Fraunhofer
FOKUS

FRAUNHOFER-INSTITUT FÜR OFFENE KOMMUNIKATIONSSYSTEME FOKUS

PUBLIC IOT – DAS INTERNET DER DINGE IM ÖFFENTLICHEN RAUM

IN KOOPERATION MIT DEN PARTNERN DES E-GOVERNMENT-LABORS

VERNETZTE OBJEKTE ERMÖGLICHEN
GENAUE ANALYSE, FLEXIBLE STEUERUNG
UND MEHR EFFIZIENZ.

VORWORT

Liebe Leserinnen und Leser,

in der verarbeitenden Industrie und der Logistik sind Objekte heute schon hochgradig digital vernetzt – man spricht daher vom *Internet of Things* (kurz: *IoT*), das hier Anwendung findet. Auch in der Heimautomatisierung werden die Waschmaschine oder die Heizung bereits vereinzelt per App von unterwegs abgefragt und gesteuert. Vernetzte Objekte und Prozesse bedeuten also neue Analyse- und Steuerungsmöglichkeiten, mehr Flexibilität und idealerweise mehr Effizienz. Noch weitgehend unbeachtet sind die Chancen und Aufgaben für Politik und Verwaltung, die durch vernetzte Objekte und die damit verbundenen neuen Datenflüsse entstehen.

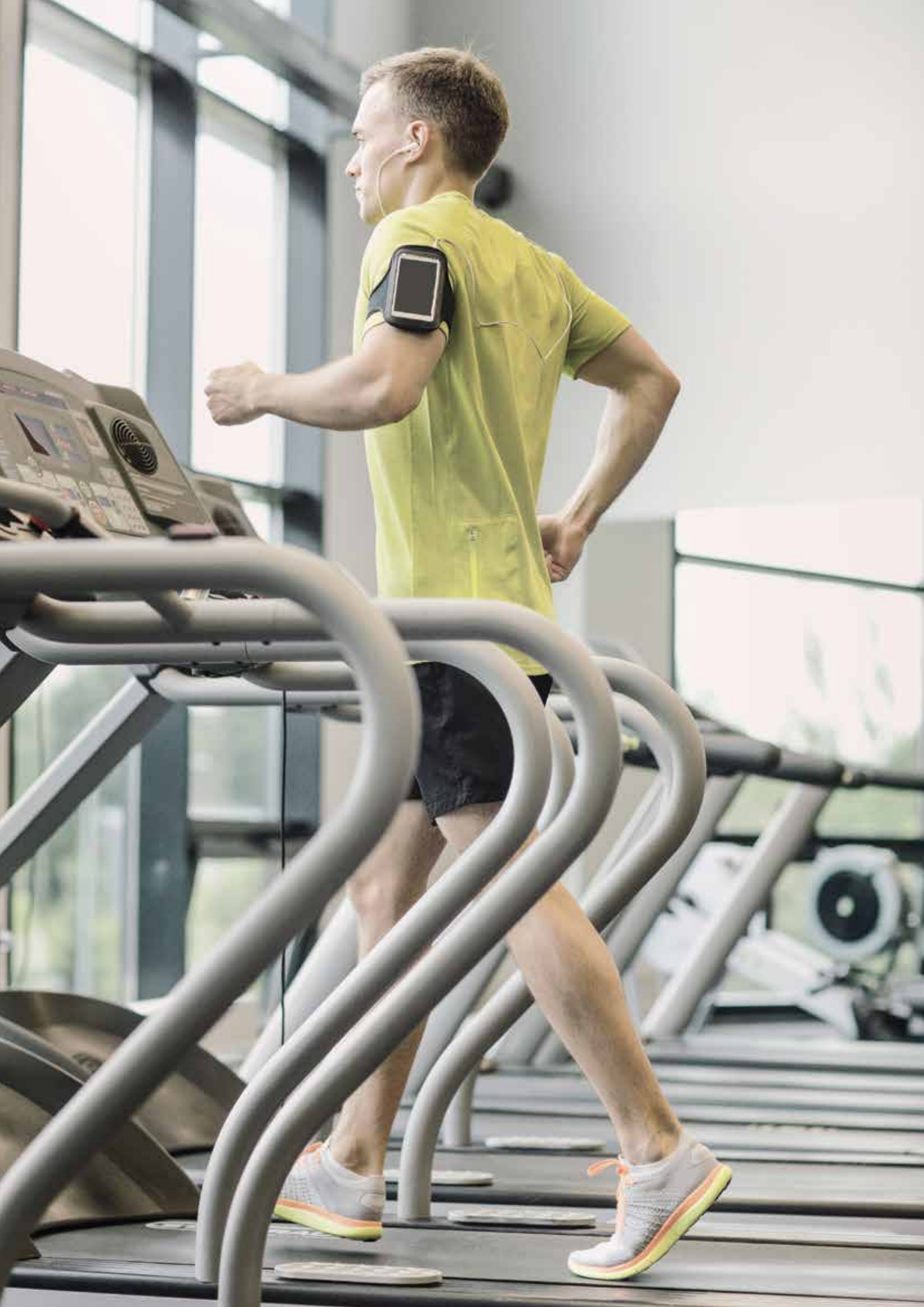
Die vorliegende Broschüre soll diese Lücke schließen und das Thema für den öffentlichen Sektor strukturieren, indem sie begriffliche Klarheit schafft, mögliche Einsatzgebiete aufzeigt und politische Handlungsfelder benennt. Die Inhalte sind in gemeinschaftlicher Arbeit von Fraunhofer FOKUS und Partnern des FOKUS eGovernment-Labors entstanden.

Eine interessante und aufschlussreiche Lektüre wünschen Ihnen

Dr.-Ing. Matthias Flügge

Jens Fromm

Leiter Geschäftsbereich Digital Public Services (DPS)
Fraunhofer-Institut FOKUS



INHALT

1. WAS IST PUBLIC IOT?

Unauffällig, aber nützlich ist das Internet der Dinge längst in unserem Alltag angekommen: An Bushaltestellen lassen sich die nächsten Abfahrtszeiten per NFC-Tags abfragen, Fahrstühle melden automatisch Ihren Wartungsbedarf und Schadstoffsensoren liefern in kurzen Intervallen ortsbezogene Daten zur Umweltbelastung. Vereinzelt wird auch die Parkraumbewirtschaftung schon mit Hilfe von Sensoren gesteuert oder die Leerung der Mülltonne nach dem tatsächlichen Füllstand veranlasst. Das *Internet of Things (IoT)*[1] beeinflusst gegenwärtige Entwicklungen massiv. Es hebt die Digitalisierung auf eine neue Stufe, indem es die Trennung zwischen physischer und digitaler Welt aufhebt. Physische Dinge werden mittels digitaler Repräsentation vernetzt. So kann ihr Zusammenwirken schneller, leichter und genauer analysiert, prognostiziert und aufgrund genau dieser Erkenntnisse optimiert und automatisiert werden. Diese optimierten Abläufe im virtuellen Modell können nun in der gegenständlichen Welt umgesetzt und dort tatsächlich wirksam werden. Wie so oft bei technischen Neuerungen ergeben sich dadurch aber auch neue Risiken und somit Aufgaben, die es zu lösen gilt.

1.1 ENTSTEHUNG DES INTERNET OF THINGS

Bereits im Jahr 1991 wurde der Begriff *Ubiquitous Computing,* die Allgegenwärtigkeit von Computern, durch Mark Weiser in seiner Arbeit über die Rechner des 21. Jahrhunderts[2] eingeführt. Weiser sagte die Ablösung damals typischer, schwergewichtiger Rechner durch eine große Anzahl kleiner, vernetzter und extrem leichtgewichtiger Rechner voraus. Im Jahr 1999 prägte Kevin Ashton[3] den Begriff des Internet of Things für Objekte der realen Welt, die über zugeordnete passive Codes oder aktive Computer-Chips eine digitale Identität erhalten und sich selbst mit dieser ausweisen können. Technologische Beispiele sind QR-Codes und RFID-Chips.

Der IoT-Begriff entwickelte sich nachfolgend dahingehend weiter, dass die Dinge auch untereinander bzw. mit dem Internet vernetzt sind und so Informationen über sich zur Verfügung stellen und austauschen können. Bei Vorhandensein entsprechender Sensoren können vernetzte Dinge auch Informationen über ihren Zustand an ihre Umgebung übermitteln bzw. diesen auf Anweisung über entsprechende Aktorik verändern. Physische und digitale Welt verschmelzen.

