WOHIN FÜHRT UNS EIGENTLICH DAS INTERNET DER DINGE?

Jörn von Lucke

Professor, Zeppelin Universität, The Open Government Institute
Am Seemooser Horn 20, 88045 Friedrichshafen, DE
Joern.vonLucke@zu.de; http://togi.zu.de / http://www.smartgovernment.de / http://www.joernvonlucke.de

Schlagworte: ***Internet der Dinge, Internet of Things, Smart Government, Smart Justice, smarte Objekte, cyberphysische Systeme, Realtime Government, IoT-Datenplattform, Smart Surveillance, Datenschutz, Informationssicherheit***

Abstract: *Das Internet der Dinge (IoT) gewinnt zur Erfüllung öffentlicher Aufgaben an Bedeutung. Neuartige smarte, also intelligent vernetzte Objekte und cyberphysische Systeme stellen bisherige Abläufe, Prozesse und Vorgehensweisen grundsätzlich in Frage. Die Kombination von sensorgenerierten smarten Daten mit Apps und Diensten, großen Datenanalysen und Anwendungen mit künstlicher Intelligenz eröffnet unter dem Schlagwort «Smart Government» neue Perspektiven für Staat, Verwaltung und Justiz. Sind diese technischen Möglichkeiten des Internets der Dinge aber gesellschaftlich wirklich wünschenswert? Führt der technische Fortschritt nicht in einen Überwachungsstaat, gerade weil er erhebliche Einsparpotentiale eröffnet und die Informationsbasis verbessert? Welche Handlungsempfehlungen müssen gegeben werden, um die Chancen für Staat und Verwaltung zu nutzen, ohne in einer smarten Überwachung des Alltags und der freien Gesellschaft zu enden?*

1. Forschungsfrage: Wohin führt uns eigentlich das Internet der Dinge?

Die intelligente Vernetzung von realen Dingen und damit das «Internet der Dinge» (Internet of Things, IoT) konnten erfolgreich eingeführt werden. Unter den Schlagwörtern «Industrie 4.0», «Vierte industrielle Revolution», «smarte Fabrik», «smarte Produktion» und «industrielles Internet» werden im Rahmen von industrieller Produktion und Logistik vor allem smarte Objekte (intelligent mit Sensoren, Aktoren und einer Kommunikationseinheit vernetzte Dinge) sowie diese nutzende cyberphysische Systeme (CPS) entworfen, entwickelt und eingesetzt. Mit ihnen lassen sich ingenieurwissenschaftliche Visionen einer smarten Fabrik, einer smarten Produktion und smarter Produkte realisieren. Diese sind dank intelligenter Vernetzung bisherigen Lösungen in vielen Bereichen deutlich überlegen und verändern vorhandene Wertschöpfungsketten disruptiv. «Industrie 4.0» steht im Kern für die technische Integration von CPS in die Produktion und die Logistik sowie für die Anwendung des Internets der Dinge und der Dienste in industriellen Prozessen, einschließlich der sich daraus ergebenden Konsequenzen für die Wertschöpfung, die Geschäftsmodelle sowie die nachgelagerten Dienstleistungen und die Arbeitsorganisation [Forschungsunion/acatech 2013, 18].

Die mit dem Internet der Dinge verbundenen Potentiale sind auch für den öffentlichen Sektor von großem Interesse. Die sich heute bietenden technischen Möglichkeiten von smarten Brillen, Body Cams, Überwachungskameras, smarten Straßenlaternen, Drohnen und Robotern legen deren Einsatz zur effektiven, wirtschaftlichen und sparsamen Erfüllung von öffentlichen Aufgaben mehr als nahe. Allerdings entwickeln sich die smarten Objekte mit ihren Sensoren, Aktoren und Funkchips zunehmend zu echten «Datenschleudern», die die Bürger und deren Alltag laufend vermessen. Andererseits gibt es Akteure, die ein Eigeninteresse haben, diese Technologien ganz bewusst auch zur Überwachung der Bevölkerung oder gar zur Destabilisierung fremder Staaten einzusetzen.

