der Daten durch all diese Systeme und über die potenziellen und tatsächlichen Zugriffe und Auswertungen durch andere ist selbst bei Fachleuten nur begrenzt vorhanden.

These 1: Selbstbestimmung ist essenziell für Datenschutz. Aber die Bedingungen müssen fair sein.

Das für den Datenschutz in Deutschland wegweisende Volkszählungsurteil des Bundesverfassungsgerichts von 1983 stellt das »Recht auf informationelle Selbstbestimmung« als zentral heraus: »Das Grundrecht gewährleistet […] die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.« (BVerfGE 65, 1). Die informierte, freiwillige und widerrufbare Einwilligung ist ein wesentliches Konstrukt des Datenschutzrechts. Allerdings ist bei vielen »Einwilligungen« in der Praxis fraglich, ob die Bedingungen »Informiertheit« und »Freiwilligkeit« tatsächlich erfüllt werden.

These 2: Bürger wollen Selbstbestimmung. Jedenfalls mögen sie keine Fremdbestimmung.

Ausreichende Möglichkeiten zur Selbstbestimmung der Bürger sind wichtig für unser demokratisches Gesellschaftssystem – vom Staat vorgegebene Fremdbestimmung wird generell kritisch betrachtet. Jedoch bedeutet die Möglichkeit zur Selbstbestimmung noch nicht, dass sie auch ausgelebt wird. Andererseits lässt sich das bewusste Nicht-Wahrnehmen der Selbstbestimmung ebenfalls der Selbstbestimmung zurechnen. Die Selbstbestimmung beim eigenen Privatsphärenschutz umfasst die Freiheit, eigene personenbezogene Daten zu veröffentlichen und sich zu exponieren.

These 3: Selbstbestimmung erfordert Verstehen. Und dies erfordert Transparenz.

Schon wegen der hohen Komplexität sind die Datenverarbeitung und die damit verbundenen Risiken nur wenigen Fachleuten verständlich. Die Enthüllungen von Edward Snowden zeigen zudem, dass mächtige Geheimdienste auf so ziemlich alle Daten Zugriff haben. Unter dieser Prämisse wird die informationelle Selbstbestimmung zur Farce.

Notwendig ist das Verständnis der Bürger, wie sie ihre Selbstbestimmung konkret ausüben können. In der digitalen Gesellschaft geht es um den Einsatz der geeigneten technischen Werkzeuge in der richtigen Konfiguration.

These 4: Selbstbestimmung erfordert Bestimmen-Wollen.

Gerade, wenn Menschen sich damit konfrontiert sehen, dass sie die Technik der digitalen Gesellschaft oder ihre Aktionsmöglichkeiten nicht vollständig verstehen, kann dies zu einer Gleichgültigkeit oder gar einem Ohnmachtsgefühl führen. Außerdem ist Selbstbestimmung anstrengend im Vergleich zu einem Verharren in der eigenen Bequemlichkeit, wenn man sich schon mit nicht gerade datenschutzfreundlich gestalteten Diensten arrangiert hat.

These 5: Selbstbestimmung erfordert echte Wahlmöglichkeiten.

Das Besondere an der Informationstechnik ist, dass im Prinzip jeder nicht nur mitmachen, sondern auch eigene Angebote in die digitale Gesellschaft einbringen kann: Schnell mal etwas programmieren, hochladen und die Nutzer-Community über das neue Angebot informieren. Ganz so einfach ist es allerdings nicht, und die meisten Nutzenden greifen auf etablierte Dienste zurück, deren Interessen nicht unbedingt im Einklang mit den

eigenen stehen. Neben der Generalentscheidung »Nutzen: ja/nein?« kann man in vielen Fällen etwas konfigurieren und damit seiner Selbstbestimmung Ausdruck verleihen. Jedoch werden meist nur wenige Optionen angeboten – viele wesentliche Verarbeitungsschritte bleiben unbeeinflussbar. Gerade datenschutzkonforme oder -verbessernde Lösungen fehlen häufig bei den angebotenen Alternativen.

These 6: Selbstbestimmung des Einzelnen kann Effekte auf andere und deren Selbstbestimmung haben.