Schon früh wurde das Potenzial von IoT für die Logistik im Bereich der Überwachung und Steuerung von Lieferketten erkannt. Auch in anderen Domänen findet die neue Technologie zunehmend Anwendung. IoT hat bereits Einzug in private Bereiche, in die verarbeitende Industrie, ins Bauwesen, in die Agrarwirtschaft und in viele andere Felder gehalten. Das Zeitalter der smarten Dinge, Daten, Dienste und Systeme hat begonnen, und auch die Gesellschaft digitalisiert sich. Nutzer haben ebenso wie physische Objekte digitale Identitäten, übermitteln Informationen über ihr Verhalten und ihre Umgebung, erhalten mitunter sogar Aufforderungen zur Änderung ihres Verhaltens. Die technische Dimension von IoT wird um eine gesellschaftliche Dimension ergänzt. Heute findet man kaum einen Fachartikel zu dem Thema, in dem nicht beide angesprochen werden.

Aus einer technischen Perspektive bestehen die funktionalen Bestandteile von IoT vereinfacht gesagt aus den vernetzten Dingen selbst, der genutzten Kommunikationsinfrastruktur und Softwareanwendungen in der Cloud. Die Dinge erfahren eine Ausrüstung mit Sensoren zur Erfassung von

1 Im Folgenden wird der englische Begriff IoT *(in der Langform: Internet of Things)* verwendet. Diese Entscheidung wurde von den Autoren bewusst getroffen, da die Abkürzungsform IoT auch in der deutschsprachigen Fachwelt weit stärker etabliert ist als eine deutsche Übersetzung. Hieran orientiert sich dann auch die Entwicklung der Begriffe Public Internet of Things (Public IoT) und Internet of Public Things.

2 Weiser, Mark (1991): *The Computer for the 21st Century.* Verfügbar unter: http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html.

3 Ashton, Kevin (2009): *That 'Internet of Things' Thing. In the real world, things matter more than ideas.* Verfügbar unter: http://www.rfidjournal.com/articles/view?4986.

IM INTERNET OF THINGS VERSCHMELZEN DIE PHYSISCHE UND DIE DIGITALE WELT.

Informationen, mit Netzwerkkomponenten zur Übermittlung von Daten sowie Aktoren zur Steuerung. Bei der Kommunikationsinfrastruktur steht die Verwendung der IP-Protokoll-Familie im Vordergrund, um eine möglichst universell verwendbare Datenübertragung zu ermöglichen. Für effektives IoT muss aufgrund der Vielzahl der Dinge die aktuelle Version 6 des Internetprotokolls (IPv6) genutzt werden, denn nur hiermit lassen sich auch in einer Zukunft mit Milliarden von smarten Dingen unterschiedliche Adressen vergeben. Die physischen Dinge werden über standardisierte Schnittstellen (APIs, Gateways) mit Software-Systemen zur Verwaltung der Geräte und Daten verbunden. Die Aufgaben dieser Systeme sind u. a. die Verwaltung von Identitäten, die Übermittlung von Daten und Anweisungen oder auch eine Konvertierung zwischen den verschiedenen IoT-Protokollen bzw. Datenformaten. Auf einer höheren Abstraktionsebene befinden sich Komponenten zur Speicherung und Auswertung der Daten. Begriffe wie Data Warehouse, Big Data, Data Analytics oder Streaming Analytics lassen sich hier einordnen. Zunehmend kommen auch Ansätze des maschinellen Lernens zum Einsatz, die aus den Daten neue Muster und Gesetzmäßigkeiten erkennen. Domänenspezifische Anwendungen interpretieren und visualisieren die Auswertungsergebnisse und leiten Planungen, Entscheidungen und ggf. zugehörige Steuerbefehle ab.

Es lässt sich erkennen, dass IoT viele Trendthemen der heutigen Informatik umfasst und verbindet. Damit hat es an den Chancen dieser Themen teil, muss sich aber auch mit deren Risiken auseinandersetzen. So verwundert es nicht, dass IoT-Konzepte insbesondere im öffentlichen Raum[4] eng mit den von der Gesellschaft für Informatik identifizierten »Grand Challenges« der Informatik[5] verbunden sind. Ohne funktionale Sicherheit (Safety), Informationssicherheit (IT-Security), Vertrauen (Trust), aber auch ohne zugehörige Entwicklungs-, Test- und Betriebskonzepte wird IoT im öffentlichen Raum weder technisch umsetzbar sein noch Akzeptanz finden.

1.2 IMPLIKATIONEN FÜR DEN ÖFFENTLICHEN SEKTOR

Am deutlichsten spürbar ist die fortschreitende digitale Vernetzung zurzeit bei Dingen, die im privaten Bereich genutzt werden. Diese lassen sich meist der Konsum- und Unterhaltungselektronik oder der Haustechnik zuordnen. Unter den Begriff *Consumer IoT* fallen Anwendungen wie smarte TVs, das vernetzte Heim oder autonom fahrende Autos. Diese Geräte und zugehörige Anwendungen werden von privatwirtschaftlichen Unternehmen angeboten und von Privatpersonen genutzt. Dessen ungeachtet können diese Produkte Regulierungsbedarfe aufwerfen, für die der Staat Rechnung zu tragen hat.

Der gesamte Bereich des Consumer IoT stellt den Gesetzgeber vor große Herausforderungen der Regulierung. In der Flut erhobener, aggregierter und ausgewerteter Daten gilt es, Datenschutz, Datensouveränität und informationelle Selbstbestimmung der Verbraucher sicherzustellen. Dies gilt insbesondere dann, wenn personenbeziehbare Daten durch physische Objekte erzeugt und weitergeleitet werden. Beispielhaft für solche Objekte sind die zunehmend in Mode kommenden Wearables, etwa Smart Watches oder Fitnesstracker: Aus Sicht des Nutzers dienen diese Geräte der Optimierung des eigenen Sportprogramms. Soweit, so unkritisch. Doch die hier gesammelten Daten sind auch für Dritte interessant, bspw. für Anbieter der entsprechenden Applikationen oder für Krankenkassen, welche neuerdings Interesse zeigen, Fitnesstracker zu subventionieren. Das zeigt, dass weitergehende Datenverwendung bereits erfolgt oder aber zumindest angedacht ist. So werden z. B. Stimmen laut, die eine Berücksichtigung dieser

4 Fromm, Jens; Hoepner, Petra; Weber, Mike; Welzel, Christian (2014): *Öffentliche Informationstechnologie: Abgrenzung und Handlungsfelder*, S. 5.
5 Gesellschaft für Informatik e.V. (2014): *Die Grand Challenges der Informatik*. Verfügbar unter: http://www.gi.de/fileadmin/redaktion/Download/GI-Grand_Challenges-Brosch%C3%BCre2014.pdf.

FÜR STAAT UND VERWALTUNG ENTSTEHEN MIT DEM INTERNET OF THINGS NEUE GESTALTUNGSRÄUME, ABER AUCH NEUE VERPFLICHTUNGEN.

Daten in der Gesundheitsakte fordern. Technisch wäre es dann ein Leichtes, die Daten auch zur Bestimmung der Beitragshöhe heranzuziehen, indem sportliche Aktivitäten mit einem Bonus, Risikosportarten oder zu wenig körperliche Aktivität jedoch mit einem Malus belegt werden. Hier gilt es zu entscheiden, ob und inwieweit dies wünschenswert ist und gegebenenfalls reguliert werden muss.

Ein weiteres Beispiel sind Kfz-Versicherer, welche in Feldversuchen bereits anbieten, ihre Tarife abhängig vom Verhalten des Fahrers anzupassen. Möglich wird dies durch den Einbau einer Black Box im Kraftfahrzeug, welche Kennzahlen zum Fahrverhalten erfasst. Dies führt bereits heute zu lebendigen Diskussionen über die Rechtmäßigkeit und die mittelbaren Folgen der automatisierten Erhebung und Auswertung von bislang rein privaten Daten und Nutzungsprofilen für kommerzielle Zwecke. Auch in diesem Umfeld ist der Staat dazu angehalten, private und wirtschaftliche Interessen vor dem Hintergrund gemeinsamer Werte auszutarieren. Seine Gestaltungsmöglichkeiten reichen von der Aufforderung zur Selbstregulierung bis hin zum direkten Eingriff in Form einer gesetzlichen Regelung.