Südkorea setzt stark auf den Bau smarter Städte im ländlichen Raum, in denen Breitband, Sensoren, Big Data und künstliche Intelligenz breite Verwendung finden. Dies sind zentrale Ansätze einer Wirtschaftspolitik, um sich im internationalen Wettbewerb mit digitaler Infrastruktur Wachstum und Wohlstand zu sichern. In Japan entwickeln Unternehmen und Forschungseinrichtungen Anwendungsszenarien rund um künstliche Intelligenz. Wichtige Leitbilder sind «Soziale Cyberphysische Systeme» als Grundlage für die «Super Smarte Gesellschaft». Japanische Unternehmen vertreiben bereits smarte Brillen, Polizeiroboter und Verhaltensmonitorsysteme. «Smart Dubai» ist ein strategischer Ansatz des Emirats Dubai, um die eigenen Smart Government-Lösungen international zu vermarkten. Das Emirat setzt auf Open Innovation, Blockchain-Technologien im öffentlichen Sektor, Flugdrohnen und eine smarte Infrastruktur. Die Stadt Taipeh veranstaltet jährlich den Smart City Summit & Expo (SCSE), um taiwanesische Produkte und Lösungen international zu positionieren. 2018 dominierten auf künstlicher Intelligenz basierte Anwendungsszenarien die Messe: smarte Gebäude, smarte Grids, smarte Gesundheitsversorgung, smarte Schulen und smarte Überwachung. Singapur setzt als «smarte Nation» auf Kl-basierte Videoanalysedienste, die automatisiert funktionieren und kaum noch als personalintensiv gelten. Derzeit wird eine smarte Sensorplattform aufgebaut, um auf von der Norm abweichendes Verhalten möglichst zeitnah reagieren zu können. Die Volksrepublik China setzt künftig auf ein Sozialbonitätssystem über Unternehmen und Bürger, das zur Berechnung von Vertrauen und Kreditwürdigkeit auch Datensammlungen über das Internet der Dinge anlegen und nutzen wird [von Lucke 2018, 181–186] [von Lucke 2018b, 2].

Diese Eindrücke einer Forschungsreise nach Asien in den Jahren 2017 und 2018 führen relativ rasch zur Forschungsfrage: «Wohin führt uns eigentlich das Internet der Dinge?» Die sich derzeit durch eine intelligente Vernetzung und das Internet der Dinge bietenden gestalterischen Möglichkeiten sind sehr vielfältig. Für Staaten, ihre Regierungen und Verwaltungen sowie die Justiz eröffnen sich mit smarten Objekten und CPS sowie mit Smart Government und Smart Justice neuartige Perspektiven, die künftig durch die Mobilfunknetzwerke der fünften Generation nahezu in Echtzeit zusammenspielen können. Nicht alle technisch vorstellbaren Möglichkeiten des Internets der Dinge können als gesellschaftlich wirklich erstrebenswert gelten. Mit welchen Dystopien muss aber gerechnet werden, wenn man der Entwicklung und den treibenden Akteuren einfach ihren Lauf lässt? An zwei Ansätzen, den IoT-Datenplattformen und Smart & Realtime Surveillance, lässt sich dies im folgenden Beitrag beispielhaft aufzeigen. Der sich aus diesen Überlegungen abzuleitende Anspruch an Staat und Verwaltung muss die Bürger als Betroffene im Blick haben. Erforderlich sind ein datenschutzkonformes und sicheres Internet der Dinge sowie ein datenschutzkonformes Smart Government, um Vorteile und Chancen für Staat und Verwaltung zu nutzen, ohne in einer smarten Überwachung des Alltags zu enden. Hier gibt es aber unterschiedliche Interessen und politische Erwartungen. Politik, Regierung und Gesetzesgeber müssen eigenverantwortlich die vorzulegenden Handlungsempfehlungen zur Gestaltung eines smarten Staats, einer smarten Verwaltung und einer smarten Justiz sammeln, bewerten, abwägen und dann ihre Entscheidungen treffen.

2. Internet der Dinge: Smarte Objekte und cyberphysische Systeme

Mit dem Begriff «Internet der Dinge» wird die Vernetzung realer Objekte über die Internet-Protokolle verständlich umschrieben. Es verbindet smarte Objekte mit ihren Sensoren, Aktoren und Kommunikationseinheiten sowie die darauf aufsetzenden CPS über die IP-Protokollsuite. Eingebettete Alltagsgegenstände und CPS lassen sich von Personen, Programmen, Diensten und Datenpaketen über eine IP-Adresse eindeutig identifizieren, ansprechen, nutzen und gegebenenfalls auch steuern. Das Internet der Dinge steht damit für die globale elektronische Vernetzung von Alltagsgegenständen und den direkten gegenseitigen Informationsaustausch von Objekten ohne menschliche Eingriffe im Sinne einer echten Kommunikation von Maschine zu Maschine. Im Internet der Dienste werden Dienste und Funktionalitäten als feingranulare Softwarekomponenten abgebildet und von Providern auf Anforderung über das Internet zur Verfügung gestellt. Web Services, Cloud Computing und standardisierte Schnittstellen ermöglichen dies. Die einzelnen Softwarebausteine sind

so miteinander integrierbar. Die enge Verzahnung des Internets der Dienste mit dem Internet der Dinge beruht darauf, dass sich zahlreiche reale Dinge wie etwa Papier bei mindestens gleichwertiger Funktionalität auch in webbasierte Dienste überführen und um ergänzende durchdachte Funktionen erweitern lassen. Vor allem durch die direkte Maschine-zu-Maschine-Kommunikation eröffnen sich zahlreiche neue Ansätze, die bei konsequenter Umsetzung grundlegende Veränderungen bedeuten [von Lucke 2015, 18–19][von Lucke 2018, 179].