Es ist nicht ungewöhnlich, dass Entscheidungen einer Person auch andere Menschen betreffen können; teilweise ist dies sogar gewollt, z. B. wenn Eltern Entscheidungen für ihre Kinder treffen. Beim Recht auf informationelle Selbstbestimmung gibt es verschiedene Facetten solch möglicher Auswirkungen:

Einige personenbezogene Daten beinhalten Informationen über andere, beispielsweise die DNA (über Verwandte). Daten über das eigene Verhalten können – selbst wenn kein offensichtlicher Bezug zu anderen Personen besteht – Beziehungsgeflechte offenbaren.

Selbstbestimmte Entscheidungen für eine Preisgabe von Informationen können auch die Erwartungshaltung bei anderen oder die soziale Norm beeinflussen: Wenn die Mehrheit (oder die einen interessierende Zielgruppe) keine Probleme damit hat, Daten herauszugeben, kann ein (selbstbestimmtes) Unterlassen der Preisgabe leicht zu Nachteilen führen.

Mittlerweile werden Analysen in Forschung und Wirtschaft zunehmend auf Basis von leicht verfügbaren Daten (Big Data) durchgeführt. Dies birgt das Risiko einer Fehlsteuerung, da auf ihre Privatsphäre besonders bedachte Personen weniger repräsentiert sind.

Viele Services in der digitalen Gesellschaft setzen auf eine Sogwirkung für weitere Nutzende. Die eigene Entscheidung für einen solchen Dienst beeinflusst auch die Entscheidungen anderer. Die meisten Dienste sind so gestaltet, dass sie immer mehr Daten sammeln und auswerten können. Daraus entsteht eine sich selbst verstärkende Machtposition.

These 7: »Privacy by Default« und »Privacy-Nudges« können die Selbstbestimmung unterstützen.

In den vorherigen Thesen hat sich gezeigt, dass die Möglichkeiten der informationellen Selbstbestimmung, so wie sie heutzutage ausgeprägt sind, nicht besonders gut zur Wahrung der Persönlichkeitsrechte in der Gesellschaft geeignet sind. Zwei wichtige Ansätze könnten künftig in diesem Zusammenhang eine wichtigere Rolle spielen: 1. »Privacy by Default« als Prinzip, nach dem jeder ohne Umkonfiguration einen Dienst nutzen können soll, ohne dass seine Privatsphäre verletzt wird, und 2. »Privacy-Nudges«, d. h. Anstupser für Menschen, damit es ihnen leichter fällt, Entscheidungen zu treffen, die gut sind für die (digitale) Gesellschaft und es denjenigen, die es wünschen, ermöglichen, ihre Privatsphäre zu wahren.

Marit Hansen
Unabhängiges Landeszentrum für Datenschutz

Marit Hansen ist Diplom-Informatikerin. Seit 2008 ist sie die stellvertretende Landesbeauftragte für Datenschutz Schleswig-Holstein und damit auch stellvertretende Leiterin des Unabhängigen Landeszentrums für Datenschutz (ULD). Dort leitet sie den Bereich »Projekte zu technischem Datenschutz« und das Innovationszentrum Datenschutz & Datensicherheit (ULD-i).

5. IT-GRUNDVERSORGUNG ALS STAATLICHE AUFGABE

Fragt man aus einer rechtlichen Perspektive nach der Daseinsvorsorge, so rückt herkömmlich der Staat als zentraler Akteur in den Mittelpunkt. Die moderne Konzeption der Leistungsverwaltung wird üblicherweise mit den Arbeiten von Ernst Forsthoff ab den 1930er Jahren verknüpft. Sein revolutionärer Ansatz bestand darin, den Blick auf die strukturellen Bedingungen menschlichen Lebens im modernen Staat zu richten, und diesen Staat insoweit in die Pflicht zu nehmen. Der historisch belastete Nukleus – der Stichwortgeber hatte schon im Jahre 1933 affirmativ den »totalen Staat« rechtswissenschaftlich besungen – war kein Hindernis für den Siegeszug, den diese Idee nach dem zweiten Weltkrieg antreten konnte.