Nicht minder bedeutsam ist das Anwendungsfeld *Industrial IoT.* Regulierungsbedarfe gehen hier weit über die Förderung von Konzepten der Industrie 4.0 hinaus. Die digitale Vernetzung in und von industriellen Anlagen sowie der Austausch, die Auswertung und die Analyse von Daten für die branchenübergeifende Optimierung von Produktions- und Produktlebenszyklusprozessen eröffnen viele neue Möglichkeiten. Mit den anfallenden Daten ließen sich bspw. Berichtspflichten aus der Umweltgesetzgebung automatisiert erfüllen. Technisch ließe sich bei Verstößen aktiv eingreifen, indem etwa eine schadstoffemittierende Anlage durch die Regulierungsbehörde einfach abgeschaltet würde. Unternehmerische Freiheiten gilt es für ein solches Szenario ebenso zu diskutieren wie Fragen der IT- und Produktionssicherheit. Generell ist zu regeln, auf welchen Wegen und in welchem Umfang staatliche Stellen kontrollierenden oder gar steuernden Zugriff auf digital vernetzte Objekte erlangen und wahrnehmen können. Dies ist insbesondere für Bereiche erforderlich, in denen eine öffentliche Gewährleistungsverantwortung existiert. Man nehme z. B. eine Kommune, die das Funktionieren der Wasserversorgung sicherstellen muss. Macht es im Ernstfall, d. h. im Falle eines dringend erforderlichen Eingriffs in das System, einen Unterschied, ob die Versorgung durch private oder durch kommunale Unternehmen erfolgt?

Betrachtet man Vernetzungsansätze nicht isoliert, sondern im Sinne eines *Smart-City*-Konzepts, erhält die Idee von IoT im öffentlichen Raum eine übergreifende Bedeutung. Das Internet of Things ist ein technologischer Grundbaustein, wenn es darum geht, städtische Prozesse mit Hilfe von Vernetzung effizienter, umweltfreundlicher und sozial inklusiver zu gestalten. Die durchgängige Optimierung von städtischen Prozessen und in staatlicher Hoheit befindlichen Ressourcen über unterschiedlichste Domänen wie Verkehr, Umwelt und Energie hinweg kann nur mit einem ganzheitlichen Ansatz gelingen, der gleichermaßen (Echtzeit-)Daten von physikalischen Objekten des öffentlichen Sektors und von privat(wirtschaftlich)en Akteuren einbezieht.

1.3 BEGRIFFSBESTIMMUNG UND ABGRENZUNG

Die genannten Beispiele zeigen bereits, dass die Vernetzung physischer Objekte im Internet of Things vor Eigentumsverhältnissen nicht Halt macht. In der Smart City können gleichermaßen Daten aus kommunalen, staatlichen, persönlichen und privatwirtschaftlichen Sensoren verknüpft werden. Dies gilt in ähnlicher Form auch für Teile des Industrial IoT – insbesondere im Bereich der kritischen Infrastrukturen – und für Anwendungsszenarien des Consumer IoT. Grundlegend unterschiedlich sind dagegen die Anforderungen an den öffentlichen

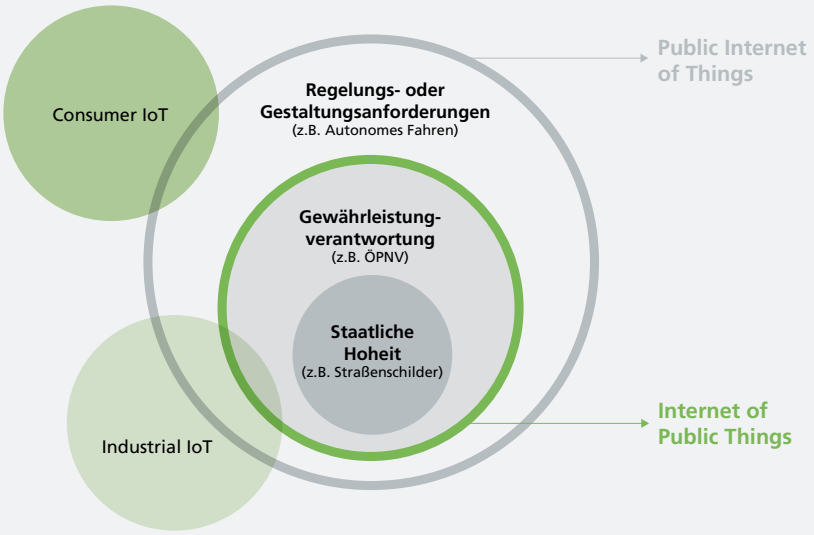


Abbildung 1: Ein- und Abgrenzung von Public IoT gegenüber verwandten Konzepten

Sektor, die etwa bei Konzeptionen wie *Smart Government*[6] Berücksichtigung finden. Zur Bestimmung eines spezifischen Beitrags des öffentlichen Sektors ist daher eine Abgrenzung zwischen dem speziellen *Internet of Public* Things und dem umfassenden *Public Internet of Things* sinnvoll.

Der enger gefasste Begriff *Internet of Public Things* umfasst jene physischen Dinge, die sich in staatlicher Hoheit oder Gewährleistungsverantwortung befinden und sich digital ausweisen können bzw. digital vernetzt sind. Die Vielfalt dieser Objekte ist bereits heute sehr groß. Sensoren findet man in öffentlichen Verkehrsmitteln, Brücken, Brandmeldern oder Hochwassermeldern, in Sicherungsanlagen z. B. von Gefängnissen, in den Sendeanlagen des öffentlichen Rundfunks und nicht zu vergessen im ganzen Umweltbereich, vom Seismografen über Wetterstationen bis zu Schadstoffsensoren in Städten.

Innerhalb der öffentlichen Verwaltung als dienstleistender Wissensorganisation hingegen sind physische Objekte mit Vernetzungspotenzial eher spärlich gesät. Positive Effekte (bessere Planungs- und Entscheidungsgrundlagen, effizientere Prozessgestaltung) sind vor allem dort mittelbar zu erwarten, wo der Datenaustausch zwischen vernetzten Dingen und den relevanten Fachverfahren automatisiert wird. Darüber hinaus bestehen die Handlungsbedarfe für die Kernverwaltung eher darin, die in staatlicher Hoheit befindlichen Dinge zu registrieren und zu katalogisieren. Beispielsweise existieren bereits heute digitale Baumkataster, die eine eindeutige Identifizierung von mit passiven RFID-Tags versehenen Bäumen mit Zusatzdaten wie Geolokation, Baumart und Zuständigkeit verknüpfen. Auch diese physischen Entitäten sind über ihre maschinenlesbaren Identitäten und Beschreibungen Teil des *Internet of Public Things*.

In vielen Bereichen des öffentlichen Lebens hat der Staat die Erfüllung öffentlicher Aufgaben an andere Akteure übertragen. Beispielsweise werden Energieversorgung, Abfallbeseitigung und Telekommunikation heute überwiegend von privatwirtschaftlichen Unternehmen betrieben und ausgebaut. Diesen Bereichen kommt, ungeachtet der privatwirtschaftlichen Leistungserstellung, eine herausragende Bedeutung für das Gemeinwesen zu, die sich aus unterschiedlichen Perspektiven mit Konzepten wie Daseinsvorsoge und kritischen Infrastrukturen begründen lässt. Die Bedeutung für das Gemeinwesen ist in der Gewährleistungsverantwortung von Staat und Kommunen begründet, die letztlich bis zur Eigenerstellung der erforderlichen Leistungen reicht. Auch wenn die Leistungen also aktuell von privaten Akteuren erbracht werden, rechtfertigen gesellschaftliche Bedeutung und öffentliche Gewährleistung eine besondere staatliche Eingriffstiefe. Oft liegen diesen Bereichen physische Infrastrukturen zugrunde, die aufgrund Ihrer Steuerungskomplexität und ihrer wechselseitigen Abhängigkeit ein hohes Potenzial für die digitale Vernetzung mit sich bringen.

Mit dem *Internet of Public Things* erschöpft sich, wie bereits angedeutet, die Rolle des öffentlichen Sektors im Bezug auf vernetzte Dinge jedoch keineswegs. Er ist auch Gestalter und Regulator und schafft Rahmenbedingungen für die Nutzung privater IoT-basierter Produkte und Dienstleistungen. Das gesamte Spektrum aus vernetzten Dingen in staatlicher Hoheit, unter Gewährleistungsverantwortung und mit Regelungs- und Gestaltungsanforderungen, lässt sich unter dem Begriff *Public Internet of Things (Public IoT)* zusammenfassen. Abbildung 1 verdeutlicht die Überlegungen.