Smarte Objekte verfügen über Sensoren, Aktoren und Kommunikationseinheiten, die es ihnen ermöglichen, mit anderen smarten Objekten sowie mit CPS zu kommunizieren. Sie lassen sich in Wearables, Smart Home-Geräte, smarte stationäre Geräte und smarte mobile Geräte unterteilen. Wearables sind Geräte, die Menschen laufend mit sich führen und die mit dem Internet direkt verbunden sind. Diese Kategorie umfasst Geräte wie etwa smarte Armbänder, smarte Uhren, Smartphones, Body Cams, smarte Brillen, smarte Hörgeräte und smarte Fußfesseln. Die Kategorie der Smart Home-Geräte umfasst vor allem Haushaltsgeräte, von Lampen und Lichtschaltern bis hin zu Bewegungsmeldern, Thermostaten, Türschlössern, automatischen Jalousien, Smart TVs, smarten Kühlschränken, smarten Waschmaschinen und smarten Zählern. Über die WLAN-Verbindung zum Router wird das Smartphone, das Tablet oder der Laptop zum Online-Dashboard und Steuergerät für die Smart Home-Anwendungen. Die Kategorie der smarten stationären Geräte umfasst alle unbeweglichen Dinge, deren Sensoren bei großer Flexibilität nun von außen zugänglich werden. Dazu gehören etwa Überwachungskameras, Umweltmessstationen und smarte Straßenbeleuchtungen. Die vierte Kategorie der smarten mobilen Geräte enthält Dinge, die oft mit einem Mobilfunknetz verbunden sind. Hierzu gehören tragbare Geräte wie tragbare Pumpen, tragbare Gassensoren und Wärmebildkameras, aber auch bemannte und unbemannte Fahrzeuge einschließlich Boden-, Überwasser-, Unterwasser- und Luftfahrzeuge (inklusive Drohnen) sowie Roboter. Alle diese smarten Objekte können und werden von ihren Besitzern für verschiedenste Aufgaben verwendet, meistens für gute Vorhaben und Zwecke, aber manchmal auch zum Schaden anderer. Anbieter, Eigentümer und Nutzer werden durch IoT-Entwicklungsplattformen in die Lage versetzt, diese für ihre eigenen Zwecke einzusetzen, aber auch um zu manipulieren und einzuschränken [von Lucke 2018c, 340–341]. Mit Hilfe ihrer Sensoren sind smarte Objekte in der Lage Zustände (wie zum Beispiel Anwesenheit, Temperatur, Feuchtigkeit, Schall, Licht, Bewegung, Materialeigenschaften) zu registrieren und diese in Form von Daten zu speichern, Aktionen auszuführen und mit anderen intelligent vernetzten Objekten über Funk zu kommunizieren. Die Sensoren erzeugen kontinuierlich Daten. Die Objekte entwickeln sich so zu «Datenschleudern», die den Alltag laufend vermessen. CPS nutzen die generierten smarten Datenbestände der smarten Objekte, werten sie aus und steuern mit ihnen auf Basis cleverer Algorithmen komplexere Gebilde [von Lucke 2018, 180–181].

CPS sind heterogen vernetzte Gebilde, die reale physische Objekte mit digitalen Informations- und Kommunikationssystemen verknüpfen und kombinieren. Bei ihnen handelt es sich um IT-Systeme als Teil von Geräten, Gebilden oder Prozessen, die über Sensoren unmittelbar physische Daten erfassen und durch Aktoren auf physische Vorgänge einwirken, die vor allem aber die erfassten Daten auswerten und speichern. Zudem können sie aktiv oder reaktiv mit der physischen und der digitalen Welt interagieren. CPS greifen zur Aufgabenerledigung in der Regel auf eine Vielzahl smarter Objekte, eingebetteter Systeme oder Sensornetze zurück, die sie auch im großen Umfang und über räumliche Entfernung nutzen [acatech 2011, 13][Geisberger/Broy 2012, 22][von Lucke 2015, 14].

Das Internet der Dinge eröffnet Organisationen und Behörden neue Wege, wie diese von besseren Informationen und unterstützenden Analysen sowie von Entscheidungen autonomer Systeme profitieren können. Smarte Objekte und CPS verbessern das Potential für eine breitere Informationsbeschaffung und eine bessere Analyse. Liegen die richtigen Daten in der geforderten Qualität zur richtigen Zeit vor, kann sich dies positiv auf die Entscheidungsunterstützung und -automation auswirken. Beispielsweise können Sensordaten helfen, das Verhalten von Personen, Dingen, Dienstleistungen oder Daten zu verfolgen und Wechselwirkungen aufzei-

gen. Dabei geht es nicht nur um vereinfachte Suchen, Protokollierungen und Auswertungen durch und für den Nutzer öffentlicher Angebote selbst. Auch Dritten könnten Auswertungsdienste auf anonymer oder mit Zustimmung des Betroffenen sogar personalisierter Basis ohne Verletzung des Datenschutzes angeboten werden [von Lucke 2018, 182]. Hieraus eröffnen sich zahlreiche Perspektiven für Staat, Verwaltung und Justiz.

