DEUTSCHES FORSCHUNGSINSTITUT FÜR ÖFFENTLICHE VERWALTUNG SPEYER
GERMAN RESEARCH INSTITUTE FOR PUBLIC ADMINISTRATION SPEYER

Mario Martini
unter Mitarbeit von
Saskia Fritzsche und Michael Kolain

Digitalisierung als Herausforderung und Chance für Staat und Verwaltung

Forschungskonzept des Programmbereichs „Transformation des Staates in Zeiten der Digitalisierung“

FÖV 85
Discussion Papers

Mario Martini
unter Mitarbeit von
Saskia Fritzsche und Michael Kolain

Digitalisierung als Herausforderung und Chance für Staat und Verwaltung

Forschungskonzept des Programmbereichs „Transformation des Staates in Zeiten der Digitalisierung“

FÖV 85
Discussion Papers

Deutsches Forschungsinstitut für öffentliche Verwaltung Speyer

2016

Gefördert durch die Bundesrepublik Deutschland

Das Werk ist in allen seinen Teilen urheberrechtlich geschützt.
Zitierhinweis: Martini, Digitalisierung als Herausforderung und Chance für Staat und Verwaltung, Speyer 2016.

Nicht im Buchhandel erhältlich
Schutzgebühr: € 5,-
Bezug: Deutsches Forschungsinstitut
für öffentliche Verwaltung Speyer
Postfach 14 09
67324 Speyer
http://www.foev-speyer.de

ISSN 1868-971X (Print)
ISSN 1868-9728 (Internet)

Mario Martini

Leiter des Programmbereichs „Transformation des Staates in Zeiten der Digitalisierung“ und Inhaber des Lehrstuhls für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht an der Deutschen Universität für Verwaltungswissenschaften Speyer

Saskia Fritzsche

Richterin in Hamburg; zuvor Forschungsreferentin am FÖV Speyer

Michael Kolain

Forschungsreferent im Programmbereich „Transformation des Staates in Zeiten der Digitalisierung“

Vorwort

Die Digitalisierung hat sich zu einem Motor grundlegender, dynamischer Veränderungsprozesse in Staat und Gesellschaft entwickelt. In diesem Prozess hat die deutsche *Industrie* als Werkbank der Welt mit hervorragend ausgebildeten Ingenieuren das Zeug zum Musterschüler im digitalen Universum. Die öffentliche *Verwaltung* gilt demgegenüber als Sorgenkind. Schon seit den Anfängen des digitalen Wandels hält sie mit der dynamischen technischen Entwicklung der wirtschaftlichen Welt nicht vollständig Schritt – dabei sollte ihr im Idealfall gerade die Rolle des Impulsgebers gesamtgesellschaftlichen Fortschritts zukommen. Der Schatz an Daten, den der Staat hütet, kann durch digitale Öffnung einerseits enormes wirtschaftliches Wertschöpfungspotenzial entfalten (Open Data); andererseits können die Effizienzvorteile digitaler Techniken den Wirtschaftsakteuren und der Gesellschaft in erheblichem Umfang staatliche Transaktionskosten ersparen. Nicht zuletzt kann die Digitalisierung eine lebendige Kultur der Partizipation, des gesellschaftlichen Austauschs und der demokratischen Entfaltung beflügeln.

Bei der digitalen Transformation der Verwaltung wächst der Forschung eine wichtige Impuls-, Beratungs- und Unterstützungsfunktion zu: Staat, Wirtschaft und Gesellschaft eint ein elementares Interesse an einer wissenschaftlichen Begleitung des digitalen Wandels. Der Bestand an Literatur, die sich mit Erscheinungsformen der Digitalisierung befasst, hat in der jüngeren Vergangenheit enormen Zuwachs erfahren. Ein ganzes Arsenal an Forschungsprojekten unterschiedlichster Disziplinen wendet sich der thematischen Aufbereitung und Begleitung der digitalen Transformation zu. Das gilt in besonderer Weise für die Informatik, die Politikwissenschaft, die Soziologie und die Ökonomik. Sie begleiten den nachhaltigen Veränderungsprozess, den die Digitalisierung über Staat und Gesellschaft gebracht hat, in ihrer Breite und Tiefe mit dem Anspruch, die damit einhergehenden Auswirkungen und das Gestaltungspotenzial auszuloten. Gerade die Informatik, insbesondere die Verwaltungsinformatik, verknüpft dies immer stärker mit dem Anspruch, die ethischen und regulatorischen Implikationen technischer Veränderungen zu erfassen und darauf normative Ableitungen zu gründen.