Befreit man das Konzept der Daseinsvorsorge von seinen paternalistisch-völkischen Verzerrungen, so offenbart sich eine zeitlose Idee: Der moderne Staat ist kein reiner Nachtwächterstaat, er verbietet nicht »in seiner majestätischen Gleichheit dem Reichen wie dem Armen, unter den Brücken zu schlafen, auf Straßen zu betteln und Brot zu stehlen« (Anatole France) – sondern er begreift es als seine Aufgabe, öffentliche Einrichtungen für die Allgemeinheit bereitzustellen, die ansonsten für praktisch alle Bürgerinnen und Bürger unerschwinglich wären und überdies in kollektiver Weise erheblich effizienter erbracht werden können: Verkehrs- und Beförderungswesen, Gas-, Wasser-, und Elektrizitätsversorgung, Müll- und Abwasserbeseitigung, Bildungs- und Kultureinrichtungen, Krankenhäuser, Friedhöfe und Bäder sind klassische Beispiele.

Daseinsvorsorge im Informationszeitalter

Welche Einrichtungen in diesem Sinne der Daseinsvorsorge zuzurechnen sind, unterliegt einem ständigen Wandel. Dieser wird einerseits durch technische, andererseits durch gesellschaftliche Innovationen hervorgerufen. Im Informationszeitalter trifft beides zusammen: Neue Informations- und Kommunikationstechnologien eröffnen ungeahnte Chancen für individuelle und gesellschaftliche Kommunikation und ermöglichen innovative Wirtschafts- und Verwaltungsmodelle. In derartigen Modellen treten Bürgerinnen und Bürger dem Staat nicht als Untertanen, sondern als selbstbestimmte Individuen gegenüber, die völlig zu Recht mehr über staatliche Prozesse wissen und mehr an ihnen partizipieren wollen.

Ein modernes Konzept der Daseinsvorsorge muss also das Verhältnis von Bürger und Staat vom Kopf auf die Füße stellen. Das bedeutet nicht zwingend, dass der Staat selbst die Straßen der Informationsgesellschaft bauen muss. Wohl aber bedarf es eines Bewusstseins dafür, dass menschliche Bedürfnisse heutzutage die Teilhabe an Wirtschafts- und Verwaltungsprozessen einschließen, die in immer kürzeren Innovationszyklen im Internet neu entstehen.

Daran kann sich die spannende Frage anschließen, ob es gerade eine staatliche Aufgabe ist, diese Leistungen und Angebote zu Bürgerinnen und Bürgern zu bringen. Konzepte der Daseinsvorsorge sind notwendig mit dem jeweils vertretenen Staatsbild und der für richtig gehaltenen Staatsaufgabenlehre verknüpft. Man kann insoweit eher etatistisch argumentieren und den Staat direkt auf die Erbringung bestimmter Leistungen verpflichten – oder man proklamiert mit klassisch-liberalen Argumenten einen Rückzug des Staates und die Konzentration auf Kernaufgaben. Ein moderner Mittelweg besteht darin, wie in Art. 87f GG für Post und Telekommunikation, den Staat für die »Gewährleistung« angemessener und ausreichender Dienstleistungen in die Verantwortung zu nehmen.

Universaldienste als Voraussetzung bürgerlicher Teilhabe

Die Erfüllung dieser Verantwortung erfolgt in diesen Bereichen durch die Definition sogenannter »Universaldienste«. Dieses Konzept könnte in einer verallgemeinerten Form auch für andere Bereiche der elektronischen Daseinsvorsorge greifen: Was sind die Universaldienste der Informationsgesellschaft, ohne die eine Teilhabe der Bürgerinnen und Bürger am digitalen Leben nicht möglich, zumindest aber unzumutbar erschwert würde?

Diese Frage weist weit über den viel diskutierten Breitbandausbau hinaus und zielt auf wesentliche Transaktionsprozesse des E-Government, aber auch auf die Ermöglichung rechtssicherer und rechtsverbindlicher Geschäftsprozesse im E-Government. In diesem Sinne sind beispielsweise Identitätsinfrastrukturen wie der neue Personalausweis oder die De-Mail ebenso Teil einer elektronischen Daseinsvorsorge wie die mit ihnen verbundenen Rechtsfolgen. Auch mit der Bereitstellung staatlicher Informationen (Open Data) übernimmt der Staat Verantwortung für neue Geschäftsmodelle und informierte Bürgerinnen und Bürger, die mit den nunmehr zugänglichen Daten wirtschaftliche und gesellschaftliche Innovationen hervorbringen.