Insgesamt ergibt sich somit für das Themenfeld Public IoT ein breites Handlungsspektrum, das von der Ausarbeitung von Strategien für die digitale Vernetzung von Dingen im öffentlichen Raum über die Bereitstellung und den Betrieb technischer IoT-Infrastrukturen bis hin zur Schaffung von regulatorischen Rahmenbedingungen reicht.

6 von Lucke, Jörn (2015): *Smart Government – Wie uns die intelligente Vernetzung zum Leitbild »Verwaltung 4.0« und einem smarten Regierungs- und Verwaltungshandeln führt,* Whitepaper, The Open Government Institute, Friedrichshafen.

2. ANWENDUNGEN VON PUBLIC IOT

Die zahlreichen Berührungspunkte und Wechselwirkungen mit dem öffentlichen Sektor zeigen, dass das Internet of Things entgegen verbreiteten Auffassungen kein rein technisches und wirtschaftliches Thema ist. Beispielhafte Anwendungen für ausgewählte Domänen machen das noch deutlicher und lassen auf die grundlegenden Querschnittsfunktionen von Public IoT rückschließen.

2.1 ÖFFENTLICHE SICHERHEIT

Im Bereich der Einsatzkräfte von Feuerwehr, Technischem Hilfswerk, Krankentransport, Polizei oder Katastrophenschutz werden bereits heute vielfältige informationstechnische Mittel eingesetzt. Sie dienen hauptsächlich zur Bereitstellung von Kommunikationsmöglichkeiten in Text, Ton und Video zwischen den beteiligten Einsatzkräften. In vereinzelten Szenarien, bspw. bei Großveranstaltungen, kann auch die Auswertung von Bewegungsdaten und Geoinformationen einen wichtigen Beitrag zur Sicherheit leisten. Durch IoT ergeben sich jedoch noch weitreichendere Möglichkeiten.

Ein Beispiel ist Sensorik, welche vorbeugend in Gebäuden, Straßen und Brücken installiert wird. Mit ihrer Hilfe werden drohende und akute Gefahren durch Verformung, Kälte, Hitze oder hohe Schadstoffkonzentrationen erkannt. Diese Gefahren können nicht nur lokal durch die Aktivierung von Warntafeln, sondern in erweiterten Szenarien auch geradewegs an die Einsatzkräfte gemeldet werden. Im Idealfall können Gefahren sogar durch frühzeitige Erkennung und sofortige Beseitigung der Gefahrenquellen vollständig beseitigt werden.

Zum anderen können IuK-Technologien, Sensoren und deren intelligente Vernetzung die Einsatzkräfte in ihrer Arbeit unterstützen und vor Verletzungen bewahren. Praktische Beispiele hierfür sind Smartphones mit speziell für den Einsatzzweck gestalteten Apps, die Nutzung einer mobilen Kommunikationszentrale für die Einsatzleitung vor Ort oder das Tragen von Kleidung, die den Träger mittels Sensorik z. B. vor Überhitzung und gefährlichen Gasen warnt. Wirken all diese Elemente zusammen, kann dieses System die Einsatzleitung automatisch auf lokale Gefahren aufmerksam machen und der Einsatzplan kann bei Bedarf angepasst werden.

Herausforderungen für Public IoT in diesen mobilen Einsatzszenarien sind die oft eingeschränkte Verfügbarkeit von Kommunikationsinfrastrukturen sowie die für Mensch und Technik problematischen Umgebungsbedingungen. Der Aufbau und die Aufrechterhaltung von Kommunikationswegen müssen daher weitestgehend automatisch erfolgen und diese müssen sich notfalls auch selbst reparieren können. Den Überblick über die Situation vor Ort zu bekommen und zu behalten, ist in Einsatzszenarien essenziell. Die Forschung beschäftigt sich daher auch mit vernetzten (teil-)autonom agierenden Maschinen wie Fahrzeugen, Robotern oder Drohnen, welche vor Ort helfen können, die Lage schnell akkurat einzuschätzen oder gefährliche Orte auch ohne menschliche Helfer zu erkunden.

2.2 VERKEHR

Im Personen- und Güterverkehr werden heute schon vielfach vernetzte Dinge eingesetzt, um Verkehrsflüsse zu messen und zu steuern. Auch im Parkraum-Management finden sich bereits Anwendungsbeispiele.[7]

Durch eine kontinuierliche Überwachung des Zustands und der Belastung der meist öffentlichen Verkehrsinfrastrukturen mittels Sensoren können Reparaturbedarfe frühzeitig identifiziert werden. Wenn eine Brücke aufgrund statischer Mängel oder eine Straße wegen Unterspülung nur eingeschränkt genutzt werden können, ließe sich dies bei der behördlichen Planung von Gefahrgut- und Schwerlasttransporten berücksichtigen. Mit Hilfe der kontinuierlichen Messung würden zudem hilfreiche Daten gewonnen, um eine dauerhafte

7 Beispiel Nizza: o. A. (2014): *Smarter parken.* Verfügbar unter: http://www.kommune21.de/meldung_18248_Smarter+parken.html.

NICHT NUR IM VERKEHRSBEREICH ERGEBEN SICH DURCH IOT VIELFÄLTIGE REGELUNGS- UND GESTALTUNGSANFORDERUNGEN.

Überlastung von Infrastrukturen zu vermeiden und Investitionen in Erhaltung, Ausbau oder Neubau langfristig einzuplanen.

Auch im Bereich der Verkehrsüberwachung und -lenkung, die teils staatlich (z. B. Verkehrsleitstellen) und teils in privater Trägerschaft (z. B. Verkehrsunternehmen) organisiert ist, entstehen für den öffentlichen Sektor durch seine Gewährleistungsverantwortung neue Handlungsfelder. So lassen sich intermodale Szenarien skizzieren, in denen Sensorinformationen aus Infrastruktur, Verkehrsmitteln, transportierten Gütern und Mobilfunknetzen zur Analyse von Verkehrssituationen beitragen. Diese Daten bilden die Grundlage zur besseren Auslastung der Verkehrsträger und zur Umleitung des Verkehrsflusses bei spontan auftretenden Störungen.

Im Verkehrsbereich ergeben sich durch IoT zudem vielfältige staatliche Regelungs- oder Gestaltungsanforderungen, wie die Diskussion um das autonome Fahren zeigt. Neben Grundsatzfragen wie der Regelung des Datenschutzes und Haftungsfragen im hochautomatisierten Fahrbetrieb sind die technischen Spezifika der Kommunikation autonomer Fahrzeuge untereinander und mit ihrer Umgebung weiter auszugestalten.

2.3 ENERGIE

Im Energiebereich geht der Trend weg von einer überschaubaren Anzahl großer Kraftwerke hin zu einer Vielzahl verteilter, kleinerer Kraftwerke. Die klassische Netztopologie vom Erzeuger zum Verbraucher wird grundlegend umgebaut. Dabei steigt die Komplexität des Netzbetriebs mit wachsender Zahl von Elektrizitätserzeugungsanlagen aus erneuerbaren Energiequellen erheblich. Sie erzeugen die Energie nämlich nicht bei Bedarf, sondern in Abhängigkeit von äußeren Faktoren wie Sonnenschein, Windstärke oder Gezeiten. Da die Speicherkapazitäten bei Erzeugern und Netzbetreibern im Vergleich zur Gesamtenergiemenge sehr gering sind, kann der überschüssige Strom das Netz aus dem Gleichgewicht von Erzeugung und Verbrauch bringen. Ein Ausweg aus dieser Problematik kann sein, dass potenzielle Verbraucher über das Vorhandensein überschüssiger Energie informiert und so zu deren Nutzung oder Speicherung motiviert werden. Dies kann z. B. durch günstige Strompreise bei hohem Angebot erfolgen oder durch hohe Preise, wenn die Nachfrage das Angebot zu übersteigen droht. Um derartige Szenarien zu ermöglichen, müssen Angebot und Nachfrage kontinuierlich abgeglichen und unter Beachtung von vorhandenen Übertragungsmöglichkeiten, Netzkapazitäten und technischen Wechselwirkungen ausbalanciert werden.