3. Intelligent vernetzte Perspektiven: Smart Government und Smart Justice

Bei Smart Government, dem smarten Staat, smarten Städten und smarten Dörfern geht es im Kern um die Frage, welcher smarten Objekte der öffentliche Sektor bedarf und in welche CPS diese einzubetten sind. Diese können durch Apps und Webdienste, Big-Data-Analysen, Anwendungen der künstlichen Intelligenz, kognitive Dienste und Nudging-Dienste gezielt ausgebaut und verbessert werden. Smart Government liefert Entscheidungsträgern verbesserte Informationen und tiefgreifendere Analysen. Zusätzlich setzt es auch auf eine stärkere Automatisierung der Abläufe und auf Steuerung und Kontrolle durch die Informationssysteme selbst. CPS werden sich zunehmend eigenständig informieren und eine Situation analysieren, aber auch automatisch und autonom Entscheidungen treffen und diese umsetzen können. Dazu setzen diese autonomen Systeme auf Algorithmen, die ihnen entweder von Entwicklern einprogrammiert wurden oder die sie sich als lernendes System im Laufe der Zeit selbst erarbeitet haben. Smarte Objekte und CPS tragen dazu bei, dass autonome Systeme selbst immer komplexere Entscheidungen treffen können. Diese profitieren vom technischen Fortschritt durch leistungsfähigere Rechner, günstige Datenspeicher, geringe Latenzzeiten, künstliche Intelligenz und die Verhaltensökonomie. Papierbasierte Abläufe werden durch smarte Verwaltungsakten ersetzt, die sich selbst ihren virtuellen Weg durch die Zuständigkeiten und Behörden suchen. Transparenz bekommt so einen immer höheren Stellenwert [von Lucke 2019, 24]. An der Gestaltung neuartiger smarter Objekte, CPS und entsprechender smarter Datenräume arbeiten Entwicklerteams weltweit. Diese Entwickler und Designer haben eine besondere Verantwortung, IT-Sicherheitskonzepte zu entwerfen und personenbezogene Daten vor unberechtigten Zugriffen zu schützen.

Bei Smart Justice geht es um die Frage, welche smarten Objekte und welche CPS die Justiz, Richter, Staatsanwälte, Justizbeamte und Gefängnisse zur wirtschaftlichen wie sparsamen Erfüllung ihrer öffentlichen Aufgaben benötigen und wo Grenzen zu ziehen sind. Smarte überwachbare Fußfesseln ermöglichen etwa neue Formen des räumlich begrenzten Hausarrests. Sie können das Verlassen von zugewiesenen Zonen einem Delinquenten warnend signalisieren und rasche Reaktionen bewirken. Reagiert dieser nicht, wird die Verwaltung rasch aktiv. Diese CPS entlasten den Strafvollzug personell und finanziell. Das Bewegungsverhalten von Personen im offenen Vollzug ließe sich alternativ mit smarten Armbändern, smarten Uhren und Smartphones verfolgen. Richter profitieren von smarten Richterarbeitsplätzen und smarten Fallakten, die bei neuen Sachständen automatisch aktualisiert und visuell verständlich aufbereitet werden. Cockpits erleichtern dem Gerichtspersonal, Gefängnispersonal und Bewährungshelfern durch aktuelle Informationsaufbereitung ihre Arbeit. Funktionieren kollaborative smarte Fallakten und der elektronische Rechtsverkehr, ist eine ganz neue Form der Rechtsprechung vorstellbar. Richter, Staatsanwaltschaft und Rechtsanwälte hätten gleichzeitig Zugriff auf die Akte und könnten über sie gemeinsam an einem Vergleich oder an der Rechtsprechung arbeiten. Werden die Dokumente des smarten Urteils und des Strafbefehls mit Zusatzinformationen erweitert, lassen sich Rechtsprechungsdatenbanken zeitnah aktualisieren und Prozesse des Strafvollzugs optimieren. Die konsequente Vernetzung erlaubt auch einen grenzüberschreitenden Verbund elektronischer Handelsregister und Grundbücher in Wirtschaftsräumen wie dem Digitalen Europäischen Binnenmarkt [von Lucke 2015, 27].

Im Kontext von Staat, Verwaltung und Justiz muss zudem abgeklärt werden, welche vorhandenen smarten Objekte und welche vorhandenen CPS heute bereits eingesetzt werden könnten und wo künftig Grenzen beim Einsatz zu ziehen sind, damit aus dem Staat kein Überwachungsstaat wird. Aus der Gestaltung des Internets der Dinge und des Internets der Dienste ergibt sich so ein enormer Rechtsgestaltungs- und Abwägungsbedarf für den Gesetzgeber, etwa wenn es mit einem Smart Government Gesetz und einem Smart Justice Gesetz

darum gehen wird die zulässigen Handlungsspielräume zu bestimmen. Mit der Pflicht zu offenen Standards und offenen Schnittstellen sollte der Gesetzgeber zudem Interoperabilität zwischen den verschiedenen Systemen, Anbietern und Akteuren von Anfang an einfordern [von Lucke 2015, 32–33][von Lucke 2017, 229].