Die Rechtswissenschaft hinkt der Entwicklung bislang wohl am weitesten hinterher. Gemessen an der Zahl rechtswissenschaftlicher Forschungseinrichtungen befasst sich nur ein verschwindend kleiner Anteil von Juristen mit Digitalisierungsfragen. Das gilt in besonderer Weise für die Staatsrechtslehre. Dabei ist gerade die deutsche Verwaltung, die traditionell von einer legalistischen Kultur geprägt ist, auf die wissenschaftliche Begleitung durch rechtswissenschaftliche Analyse angewiesen.

So ist es konsequent, dass das Deutsche Forschungsinstitut für öffentliche Verwaltung (FÖV) – als traditionell in besonderem Maße mit juristischem Sachverstand bestückter „Thinktank" – einen klaren Forschungsschwerpunkt auf die Digitalisierung der Verwaltung legt: Seit Januar 2016 operiert der Programmbereich „Transformation des Staates in Zeiten der Digitalisierung" als wissenschaftlicher Ansprechpartner für Bund und Länder in Digitalisierungsfragen. Diese Ausrichtung ist zugleich Ausdruck des institutionellen Transformationsprozesses, den das Forschungsinstitut selbst in jüngster Zeit durchlaufen hat: Das FÖV fokussiert sich stärker thematisch und bündelt seine Ressourcen für eine konzentrierte Behandlung ausgewählter Themenbereiche, die für Staat und Gesellschaft nachhaltige Transformationsdynamiken auslösen.

Der Programmbereich „Transformation des Staates in Zeiten der Digitalisierung" bleibt dabei dem Handlungsmotto des Forschungsinstituts treu: „Forschung *über* und *für* die öffentliche Verwaltung". Er zielt auf eine wissenschaftlich exzellente Forschung, deren Ergebnisse in die politische und administrative Praxis einfließen können und damit wissenschaftlichen Anspruch sowie praktische Verwertbarkeit der Ergebnisse miteinander verbindet.

In einem von technischen Innovationen geprägten, sich immer schneller wandelnden Umfeld steigt die Bedeutung einer ausbalancierten Verteilung zwischen Grundlagen- und anwendungsorientierter Forschung. So entspricht es dem Selbstverständnis des Programmbereichs, in seinen Projekten wissenschaftlich anspruchsvolle Forschungsfragen zu beantworten, die aufgrund ihrer konkreten Themenstellung und Ausrichtung zugleich einen praktischen Mehrwert für die Verwaltung versprechen. Diesen Spagat meistern zu können, ist eine der Stärken des Forschungsstandorts in Speyer.

Diesem Anspruch verpflichtet, versteht der Programmbereich es als seine Aufgabe, die grundlegenden Wandlungen wissenschaftlich zu begleiten, denen sich Staat und Verwaltung in einem dynamischen Prozess technologischer Veränderungen ausgesetzt sehen. Mit diesem Transformationsprozess verbinden sich nicht nur Herausforderungen. Er birgt vor allem viele Chancen, die es zu nutzen gilt. Zu ergründen, wo die Potenziale des digitalen Wandels liegen und wie sie sich zum Wohle aller Mitglieder eines Gemeinwesens heben lassen, gehört zu den vornehmsten Aufgaben wissenschaftlicher Arbeit.

Allen Forschungsthemen des Programmbereichs ist dabei ein regulatorischer Anspruch gemeinsam. Sie zielen mit unterschiedlicher fachlicher Schwerpunktsetzung darauf ab, Handlungsempfehlungen für Anpassungen der Steuerungsressourcen „Recht, Verfahren und Organisation“ in dem Transformationsprozess des digitalen Wandels zu erarbeiten. Sie eint die übergreifende Forschungsfrage: Wie kann der Staat das Potenzial der Digitalisierung für die Erreichung seiner Zwecke nutzen, ohne dabei gesellschaftlich anerkannte und normativ verankerte Grundüberzeugungen des Persönlichkeitsschutzes, das Gebot rechtsstaatlicher Bindung und – damit verbunden – die innere Glaubwürdigkeit staatlichen Handelns infrage zu stellen.