Das dafür erforderliche System zur Erfassung von Angebots- und Nachfragedaten stellt ein anspruchsvolles Beispiel für Public IoT unter Berücksichtigung technischer und marktwirtschaftlicher Aspekte dar. Gerade im Zusammenspiel mit E-Mobility und der Nutzung von IoT im Verkehr lassen sich interessante Nutzungsszenarien entwickeln, bei denen etwa Elektrofahrzeuge als Stromspeicher in nachfragearmen Zeiten dienen. Gleiches gilt auch für die Ausgestaltung von Smart-Home-Szenarien, in denen die Stromnachfrage in Teilen zeitlich und angebotsabhängig gesteuert werden kann. Mit der sukzessiven Einführung von intelligenten Stromzählern, sogenannten *Smart Metern,* wird eine technische Voraussetzung dafür geschaffen. In beiden Fällen ist jedoch die Harmonisierung von Technik und rechtlich abgesicherten Geschäftsmodellen zu beachten.[8]

2.4 UMWELT UND BAUEN

Besonders hohe Verwaltungsaufwände entstehen in Domänen wie Umwelt, Bau oder Agrarwirtschaft durch eine Vielzahl von Regeln, deren Einhaltung gegenüber öffentlichen Stellen dokumentiert werden muss. So gibt es Grenzwerte für

8 Bundesministerium für Wirtschaft und Energie (2015): *Förderprogramm »Schaufenster intelligente Energie - Digitale Agenda für die Energiewende« (SINTEG).* Verfügbar unter: http://www.bmwi.de/DE/Themen/Energie/Netze-und-Netzausbau/sinteg.html.

Industrieabwässer, für die Emission von Treibhausgasen oder für die Bodenqualität landwirtschaftlicher Nutzflächen. Auch die Statik von Bauwerken, das Funktionieren von Brandschutzeinrichtungen in Gebäuden oder die Störfreiheit technischer Anlagen in kritischen Infrastrukturen müssen regelmäßig überprüft und gemeldet werden. Schon heute entstehen durch vernetzte Geräte diverse Daten, die für solche Meldungen relevant sind. Wasserversorger und emissionsreiche Industrien messen in kurzen Intervallen Stoffkonzentrationen, um die Einhaltung staatlich definierter Grenzwerte zu überprüfen. Durch eine automatische Übermittlung solcher prüfrelevanter Daten an entsprechende Fachverfahren in den Behörden lassen sich automatisch Bescheide oder Bußgelder für Grenzwertüberschreitungen erstellen. Große Skalenwirkung entfaltet diese Automatisierung dort, wo überschneidende Meldepflichten gegenüber mehreren Stellen notwendig sind und redundante Meldungen reduziert werden können.

Im privaten Umfeld gibt es erste Feldversuche in der Entsorgung: Mülltonnen erkennen über Sensoren Ihren Füllstand und kommunizieren diesen an den Entsorgungsbetrieb, der damit wiederum die Müllabfuhrrouten bedarfsgerecht optimiert.

Das Potenzial der digitalen Vernetzung geht aber über die reine Automatisierung von Prüfungen hinaus. Kontinuierliche Datenerfassung und -auswertung lassen es auch zu, Veränderungsprozesse (bspw. abnehmende Wasserqualität) und Gefahrensituationen (bspw. veränderte Statik eines Gebäudes) einschließlich eventueller Ursachen frühzeitig zu erkennen und präventive Gegenmaßnahmen einzuleiten. Anhand von Entwicklungsprognosen können zudem Folgekosten für verschleppte Investitionen simuliert werden. Dies ermöglicht eine weitsichtigere Planung für den Einsatz von Investitionsmitteln.

2.5 GESUNDHEITSWESEN

In nahezu allen Bereichen des Gesundheitswesens lassen sich die Potenziale von IoT erkennen. Dabei geht es nicht nur um Logistikverbesserungen für medizinische Verbrauchsgegenstände. Insbesondere Geräte, die Vitaldaten erfassen, visualisieren oder in anderer Form aufbereiten, bringen viele Möglichkeiten für die digitale Vernetzung mit sich. Aktuell sind diese Geräte aufwendig in technische Insellösungen für spezifische Anwendungen eingebunden. In einem krankenhausinternen »Intranet of Things« wäre es hingegen möglich, isolierte Datenströme der Medizintechnik miteinander zu vernetzen und für eine Vielzahl weiterer Anwendungen, bspw. die klinische Forschung, wiederzuverwenden.

Ein weiterer Bereich, in dem IoT weitreichende Änderungen mit sich bringen wird, ist die Prävention und Nachsorge im häuslichen Umfeld. Nicht-medizinische Lifestyle-Produkte können auch unmittelbar in medizinische Tele-Monitoring-Lösungen eingebunden werden. So wird die Nutzung patienteneigener Personenwaagen und Smartphones für die telemedizinische Betreuung von schwer herzinsuffizienten Patienten möglicherweise manch heute verwendete Spezial-Hardware ersetzen. Um diese Integrationsmöglichkeiten zu schaffen, sind jedoch noch einheitliche interoperable Schnittstellen und Datenformate zu erarbeiten. Zudem entstehen Fragen zur Qualität und Zertifizierung der genutzten Geräte. Klar ist, dass nicht alle Smart Wearables als Medizinprodukte geeignet sind.

Abbildung 2: Fachdomänen übergreifende Querschnittsfunktionen von Public IoT

2.6 MESSEN, AUTOMATISIEREN, OPTIMIEREN, VORAUSSCHAUEN, STEUERN

Die Breite der Anwendungsfelder von Public IoT kann hier keinesfalls erschöpfend dargestellt werden. Die wenigen aufgeführten Beispiele zeigen jedoch bereits die grundlegenden Querschnittsfunktionen von Public IoT auf (Abbildung 2).

Die kontinuierliche, automatisierte **Messung** von Kennzahlen erlaubt die Überprüfung von Dingen und Infrastrukturen wie öffentlichen Gebäuden und Verkehrswegen. Durch Vernetzung und Sensorik kann die Erhebung von Kennzahlen deutlich effizienter und dadurch engmaschiger erfolgen. Kosten durch manuelle Kontrollen und zu spät erkannte Schäden werden reduziert.

Durch die Nutzung von Echtzeitinformationen wird die **Automatisierung** von Prozessen erleichtert. Beispielsweise kann durch die automatische Initiierung von Warnungen bei hohen Schadstoffkonzentrationen deutlich schneller und effektiver auf sich verändernde Rahmenbedingungen im öffentlichen Raum reagiert werden.

Eine **Optimierung** der Verteilung von Lasten, der Auslastung von Kapazitäten und der Nutzung von verfügbaren Ressourcen in öffentlichen Infrastrukturen wird durch die Dynamisierung zuvor statischer Regelkreise erreicht. Der über Sensorik erhobene Zustand vernetzter Dinge dient dabei als Grundlage, um mittels Aktorik Einfluss auf den Zustand anderer Objekte zu nehmen.

Durch die gezielte Analyse erhobener Daten, die vernetzte Objekte im öffentlichen Raum in großer Menge liefern, können zudem bislang unbekannte Zusammenhänge und Abhängigkeiten erkannt und **Prognosen** getroffen werden, die Entscheidungen besser fundieren und vorausschauendes und ganzheitlich orientiertes Handeln vereinfachen.

Public IoT kann damit auch ein Instrument der politischen **Steuerung** werden. So liefern durch IoT erhobene Massendaten eine Entscheidungsgrundlage für die Anpassung rechtlicher Regelungen. Diese wiederum können mittels IoT parametrisiert und dynamisiert werden. So wird es technisch möglich, die Kfz-Besteuerung direkt an den real gemessenen – dem Fahrverhalten entsprechenden – Schadstoffausstoß zu koppeln.

Wie auch schon die anderen Funktionen sind derartige Steuerungsszenarien kritisch zu diskutieren. Einerseits: Indem Regulierung dynamisch angepasst erfolgt, wird sie effektiver und die Steuerungsinstrumente können dennoch transparent gemacht werden. Andererseits: Je stärker Kontrolle und Sanktionierung zeitlich zusammentreffen, je mehr auf Personen beziehbare Daten erhoben und ausgewertet werden, desto stärker ergibt sich eine Überwachungskulisse, die sich einschränkend auf die gefühlte und tatsächliche persönliche Freiheit von Bürgerinnen und Bürgern auswirken kann.

3. HANDLUNGSFELDER FÜR DEN ÖFFENTLICHEN SEKTOR

Aus den zuvor skizzierten Anwendungen und Querschnittsfunktionen von Public IoT lassen sich zahlreiche Handlungsfelder für den öffentlichen Sektor erkennen, von denen vier hier schlaglichtartig dargestellt werden sollen: 1) IoT hebt die Digitalisierung auf eine neue Stufe, die eine breite Auseinandersetzung mit ihren Chancen und Risiken erforderlich macht: als gesamtgesellschaftlicher Diskurs ebenso wie als Positionsbestimmung von Politik, Verwaltung und anderen öffentlichen Einrichtungen. 2) In nahezu allen IoT-Szenarien sind Datenschutz-Fragen relevant, für deren Beantwortung der Staat die Leitplanken und den rechtlichen Rahmen setzen muss. 3) Die Vielfalt an technischen Lösungsoptionen zeigt die Notwendigkeit für Standardisierungsaktivitäten auf, die der öffentliche Sektor nicht nur grundsätzlich unterstützen sollte, sondern in die er seine spezifischen Bedarfe dediziert einbringen muss. 4) Staat und öffentliche Verwaltung haben zudem ihren Teil dazu beizutragen, dass leistungsfähige technische Infrastrukturen für IoT-Anwendungen im öffentlichen Raum be- bzw. entstehen.