Wie weit die staatliche Verantwortung im Einzelfall reicht, bedarf der Aushandlung: Nicht alle meinungsbildenden Internetangebote benötigen eine Breitbandverbindung – es gibt aber auch datenintensive Anwendungen, in denen gesellschaftlich relevante Kommunikation stattfindet. Außerdem sollte sich der Staat so wenig wie möglich in die Frage einmischen, welche Inhalte tatsächlich gesellschaftlich relevant sind; andernfalls könnte ein wesentlicher Innovationstreiber des Internets – die Entwicklung »von unten« – in Gefahr geraten. Zu warnen ist überdies davor, dass sich der Staat im Bereich der elektronischen Daseinsvorsorge auf ein kommunikatives Existenzminimum zurückzieht. So wichtig es ist, den Pfändungsschutz oder die Berechnung der Grundsicherung an aktuelle Entwicklungen anzupassen, so wenig taugt diese Perspektive als Maßstab für den strategischen Umgang mit dem Problem einer IT-Grundversorgung.

Verkehrsregeln für IT-Infrastrukturen

Schlussendlich ist auf ein wesentliches, oft vernachlässigtes Element der Daseinsvorsorge hinzuweisen: Ebenso wie hergebrachte Infrastrukturen brauchen auch die Elemente der elektronischen Daseinsvorsorge gewisse »Verkehrsregeln«. So wie der Staat Vorgaben für das Verhalten im Straßenverkehr macht und ihre Verletzung ahndet, muss er auch im Internet für einen effektiven Schutz der Beteiligten, insbesondere vor Verletzungen ihrer Grundrechte, sorgen.

Der Staat der Informationsgesellschaft benötigt mündige, informierte, partizipierende Bürgerinnen und Bürger, die ohne Sorge um ihre Privatheit am digitalen gesellschaftlichen Leben teilhaben und dieses mit den Erfahrungen ihrer individuellen Lebenswelten bereichern. Der Staat kann sich diese Bürgerinnen und Bürger nicht schnitzen, und er sollte sie auch nicht durch einen digitalen Anschluss- und Benutzungszwang in E-Government Prozesse pressen. Er kann aber Verantwortung für die infrastrukturellen Voraussetzungen übernehmen und dem Einzelnen die Möglichkeit ihrer Nutzung garantieren. Die Akteure in Bund, Ländern und Kommunen sollten beides viel stärker als bisher als ihre Aufgabe begreifen.

Prof. Dr. Gerrit Hornung
Universität Passau

Gerrit Hornung studierte Rechtswissenschaften und Philosophie an den Universitäten Freiburg und Edinburgh mit anschließendem Referendariat in Hamburg. Er promovierte und habilitierte an der Universität Kassel und war von 2006 bis 2011 Geschäftsführer der dortigen Projektgruppe verfassungsverträgliche Technikgestaltung. Seit 2011 ist er Professor für Öffentliches Recht, IT-Recht und Rechtsinformatik an der Universität Passau und Sprecher des dortigen interfakultären Instituts für IT-Sicherheit und Sicherheitsrecht.

6. ÖFFENTLICHER RAUM 2.0: IT IM WANDEL

Informationstechnologien durchdringen immer mehr Lebensbereiche. Online sein, Inhalte teilen sind dabei heute bereits mehr als Trends. Sie werden zum Lebensgefühl, zu einer Erwartungshaltung der Bürgerinnen und Bürger. Dabei wird der Staat immer häufiger in der Verantwortung dafür gesehen, dass bestimmte IT-Infrastrukturen betrieben und für Interessierte verfügbar sind – und sicher, effizient und übergreifend funktionieren. Die Herausforderungen offenbaren 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 vielfältigen Erwartungen, die ein immer größerer Teil der Gesellschaft als aktive Nutzer öffentlicher Informationstechnologien an diese richtet und zunehmend als Anforderungen formuliert.