4. Perspektiven in Echtzeit: Realtime Government und Realtime Justice

Das taktile Internet als erkennbare nächste Entwicklungsstufe des Internets wird dafür sorgen, dass in einem Jahrzehnt über gigabitbreitbandige Netzwerke und die künftige fünfte Mobilfunkgeneration (5G) nahezu in Echtzeit Netzwerkkommunikation und Handeln erfolgen können. Durch minimale Reaktionszeiten im Millisekunden-Bereich, höchste Verfügbarkeit, Zuverlässigkeit und Sicherheit werden Wirtschaft, Verwaltung und Gesellschaft einen weiteren Innovationsschub erfahren. Es ermöglicht durch taktile und haptische Sinneseindrücke eine neue Dimension in der Mensch-Maschine-Kommunikation und beschleunigt die Interaktion von Maschinen. Zudem werden Anwendungen der künstlichen Intelligenz zeitnah Anfragen auswerten und mit Menschen verbal kommunizieren können [VDE-ITG 2014, 3–4][von Lucke 2015, 25][von Lucke 2018, 180].

Die minimalen Reaktionszeiten im Millisekundenbereich bei höchster Verfügbarkeit erlauben ein Echtzeitprinzip über größere Distanzen. Von Sendern ausgelöste Impulse haben dann Reaktionen beim Empfänger fast in Echtzeit zur Folge. Zuverlässig und vor Unberechtigten geschützt können so Eingriffe aus der Ferne ausgelöst oder begleitet werden. Diese steuernden Eingriffe eröffnen neue Möglichkeiten zur Steuerung von schnell beweglichen Teilen, Robotern oder anderen smarten Objekten. In Verbindung mit optischen Sensoren und smarten Brillen ergeben sich neue Ansätze für die virtuelle Realität und die erweiterte Realität. Dies bietet neuartige Perspektiven für Montage- und Reparaturarbeiten, Telechirurgie, Assistenzsysteme, kooperative Verkehrssysteme und Lernumgebungen. Nutzer werden permanent mit Aktualisierungen zu rechnen haben, was die Komplexität weiter erhöhen wird [VDE-ITG 2014][von Lucke 2017, 230][von Lucke 2018, 180].

Staat, Verwaltung und Justiz stehen auch hier vor der Frage, in welchen Bereichen Investitionen in ein «Realtime Government» und eine «Realtime Justice» zur Erfüllung öffentlicher Aufgaben überhaupt sinnvoll und vertretbar wären. Visuell aufbereitete Zusatzinformationen und Assistenzdienste, die automatisch aus den Akten heraus generiert werden können, ermöglichen neuartige Ansätze für Strafprozess- und Verwaltungsverfahren. Drohnen und Roboter können Menschen bei Analyse-, Montage- und Reparaturarbeiten entlasten und so dringend gesuchte Produktivitätsreserven freisetzen. Zugleich muss aber auch über Grenzziehungen nachgedacht werden. Nicht alles, was in Echtzeit aus der Ferne durch das Internet der Dinge möglich wäre, ist aus Sicht des Staates, der Justiz und der Bevölkerung auch wünschenswert[von Lucke 2017, 230–231][von Lucke 2018, 180].

5. Dystopie: Gläserne Bürger durch frei zugängliche IoT-Datenplattformen

Österreich und Deutschland haben mit dem Dritten Reich (1933/38–1945) und der Deutschen Demokratischen Republik (1949–1990) Erfahrungen mit Diktaturen erdulden müssen. Eine umfassende Überwachung der Bevölkerung, eine Identifikation möglicher Gegner und deren Bekämpfung waren in diesen beiden Diktaturen ganz wesentlich für die Machtsicherung der politischen Eliten. Die «Geheime Staatspolizei» (1933/38–45: «Gestapo») und die DDR-Geheimpolizei «Staatssicherheit» (1949–90: «Stasi») agierten allerdings in einer papierbasierten Welt. Informationen wurden über Berichte, Anzeigen und Verhöre gesammelt und in Papierakten archiviert. Die Methoden und die Folgen dieser Überwachung waren jedoch so menschenverachtend und tödlich, dass die Väter und Mütter des deutschen Grundgesetzes zahlreiche Regelungen als unverletzliche Grundrechte und gleichzeitig eine unabhängige Rechtsprechung verankerten, sodass eine vollständige Überwachung der Bevölkerung ohne Rechtskontrolle nicht wieder möglich sein sollte [von Lucke 2018, 184].