3.1 POSITION BESTIMMEN UND DISKURS ANSTOSSEN

Mit den neuen Möglichkeiten durch Public IoT wachsen auch die Risiken. So stellen sich Fragen nach der eigenen Nutzung und den notwendigen Beschränkungen gleichermaßen für jede einzelne Person wie auch für die Gesellschaft und ihre funktionalen Bereiche – und damit auch für Politik und Verwaltung. Dabei liegt der wesentliche Unterschied zu früheren Phasen der Digitalisierung in der auch theoretisch kaum noch gegebenen Exit-Option. Lässt sich der heimische PC einfach abstellen, fällt dies bei vernetzten Alltagsgegenständen ungleich schwerer. In Bereichen wie Consumer IoT besteht noch eine – zumindest theoretisch – ausgeprägte Wahlmöglichkeit, bspw. ein vernetztes oder klassisches Haushaltsgerät zu erwerben. Im Public IoT besteht diese Wahlfreiheit nicht in gleicher Weise, wenn etwa der Smart Meter für die Stabilität der Energieversorgung unerlässlich ist. Es gilt daher, sich mit dem entstehenden Gestaltungspotenzial frühzeitig auseinanderzusetzen, Chancen und Stärken zu erkennen sowie Risiken und Gefahren ernst zu nehmen und angemessen zu bewerten.

Staat und Verwaltung stehen zunächst vor der Aufgabe, die eigene Position zu bestimmen. Dabei muss ebenso nach der Effizienz und Effektivität neuer Lösungen gefragt wie auch ihre Angemessenheit vor dem Hintergrund der Risiken bewertet werden. Hierzu braucht es innerhalb der Organisationen den notwendigen Freiraum und auch die Abstimmung der Interessen und Vorstellungen zwischen den beteiligten Institutionen. Staat und Verwaltung sind keine monolithischen Akteure, und divergierende Sichtweisen etwa zur Zweckbindung von erhobenen Daten gilt es zu identifizieren und zusammenzubringen.

Diese eher nach innen gerichtete Positionsbestimmung sollte durch einen breiten politischen und gesellschaftlichen Diskurs über die Grenzen von Public IoT flankiert werden. Mit Industrie 4.0 und Arbeit 4.0 ist bereits in zwei Politikfeldern eine öffentliche Debatte über grundlegende gesellschaftliche und wirtschaftliche Veränderungen durch das Internet of Things im Gange. Der gesellschaftliche Diskurs ist nun um den Aspekt zu erweitern, dass Staat und Verwaltung künftig selber stärker die Möglichkeiten von IoT nutzen werden. Zielsetzung muss es sein, Folgebetrachtungen auf eine breitere Basis zu stellen, die Akzeptanz für sinnvolle Lösungen zu stärken und Grenzen zu identifizieren. Die Spannungsfelder, die sich dabei abzeichnen, wurden bereits bei der obigen Betrachtung der Beispiele deutlich. Wie lassen sich Datensparsamkeit und Zweckbindung der Datenverarbeitung gewährleisten, wenn vernetzte Datenbestände sogar Rückschlüsse auf diejenigen erlauben, über die gar keine Daten direkt gesammelt werden? Wo und wann wird die – womöglich äußerst effektive und effiziente – Überwachung gesetzlicher Regelungen anhand von Echtzeitdaten zu einem Eingriff in die individuelle Freiheit von Bürgerinnen und Bürgern?

STAAT UND GESELLSCHAFT SOLLTEN SICH MIT DEM ENTSTEHENDEN GESTALTUNGSPOTENZIAL DURCH IOT FRÜHZEITIG AUSEINANDERSETZEN.

Für Staat und Verwaltung geht es letztlich um die Unterstützung und um die aktive Teilnahme an gesamtgesellschaftlichen Diskursen über Möglichkeiten und Grenzen der Digitalisierung. Gelten die Herausforderungen für den Bereich Public IoT aufgrund der eingeschränkten Exit-Option in verstärkter Weise, lassen sie sich in vergleichbarer Weise in anderen Bereichen der Digitalisierung ausfindig machen. Die Bereitwilligkeit, mit der digital vernetzte Dinge aktuell bereits genutzt werden, zeigt den bestehenden Regulierungsbedarf auf. Den Ängsten vor einem Überwachungsstaat gilt es ebenso zu begegnen wie den Risiken gläserner Konsumenten bei einzelnen Unternehmen. Die gegenwärtige Diskussion um die Entwicklung und spätere Verwendung autonomer Waffensysteme zeigt, dass die potenziellen Bedrohungslagen keinesfalls auf virtuelle Welten begrenzt bleiben und die Diskurse nicht zuletzt auch grundlegende moralische Fragen zu behandeln haben.

3.2 DATENSCHUTZ GESTALTEN UND GEWÄHRLEISTEN

Es ist klar geworden: Das Internet of Things ist eine Datenerhebungs- und -korrelationsmaschine. Personenbezogene Daten, d. h. Daten, für die sich ein Bezug zu einer konkreten Person herstellen lässt, werden durch den Gesetzgeber besonders geschützt. Maßgeblich ist die neue Datenschutzgrundverordnung der Europäischen Union (EU-DSGVO), die das Datenschutzrecht in den Mitgliedsstaaten vereinheitlichen soll. Datensouveränität und Datenschutz sind dabei Grundbedingungen, die die Mitgliedsstaaten durchsetzen müssen. So ist z. B. sicherzustellen, dass für die weitere Nutzung personenbezogener Daten eine Einwilligung vorliegt und zudem die Datensicherheit beim Anbieter einer Anwendung nachvollziehbar ist. Diese Thematik berührt insbesondere auch den grenzübergreifenden Datentransfer und die Durchsetzung internationaler Datenschutzabkommen.

Die Grundsätze der Zweckbindung und Datensparsamkeit schließen das Sammeln von personenbezogenen Daten unter der bloßen Mutmaßung der späteren Verwendung aus. Die informierte Einwilligung zur Erhebung persönlicher Daten kann durch die betroffene Person jederzeit widerrufen werden. Dieser Grundsatz wird durch umfangreiche Auskunfts- und Informationspflichten ergänzt. Weiterhin sieht die EU-DSGVO ein Recht auf Löschung und ein Recht auf Datenportabilität vor.

Für IoT im öffentlichen Raum ergeben sich aus den Datenschutzbestimmungen grundlegende Herausforderungen. Fraglich ist, ob das Grundprinzip »Privacy by design and by default« angewendet werden kann und selbst bei perfekter technischer Umsetzung den rechtlichen Anforderungen genügt. Um die Tragweite aufzuzeigen, ist ein Vergleich zu den Herausforderungen, die sich bei Cloud Computing oder Big Data ergeben, zielführend. Der Personenbezug von im IoT erhobenen Daten ist weit weniger eindeutig als bei anderen Daten. So geben bspw. Fahrzeugdaten sehr schnell Informationen zum Fahrer preis, wenn das Fahrzeug nur von einer Person genutzt wird. Bei mehreren Nutzern lässt sich ein Personenbezug durch die Verknüpfung mit anderen, möglicherweise frei zugänglichen Daten schnell herstellen. Dieser mittelbare Personenbezug kann einer Wahrnehmung des Rechts auf informationelle Selbstbestimmung entgegenstehen. Bei enger Auslegung dürften entsprechend kaum Daten als gänzlich personenbezugsfrei gelten, bei weiterer Auslegung lässt sich das Recht auf informationelle Selbstbestimmung kaum mehr wahrnehmen. Ein Opt-out ist schwerlich möglich, da IoT-Systeme außerhalb des eigenen Einflussbereichs kontinuierlich personenbeziehbare Daten sammeln.