Diese Herausforderungen gilt es, am Gemeinwohl orientiert, proaktiv, neutral und kenntnisreich zu begleiten. Dabei wird immer wieder die überragende Bedeutung heutiger Informationstechnologien und digitaler IT-Netzinfrastrukturen deutlich. Sie werden für Wirtschaft und gesellschaftliche Teilhabe bereits heute zu einer kritischen 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. Diese öffentliche IT ist also weit mehr als Hard- und Software von Behörden. Öffentliche IT bezeichnet vielmehr die Informationstechnologien im öffentlichen Raum, respektive die IT, auf der dieser Raum aufsetzt. Der Begriff des öffentlichen Raumes war ursprünglich stark geographisch geprägt, synonym zu verstehen mit einem Markt- oder Kirchplatz. Ein solch geographisch geprägtes Bild des öffentlichen Raumes ist aber heute nicht mehr zeitgemäß. So erfüllt der öffentliche Raum nicht nur städtebauliche Funktionen, sondern dient darüber hinaus als Ort des sozialen, wirtschaftlichen und politischen Austausches auch und gerade im virtuellen Raum. So steht die IT im öffentlichen Raum, ob privatwirtschaftlich oder staatlich betrieben, immer mehr unter der Verantwortung des Staates bzw. unter seinem besonderen Schutz. Wie weit diese Verantwortung reicht, reichen soll bzw. reichen muss und unter welchem besonderen Schutz diese öffentliche IT steht, diese Fragen erfordern eine proaktive Diskussion über eine innovations- und kommunikationstreibende, übergreifende öffentliche IT in Deutschland.

Betrachtet man also IT im öffentlichen Raum nicht mehr als eine jeweils voneinander abgetrennte anwendungsspezifische Infrastruktur, sondern als eine übergreifende Gesamtinfrastruktur mit gleichen oder zumindest ähnlichen Basiskomponenten, so wird sehr schnell deutlich, dass man über Domänen hinweg vor identischen Herausforderungen steht. Ob in der Anwendungsdomäne Energie, wo langfristig von der Stromproduktion bis zum Endgerät alle relevanten Netzknoten in ein intelligentes Stromnetz (Smart Grid) integriert werden sollen, oder im Bereich der intelligenten Verkehrs- und Transportsysteme, wo Informations- und Kommunikationstechnologien im Straßenverkehr, einschließlich seiner Infrastrukturen, Fahrzeuge und Nutzer, sowie beim Verkehrs- und Mobilitätsmanagement und für Schnittstellen zu anderen Verkehrsträgern bereits heute eingesetzt werden – überall geht es um Verfügbarkeit, Sicherheit, Datenschutz und Handhabbarkeit.

Öffentliche IT wird zukünftig in unserem öffentlichen Leben eine wachsende Rolle spielen, so dass neue Anforderungen auf die öffentliche Hand zukommen:

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. Teile der von Staat, Kommunen und anderen öffentlichen Einrichtungen betriebenen oder beauftragten IT-Infrastruktur bilden eine wesentliche Basis öffentlicher IT.

– Öffentliche Daten und IT-Infrastrukturen sind leicht zugänglich und können durch staatliche, privatwirtschaftliche oder private Stellen bereitgestellt werden.

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 damit 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. Datenschutz und informationelle Selbstbestimmung sind wesentliche Elemente.
– 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 IT offen zu denken. Bislang war IT sehr stark mit organisatorischen Grenzen assoziiert. Öffentliche IT eröffnet aber die Möglichkeit bestimmte Technologien als Basiskomponenten für ein anwendungsübergreifendes Miteinander zu begreifen und Technik und Organisation voneinander zu trennen. Ressortgrenzen und gemeinsamer Betrieb von Anwendungen sind kein Gegensatz, sondern können helfen Kosten zu sparen, Herausforderungen von Interoperabilität und Standards zu attackieren und leichteren Zugang für Bürgerinnen und Bürger zu schaffen. So rückt die Vision einer öffentlichen IT – vernetzt und sicher – ein Stückchen näher.

Jens Fromm
Kompetenzzentrum Öffentliche IT (ÖFIT)

Jens Fromm leitet das Kompetenzzentrum Öffentliche IT (ÖFIT) am Fraunhofer-Institut FOKUS. Als Leiter des durch das Bundesministerium des Innern geförderten Kompetenzzentrums beschäftigt er sich insbesondere mit den Themengebieten öffentliche IT, E-Government, IT-Infrastrukturen, elektronische Identitäten und Interoperabilität. Zusätzlich leitet er das Common Criteria Certification Lab am Fraunhofer FOKUS, das Zertifizierungsverfahren unter Aufsicht des BSI begleitet.

GEFÖRDERT VOM

Bundesministerium
des Innern

:C) =O =)

:/ :O(:C

XP ;-P ;)

=D X(:>

:-O :(-:

=P C", :]

KONTAKT

Jens Fromm
Leiter Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
info@oeffentliche-it.de

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

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

CC BY

kre | 1405 (Grafik: Fraunhofer FOKUS)