Die Sorge vor dem gläsernen Bürger durchzieht seit dem Ende der nationalsozialistischen Herrschaft 1945 die Gesetzgebung in Österreich und in Deutschland. Der Staat soll künftig nicht mehr in die Lage versetzt

werden, umfassende Profile über alle Bürger anzulegen, um diese zu überwachen und gegen diese zu verwenden. Schließlich würde jede Form von Profilbildung einer Überwachung entsprechen und die Bürger in ihrer Entwicklung und Lebensgestaltung inakzeptabel einschränken. Dieser durch die Datenschutzgesetze und die DSGVO konkretisierte Rahmen besitzt für die Republik Österreich, die Bundesrepublik Deutschland und ihre Behörden bis heute Gültigkeit. Trotz staatlicher Beauftragter für den Datenschutz könnte dieser Rahmen aber jederzeit durch den Gesetzgeber mit den erforderlichen parlamentarischen Mehrheiten auch modifiziert werden. Pikanterweise halten sich zudem einige ausländische Nachrichtendienste nicht an diese nationalen Gesetze. Sie sammeln systematisch Daten über Bürger und Unternehmen anderer Staaten und nutzen auch ihre gewonnenen Erkenntnisse, gegebenenfalls im Verbund, sofern sich für sie daraus relevante Vorteile ergeben. Pragmatisch wird auf freiwilliger und unfreiwilliger Basis auch mit Plattformbetreibern zusammengearbeitet, sollten diese über relevante Datenbestände verfügen. Mit Blick auf die sich gerade im Aufbau befindlichen, teils frei zugänglichen Datenplattformen für das Internet der Dinge werden auch hier Begehrlichkeiten geweckt [Snowden 2013][Paganini 2016].

In Zeiten smarter Objekte lassen sich solche Überwachungssysteme gezielt ausbauen, denn die Bürger nutzen ihre Gadgets und Wearables zunehmender und werden so durch die Generierung neuer Daten immer gläserner. Dies könnten Staaten auch gezielt nutzen. Die Republik Singapur lässt sich bereits eine eigene nationale Sensorplattform («Smart Nation Sensor Platform») errichten, über die alle Sensoren und smarten Objekte im Stadtstaat erschlossen und mit Daten- und Videoanalysesystemen ausgewertet werden sollen. Geplant ist jede Straßenbeleuchtung mit Überwachungskameras und weiteren Sensoren zu einer smarten Laterne aufzurüsten. Die Überwachungskameras der Straßenverkehrsbehörde werden ebenso eingebunden wie die Videoüberwachungssysteme aller Hotels, Einkaufszentren und Bürogebäude im Stadtstaat. In der Nationalen Sensorplattform sollen diese Daten und Videofilme dann kombiniert und analysiert werden. Mittelfristig wird sogar an den Zugriff auf Smartphones der Bürger gedacht, die sich als sehr effektive Sensoren vor Ort erwiesen haben. Mitarbeiter der Sensorplattform erlernen gerade mit Hilfe von KI-Systemen die zusammengeführten Daten zu analysieren, um außergewöhnliche Ereignisse zu erkennen. Moderne KI-basierte Videoanalysedienste binden nur wenig Personal. Für die Überwachung von 10‘000 Kameras sind nur noch 10 Mitarbeiter erforderlich. Erkennt der Algorithmus mit Hilfe künstlicher Intelligenz, dass etwas Seltsames passiert, wird der Kontrolleur nahezu in Echtzeit informiert und kann gezielt reagieren. Ziel ist ein besseres Verständnis, was am Puls der Stadt gerade vor sich geht. Tatsächlich werden die Bürger aber immer gläserner [Lee 2017][GovTech 2017][von Lucke 2018, 185].

6. Dystopie: Überwachungsstaat dank Smart & Realtime Surveillance

In der Republik Österreich und der Bundesrepublik Deutschland übernehmen heute Ordnungsdienst, Feuerwehr, Polizei, Justiz und Verfassungsschutz die Aufgaben der inneren Sicherheit und Ordnung. Sie sollen Staat und Gesellschaft vor Kriminalität, Terrorismus und vergleichbaren Bedrohungen aus dem Inneren der Gesellschaft schützen. Bei ihrer Aufgabenwahrnehmung orientieren sich die Sicherheitsbehörden an Recht und Gesetz. Gegen ihre Maßnahmen kann gerichtlich vorgegangen werden. Als Reaktion auf den technischen Fortschritt werden immer wieder Gesetzesnovellen in die Gesetzgebung eingebracht, aktuell etwa die Polizeiaufgabengesetze, damit die Sicherheitsbehörden auch modernste Informations- und Kommunikationstechniken zur Erfüllung öffentlicher Aufgaben einsetzen können. Solche Novellen finden in der Bevölkerung und in Fachkreisen nicht nur Zustimmung. Mit Blick auf die Vergangenheit besteht stets die Sorge, dass diese Technik auch zur dauerhaften Überwachung der Bevölkerung eingesetzt werden könnte. Im Rahmen der laufenden und anstehenden Debatten zu intelligent vernetzten und in Echtzeit reagierenden Überwachungssystemen (Smart & Realtime Surveillance) werden die Argumente angehört und abgewogen werden müssen, ehe der Gesetzgeber Entscheidungen zur Sicherung staatlicher Zugriffe auf smarte Objekte, CPS und die neuartigen Datenräume der Internets der Dinge zu treffen hat.