In diesem Zusammenhang ist auch das Thema anonymisierter Persönlichkeitsprofile zu betrachten: Betreiber von auf IoT-Technologien beruhenden Diensten verwenden spezielle Algorithmen, um Personenbezüge zu entfernen, ohne dabei jedoch Datenattribute zu verlieren, die eine Verwendung der so anonymisierten Daten zur Erstellung von Personenprofilen

erlauben. Solche Profile werden zur Optimierung der erbrachten Dienstleistungen und vielfach auch zur Erzeugung von interessenbezogener Werbung genutzt. Inwieweit und unter welchen Bedingen eine solche Verwendung rechtskonform ist, sollte Gegenstand eines gesellschaftlichen Diskurses und juristischer Analysen sein. Um Auskunfts- und Löschungsrechte zu gewährleisten, muss der Personenbezug von Nutzerdaten allerdings eindeutig sein.

Auch aus dem Recht auf Datenportabilität entstehen weitere technische Herausforderungen: Persönliche Daten müssen hersteller- und betreiberunabhängig von einem System unter Verwendung gängiger Formate und Protokolle auf ein anderes übertragbar sein. Insbesondere sind hierfür standardisierte, offene Schnittstellen notwendig, die gegen nicht autorisierten Zugriff gesichert sind.

3.3 STANDARDISIERUNG UNTERSTÜTZEN

Standardisierungsbestrebungen zum IoT gibt es mehr als genug, es fehlt jedoch eine Harmonisierung der Arbeiten von unterschiedlichen Gremien. Wie ausgeführt, kann IoT nicht als isolierte Entwicklung betrachtet werden, sondern umfasst unterschiedlichste Trendthemen wie Cloud- und Fog-Computing, Big Data (Analytics), M2M, (Complex) Event Processing und Security. In diesen Teilbereichen liegen die Herausforderungen nicht in der Entwicklung neuer Standards, sondern vielmehr darin, existierende Standards in eine IoT-Referenzarchitektur einzupassen und ggf. IoT-bezogen zu profilieren. Wie bei jedem anderen Standard ist dabei die Frage zu beantworten, wieso in genau diesem Gebiet ein Standard benötigt wird und was mit diesem Standard erreicht werden soll. Auch hier hilft eine Referenzarchitektur weiter, die aufzeigt, welche internen und externen Schnittstellen eines IoT-Systems existieren, an denen Interoperabilität erforderlich ist.

Eine spezifische Eigenschaft von IoT ist seine Erweiterbarkeit. Zum Zeitpunkt der Realisierung steht zumeist noch nicht fest, welche Sensoren und Aktoren während des Betriebs Bestandteil eines Gesamtsystems sein werden. Die Schnittstellen zu diesen einzubeziehenden Dingen müssen daher standardisiert und die Identifikation der Dinge eindeutig sein. So ist es nicht verwunderlich, dass Organisationen wie ISO und DIN unter dem Schlagwort »Automatic Identification and Data Capture – AIDC« im SC31[9] ebenso wie das Europäische Institut für Normung CEN im TC 225 die Standardisierung der Identifikation der smarten Dinge vorantreiben. Domänenspezifische Standards wie »IoT im Bereich Logistik« werden im ISO TC 122 behandelt. Das ISO/IEC JTC1 versucht seit 2015, die Vielzahl der bereits existierenden Standards zu strukturieren. In einer ersten Bestandsaufnahme wurden dazu über 400 relevante Standards und über 20 Referenzarchitekturen und Frameworks von Organisationen wie ISO, IEC, ITU, W3C, OMG, OGC, 3GPP, GS1, OMA, ETSI oder IEEE identifiziert. Wie bei anderen Trendthemen verfolgt das ISO/IEC JTC1 den Ansatz, das Thema mittels der Identifikation typischer Anwendungsfälle, der Definition eines spezifischen Vokabulars, der Durchführung einer Gap-Analyse, der Betrachtung von Sicherheitsaspekten und der Definition einer umfassenden Referenzarchitektur anzugehen.

Eine zusammenfassende Beschreibung des Stands der Technik beim IoT, auch unter Berücksichtigung von Standardisierungsaspekten, findet man bspw. in den Veröffentlichungen des European Research Clusters on the Internet of Things (IERC)[10] oder unter dem Oberbegriff *cyber-physikalische Systeme* auf den Web-Seiten des amerikanischen NIST.[11]

Von vielen Standardisierungsgremien wird der Weg gewählt, die wichtigsten Standardisierungspotenziale ausgehend von Anwendungsfällen zu identifizieren. Die Anwendungsdomäne

9 Website der ISO-Arbeitsgruppe: http://www.iso.org/iso/iso_technical_committee.html?commid=45332.
10 Website des Clusters: http://www.internet-of-things-research.eu/.
11 Website des NIST: https://pages.nist.gov/cpspwg/.

STANDARDISIERUNGSBESTREBUNGEN ZUM IOT GIBT ES MEHR ALS GENUG, ES FEHLT JEDOCH EINE HARMONISIERUNG DER ARBEITEN VON UNTERSCHIEDLICHEN GREMIEN.

Public IoT wird dabei bislang noch kaum einbezogen. Hier muss es öffentliche Aufgabe sein, Anwendungsfälle mit Anforderungen des öffentlichen Sektors zu identifizieren und zugehörige Standardisierungspotenziale abzuleiten. Die Standardisierungsaktivitäten des öffentlichen Sektors müssen sich insbesondere auf Fragen des Datenzugangs, der Interoperabilität sowie des Datenschutzes und der Datenportabilität konzentrieren. Daraus ergibt sich auch die Notwendigkeit einer aktiven Mitarbeit bei übergreifenden Fragestellungen etwa zur Ausgestaltung der IoT-Infrastruktur.

3.4 LEISTUNGSFÄHIGE BASISINFRASTRUKTUREN ERMÖGLICHEN

Im notwendigen IoT-Unterbau kommt zwei Bereichen eine besondere Bedeutung zu: der Kommunikationsinfrastruktur für die Datenübertragung und der Entwicklungs- und Betriebsinfrastruktur für die Bereitstellung neuer Anwendungen und Produkte. Im darauf aufsetzenden Oberbau findet man Bausteine zur Verwaltung von Identitäten und Geräten, zur Speicherung, Analyse und Visualisierung von Daten sowie zur Integration in bestehende (Unternehmens-)Software.

Der öffentliche Sektor kann die Entwicklung von leistungsfähigen Infrastrukturen für Public IoT auf vielfältige Weise unterstützen.

Als Nutzer von Public IoT sollte er darauf hinwirken, dass standardisierte, offene Datenformate und sichere Übertragungsprotokolle verwendet werden, für die dann verschiedene, alternativ nutzbare Softwarebibliotheken verfügbar sind. Aufgrund der langen Nutzungszeit von Infrastrukturen und damit verbundenen IoT-Komponenten muss zudem einkalkuliert werden, dass die eingesetzten Produkte oder deren Hersteller nicht bis zum Ende der Lebensdauer am Markt verfügbar sind. Dies erfordert ein erhebliches Umdenken gegenüber den inzwischen sehr kurzen Produktzyklen von Consumer IoT. Die Auswirkungen von IT-Sicherheitsvorfällen betreffen nicht nur Anbieter und direkte Nutzer eines IoT-Gesamtsystems, sondern gehen möglicherweise weit über diese hinaus. Hier sind öffentliche Stellen gefragt, Soft- und Hardwaremodule zur sicheren Kommunikation bereitzustellen oder zu überprüfen bzw. entsprechende Test- und Zertifizierungsanforderungen zu formulieren.

Darüber hinaus ist die Marktentwicklung im Blick zu behalten: Es stehen bereits zahlreiche, z. T. kostenfreie Cloud-Plattformen und Basisdienste großer Internet-Unternehmen bereit, auf denen IoT-Anwendungen aufsetzen können. Netzwerkeffekte führen hier leicht zu einer Konzentration des Marktes. Wichtig ist es daher, verschiedene Aspekte von Offenheit konsequent zu berücksichtigen, und eine komplette Abhängigkeit von einem oder wenigen Anbietern zu verhindern. Angesichts der aktuellen Marktpositionierung europäischer Lösungsanbieter kann es zudem sinnvoll sein, die Entwicklung alternativer Plattformen und hochqualitativer Angebote in ausgewählten IoT-Anwendungsbereichen zu fördern.

Bei der Entwicklung von IoT-Infrastrukturen für den öffentlichen Sektor ist darauf zu achten, dass mittels standardisierter Schnittstellen und Datenformate der Übergang zu privaten IoT-Infrastrukturen möglich ist. Die weitgehende Nutzung gemeinsamer Infrastrukturen erhöht die Wirtschaftlichkeit und macht es möglich, zukünftige, innovative Lösungen weiterzuentwickeln. Isolierte Infrastrukturen sollten nur bei entsprechendem Bedarf aufgebaut werden.