Body Cams, Überwachungskameras und Drohnen legen den Einsatz von smarten Objekten und CPS zur Erfüllung von Aufgaben der öffentlichen Sicherheit mehr als nahe. Auch die laufende Generierung von immer größeren Datensammlungen im Internet der Dinge kommt den Sicherheitsbehörden mehr als entgegen, zumal KI-basierte Analysedienste rasch hochwertige Auswertungen über Bild-, Ton- und Videoaufnahmen bei geringem Personalbedarf und erheblichen Einsparpotentialen liefern. Selbst wenn 2019 erst mit dem Aufbau erster Prototypen für IoT-Datenplattformen in urbanen und kommunalen Datenräumen begonnen wird und diese noch einige Jahre bis zur technischen Ausreifung benötigen, so sind die damit verbundenen Chancen und Risiken einer vollkommenen Überwachung des Alltags für Sicherheitsbehörden und Bevölkerung mehr als offensichtlich. Und mag der Aufbau eigener IoT-Datenplattformen durch die Sicherheitsbehörden in Europa noch als abwegig erscheinen, so werden Erfolgsmeldungen und Szenarien aus Asien weitere Begehrlichkeiten wecken, die zu Beginn des Jahres 2019 eigentlich noch als völlig unvorstellbar gelten.

7. Anspruch: Datenschutzkonformes und sicheres Internet der Dinge

Abschließend stellt sich die Frage, welche Handlungsempfehlungen jetzt gegeben werden müssen, um die Vorteile und Chancen des Internets der Dinge auch für Staat und Verwaltung zu nutzen, ohne in einer smarten Überwachung des Alltags und der freien Gesellschaft zu enden. Technisch betrachtet ist das Internet der Dinge 2019 bereits gelebte Realität. Es macht Wirtschaft und Gesellschaft aber verletzlich. Tatsächlich gibt es versteckte Hintertüren in Hardware, Software und Netzwerkknoten. Das laufende Abhorchen von Datenübertragungen und das gezielte Kopieren und Analysieren von IoT-Datensammlungen gehören zum Repertoire der Nachrichtendienste. Verbote werden deswegen kaum noch helfen, da sie kaum greifen und entsprechende Aktivitäten nicht verhindern. Datenschutz und Informationssicherheit im Internet der Dinge müssen nun forciert werden.

Mit Blick auf die Erfahrungen der Diktaturen im Dritten Reich und in der DDR sowie die Errungenschaften des Datenschutzes und des Rechts auf informationelle Selbstbestimmung bleibt eine Überwachung der Bürger und deren Verhalten im Alltag auf Basis smarter Objekte weiterhin inakzeptabel. Smarte Objekte und CPS dürfen nicht zu Instrumenten der Überwachung und Unterdrückung bestimmter oder aller Bevölkerungsgruppen werden. Der Schutz personenbezogener Daten muss auch im Internet der Dinge sichergestellt werden. Politischen Forderungen nach einem Abbau des Datenschutzes (Staatsministerin Dorothee Bär 2018: «aus dem 18. Jahrhundert») insbesondere von Seiten führender Sicherheitspolitiker muss mit Blick auf die vorhandenen Bedrohungen mehr als eine Absage erteilt werden. Es gilt den Schutzbedarf angemessen auszubauen. Die IT-Grundschutzwerke sind mit Blick auf technische Entwicklungen zu pflegen und zu aktualisieren. Das Internet der Dinge muss noch stärker in den Fokus der Beauftragten für den Datenschutz rücken. Insgesamt bleibt es weiterhin eine Aufgabe des Staates, Bürger vor unerwünschten Auswirkungen gespeicherter Daten zu schützen. Dafür müssen im aufgabenadäquaten Umfang auch personelle und finanzielle Ressourcen über Stellenpläne und Haushaltspläne bereitgestellt werden.

Mit Blick auf die Begehrlichkeiten fremder Nachrichtendienste muss auch in die Gewährleistung von Daten- und Informationssicherheit im Internet der Dinge investiert werden. Dies dient dem Schutz gegen Hackerangriffe, Verluste, Angriffe und Missbräuche und stärkt die eigene Resilienz. Das Internet der Dinge verändert Wertschöpfungsketten und Geschäftsmodelle, schafft neue Netzwerke und Verbünde. Staat, Verwaltung und Justiz müssen wie Wirtschaft und Industrie sicherstellen, dass sie unter den neuen Rahmenbedingungen des Internets der Dinge sicher und verlässlich funktionieren. Das bedeutet, dass für Informationssicherheit, Schutzmaßnahmen und Resilienz ebenfalls im aufgabenadäquaten Umfang personelle und finanzielle Mittel bereitzustellen sind.

Staat, Verwaltung und Justiz stehen vor der Herausforderung zu überprüfen, inwieweit das Internet der Dinge und das taktile Internet sowie smarte Objekte, CPS und auf künstlicher Intelligenz basierende autonome Systeme zur effektiven, wirtschaftlichen und sparsamen Erfüllung öffentlicher Aufgaben eingesetzt werden können

oder sogar müssen. Erprobungsgesetze wie ein Smart Government Gesetz und ein Smart Justice Gesetz können helfen, erste Erfahrungen zu sammeln, Kompetenzen aufzubauen und Kapazitäten zu halten. Mit Blick auf historische Erfahrungen wird die Sorge vor einem smarten Überwachungsstaat dauernd bestehen bleiben. Mit Augenmaß müssen Politik, Verwaltung und Justiz Wege finden, wie einerseits die öffentliche Sicherheit gewährleistet bleibt und andererseits die Bevölkerung nicht unverhältnismäßig überwacht wird. Diskurse, Debatten und die Festlegung der rechtlichen Rahmenbedingungen werden dazu beitragen, die Risiken und Gefahren eines smarten Überwachungsstaats zu erkennen, zu reduzieren und zu verhindern.

8. Literatur

acatech, Cyber-Physical Systems – Innovationsmotor für Mobilität, Gesundheit, Energie und Produktion, acatech POSITION, Springer Verlag, Heidelberg 2011.

Geisberger, Eva / Broy, Manfred, agendaCPS – Integrierte Forschungsagenda Cyber-Physical Systems, acatech Studie, acatech – Deutsche Akademie der Technikwissenschaften e.V., München/Garching 2012.

GovTech, Factsheet Smart Nation Sensor Platform, Singapur 2017.

Lee, Hsien Loong, National Day Rally 2017 English Speech, Prime Minister's Office, Singapur 2017.

von Lucke, Jörn, Smart Government – Wie uns die intelligente Vernetzung zum Leitbild «Verwaltung 4.0» und einem smarten Regierungs- und Verwaltungshandeln führt, Zeppelin Universität gemeinnützige GmbH, Friedrichshafen 2015.

von Lucke, Jörn, Internet-Trends bringen neue Fragestellungen für die Rechts- und Verwaltungsinformatik, in: Erich Schweighofer / Franz Kummer / Walter Hötzendorfer / Christoph Sorge (Hrsg.): Trends und Communities der Rechtsinformatik, Band 326, Österreichische Computergesellschaft, Wien 2017, S. 225–232.

von Lucke, Jörn, In welcher smarten Welt wollen wir eigentlich leben?, in: Verwaltung & Management, 24. Jahrgang, Heft 4, Baden-Baden 2018, S. 177–196.

von Lucke, Jörn, Schöne neue Welt?, Smart Government, in: zu Daily, Zeppelin Universität, Friedrichshafen 2018b, Online: https://www.zu-daily.de/daily/zuruf/2018/09-19_von-lucke-schoene-neue-welt.php.

von Lucke, Jörn, Von smarten Städten zu Smart Government – Eindrücke aus Südkorea, Japan und den Vereinigten Arabischen Emiraten, in: Erich Schweighofer / Franz Kummer / Ahti Saarenpää / Burkhard Schafer (Hrsg.): Datenschutz / LegalTech – Data Protection / Legal Tech, Editions Weblaw, Bern 2018c, S. 339–348.

von Lucke, Jörn, Disruptive Modernisierung von Staat und Verwaltung durch den gezielten Einsatz von smarten Objekten, cyberphysischen Systemen und künstlicher Intelligenz, in: Michael Räckers et. al. (Hrsg.): Fachtagung Verwaltungsinformatik 2019, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2019, in Druck.

Paganini, Pierluigi, The NSA wants to exploit IoT devices for surveillance and sabotage, Security Affairs, 2016, Online: https://securityaffairs.co/wordpress/48319/iot/nsa-iot-devices.html.

Forschungsunion Wirtschaft – Wissenschaft und acatech – Deutsche Akademie der Technikwissenschaften e.V., Deutschlands Zukunft als Produktionsstandort sichern – Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, Abschlussbericht des Arbeitskreises Industrie 4.0, Frankfurt 2013.

Snowden, Edward, The Snowden Files – Dates when PRISM Collection Began For Each Provider, The Guardian/Der Spiegel, London/Hamburg 2013.

VDE-ITG, Positionspapier «Das Taktile Internet», Die Informationstechnische Gesellschaft im Verband der Elektrotechnik Elektronik Informationstechnik e.V., Frankfurt 2014.