Um Sensoren in größeren Mengen wirtschaftlich zu vernetzen oder auch mobile Systeme an das Internet anzubinden, bedarf es drahtloser Kommunikationsnetze. Zu diesem Zweck kommen frei nutzbare (z. B. bei WLAN) als auch lizensierte Frequenzbereiche (bspw. im Mobilfunk) zum Einsatz. Aufgrund physikalischer Eigenschaften in Bezug auf Reichweite oder Materialdurchdringung sind für verschiedene Einsatzszenarien verschiedene Frequenzbereiche geeignet. Im Rahmen der

BASISINFRASTRUKTUREN FÜR PUBLIC IOT SOLLTEN DEN AUSTAUSCH MIT PRIVATEN IOT-INFRASTRUKTUREN ÜBER STANDARDISIERTE SCHNITTSTELLEN UND DATENFORMATE ERMÖGLICHEN.

Regulierung des Funkspektrums ist diese begrenzte Ressource einerseits bedarfsgerecht für die verschiedenen Anwendungen und Anwendergruppen zur Verfügung zu stellen, andererseits sind die Regelungen international zu harmonisieren.

Darüber hinaus ist für die Realisierung von IoT-Anwendungen der Zugang zum Internet essenziell, es bedarf also flächendeckender Verfügbarkeit und ausreichender Bandbreite. Um die Entwicklung innovativer Dienste zu fördern, sollte zudem keine Filterung durch Provider erfolgen. Befinden sich Komponenten nicht in einem eigens abgesicherten Netz (VPN), so sind spezielle Internet-Anschlüsse für Sensoren oder Maschinen denkbar, die IT-Sicherheit auf der Provider-Seite unterstützen. Entsprechende funktionale Klassen von Internetzugängen müssten dann in der Regulierung unterschieden werden. Möglich ist neben dem privaten Betrieb lokaler Funknetze auch der Aufbau öffentlicher IoT-Mobilfunknetze. Der Schwerpunkt von angebotenen Diensten liegt dann bei niedrigen Datenraten, womit ein niedriger Energieverbrauch bzw. lange Akkulaufzeiten ermöglicht werden. Zudem sollte geprüft werden, ob auch im Bereich kritischer Infrastrukturen eigene autonome Funk- und Datennetze sinnvoll sind und wie diese technisch umgesetzt werden können.

Der Kommunikationsinfrastruktur zuzurechnen sind außerdem Verzeichnisdienste (bspw. DNS), welche die Erreichbarkeit der vernetzten Dinge sicherstellen. Dazu gehören auch Adress- und Namensräume wie IP-Adressen. Diese Infrastrukturen sind genossenschaftlich oder privat organisiert; aufgrund der steigendenden Bedeutung des weiterhin reibungslosen Betriebs der Netzinfrastrukturen kommt dem Staat die Aufgabe zu, das Funktionieren dieser Infrastrukturen zu überwachen, um bei Fehlentwicklungen rechtzeitig eingreifen zu können.

4. AUSBLICK UND FRAGEN FÜR DIE WEITERE DEBATTE

Im Internet of Things verschmelzen die physische und die digitale Welt. Es hebt die Digitalisierung auf eine neue Stufe – mit tiefgreifenden Folgen für den öffentlichen Sektor.

Das Papier hat hier mit dem *Internet of Public Things* und *Public Internet of Things* zwei Begrifflichkeiten unterschieden. Im Internet of Public Things, dem Bereich digital vernetzter physischer Objekte in staatlicher Hoheit oder Gewährleistungsverantwortung, verfügt der öffentliche Sektor über direkte Gestaltungsmacht. Die Nutzungspotenziale reichen von der effizienten Kontrolle von Dingen und Infrastrukturen im öffentlichen Raum über die Automatisierung von Prozessen und die Optimierung der Nutzung von öffentlichen Ressourcen bis hin zur vorausschauenden Datenanalyse und neuen Möglichkeiten der politischen Steuerung.

Daraus ergeben sich verschiedene Fragen an Politik und Verwaltung: Welche Dinge im öffentlichen Raum sollen digital identifizierbar sein? Welche Verzeichnisse sind in der öffentlichen Verwaltung dafür aufzubauen? Welche öffentlichen Dinge sind zukünftig mit Sensorik, welche mit Aktorik auszustatten? Bei welchen Beschaffungen muss IoT-Fähigkeit bereits heute berücksichtigt werden? Welche Standards sind zu berücksichtigen bzw. neu zu schaffen? Welche technologischen IoT-Komponenten und -Plattformen sollten öffentliche IT-Dienstleister bereitstellen? Wie sind Aufgaben und Verantwortlichkeiten für IoT-Infrastrukturen zwischen Bund, Ländern und Kommunen verteilt?

Zugleich schafft der Staat Rahmenbedingungen für die Nutzung privater IoT-basierter Produkte und Dienstleistungen, deren Ausgestaltung privaten Akteuren obliegt. Das Spektrum der vernetzten Dinge, aus dem sich für den Staat spezifische Regulierungsfunktion ergeben, wird unter dem Begriff *Public Internet of Things (Public IoT)* gefasst.

Für die Regelung des Datenschutzes entstehen durch das exponentielle Wachstum personenbeziehbarer Daten neue qualitative Herausforderungen. Die digitale Vernetzung von Objekten bringt ferner neue unmittelbare und mittelbare Sicherheitsrisiken und damit verbundene Haftungsfragen mit sich. Der Staat ist zudem in der Verantwortung, Informationsstrategien zu entwickeln, um die Öffentlichkeit für die Regeln und Risiken dieser neuen Dimension der Vernetzung zu sensibilisieren. Auch können aktuelle rechtliche oder politische Rahmenbedingungen dem wirtschaftlichen Einsatz von Public IoT durchaus entgegenstehen. Um Facettenreichtum und Souveränität zu erhalten, gilt es, Monopolisierungstendenzen einzudämmen. Nicht zuletzt braucht Public IoT nachhaltige Basisinfrastrukturen, die von kurzen technologischen Innovationszyklen unabhängig sind.

Auch für den weiteren Bereich von Public IoT ergeben sich zahlreiche Fragen: Wer erhält lesenden oder steuernden Zugriff auf Sensoren und Aktoren im öffentlichen Raum? Welche Daten sollten der Öffentlichkeit zur freien Weiterverwendung zur Verfügung gestellt werden? Welche Daten sind in welcher Granularität öffentlichen Stellen bereitzustellen? Welche Schnittstellen gilt es zu schaffen? Wo muss der Staat Datenschutz und Haftungsregelungen nachjustieren?

Es ist klar geworden: Public IoT ist kein rein technisches Konzept. Es kann nicht losgelöst von anderen IT-Entwicklungen, organisationalen Prozessen, gesellschaftlichem Bedarf und politischer Verantwortung betrachtet werden. Anwendungsfelder finden sich über alle Politikfelder hinweg. Staat und Verwaltung sollten das Internet of Things ernst nehmen. Seine Auswirkungen sind weit häufiger von öffentlichem Belang als es zunächst den Anschein hat. Umso dringlicher ist eine gesellschaftliche Debatte, die nach den Licht- und Schattenseiten fragt und ein wünschenswertes Maß an digitaler Vernetzung auslotet. Die neuen Spielräume sollten ebenso wenig unterschätzt werden wie Regulierungsaufgaben und langfristige Gestaltungmöglichkeiten.

IMPRESSUM

Herausgeber
Dr.-Ing. Matthias Flügge, Jens Fromm

Redaktionsteam
Dr. Mike Weber, Dr. Klaus-Peter Eckert, Roman Konzack

Gestaltung
Reiko Kammer

Bildnachweise
Cover, Ingo Bartussek, fotolia.com
Seite 1, Erich Pietzsch, fotolia.com, (CC0 1.0 Universal)
Seite 2, Syda Productions, shutterstock.com
Seite 8, Photocapy, flickr.com, (CC BY-SA 2.0)
Seite 11, lilou, pixabay.com
Seite 13, Ben_Kerckx, pixabay.com
Seite 16, FraukeFeind, pixabay.com
Seite 19, Andrew Moore, flickr.com, (CC BY-SA 2.0)

Engineering a
Connected World

KONTAKT

Roman Konzack
Leiter Forschungskommunikation und Labore
Geschäftsbereich Digital Public Services
Tel.: +49 30 3463-7115
Fax: +49 30 3463-99-7115
dpskontakt@fokus.fraunhofer.de

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

https://www.fokus.fraunhofer.de/dps

kre | 1605