Mit seinem rechtswissenschaftlichen Schwerpunkt schließt der Programmbereich „Digitalisierung“ ein Stück weit eine Lücke in der sich bildenden wissenschaftlichen Phalanx. Im Verbund mit anderen Disziplinen richtet er einen konzentrierten, interdisziplinären Blick auf die Dynamiken, welche die Digitalisierung für den Staat im Allgemeinen und die öffentliche Verwaltung im Besonderen auslöst. Eigener Anspruch des Programmbereichs ist dabei, die unterschiedlichen Perspektiven derjenigen Wissenschaftsdisziplinen, die sich mit dem Phänomen der Digitalisierung auseinandersetzen, am Forschungsinstitut zu integrieren und sie im Rahmen einer Grundlagenforschung zu einer übergreifenden Erkenntnisschicht zu amalgamieren. Aus seinen interdisziplinär gewonnenen wissenschaftlichen Einsichten generiert der Programmbereich integrative Lösungen. Die Kooperation mit technischen Wissenschaften versteht er dabei alles andere als Selbstzweck, denn – um es in den Worten zweier renommierter Datenforscher zu sagen: „Gesetzge-

berischer Eingriff und Regulation erfordern nicht nur Klarheit in den Zielen, sondern auch Verständnis der Entwicklungen und der zur Verfügung stehenden Instrumente“[1].

Das Forschungsprogramm hat den Beiräten des Forschungsinstituts – Nutzerbeirat, Wissenschaftlicher Beirat und Verwaltungsrat – vor dem Start des Programmbereichs zur Begutachtung vorgelegen. In einer aktualisierten und stark gekürzten, insbesondere um reine Institutsinterna bereinigten Fassung macht der Programmbereich seine Forschungsprojekte der Öffentlichkeit zugänglich – zu Informationszwecken und als Beitrag zum wissenschaftlichen Diskurs.

Besonderer Dank gilt allen, die an der Entstehung und Verbesserung dieses Forschungsprogramms mitgewirkt haben, insbesondere den Beiräten des Instituts sowie den Senior Fellows Prof. Dr. *Ines Mergel*, Prof. Dr. *Christoph Sorge*, Prof. Dr. *Hermann Hill*, Prof. Dr. *Helmut Krcmar*, Prof. Dr. Dr. h.c. (NUM) *Jan Ziekow*, der Verbundkoordinatorin Dr. *Nadja Braun Binder*, ferner den Forschungsreferenten des Programmbereichs Dr. *Florian Ammerich*, *Martin Feldhaus, Michael Kolain, Manuel Misgeld, Manfred Müller, David Nink, Tobias Rehorst, David Wagner, Quirin Weinzierl*, *Markus Wojtczak* sowie meiner langjährigen Mitarbeiterin *Saskia Fritzsche*.

Speyer, im November 2016 *Mario Martini*

1 *Hofmann/Schölkopf*, Vom Monopol auf Daten ist abzuraten, FAZ vom 29.1.2015, S. 14.

Inhaltsverzeichnis

A. Transformationsimpulse des digitalen Wandels für die öffentliche Verwaltung und gesetzgeberische Regulierungsstrategien 1

I. Chancen technischer Entwicklungsdynamik 1

1. Ökonomische Dimension 1

2. Gesellschaftliche Dimension 2

3. Politisch-administrative Dimension 4

II. Herausforderungen und Steuerungsaufgaben 5

1. Rahmenbedingungen 5

a) Taktfrequenz erforderlicher Anpassungen 5

b) Reichweite des Anpassungsbedarfs 6

c) Unausgeschöpfte Potenziale des Status quo 6

2. Digitale Sicherheit 10

3. Persönlichkeitsschutz 12

4. Technologische Abhängigkeiten 14

a) Abhängigkeiten der Verwaltung von privaten Dienstleistern 14

b) Abhängigkeit des Individuums von digitalen Angeboten als Teilhabevoraussetzung 15

5. Digitale Infrastruktur 17

6. Benutzerfreundlichkeit 19

7. Digitale Automatisierung und Autonomisierung 21

8. Digitale Organisationskultur 22

B. Zielmarken digitaler Staatlichkeit und ihrer wissenschaftlichen Begleitung 23

I. Leitbild der Staats- und Verwaltungstransformation durch digitalen Wandel 23

II. Selbstverständnis des Programmbereichs 24

III. Aus dem Erkenntnisinteresse und identifizierten Forschungsthemen abgeleitete übergreifende Forschungsfrage des Programmbereichs 25

1. Identifizierung und Auswahl der Forschungsthemen ... 25

2. Umwälzungsprozesse der Digitalisierung und ihre Herausforderungen für Staat und Verwaltung 26

C. Transformationsdynamiken einer standardmäßig digital agierenden Verwaltung (Kernforschungsthemen) 29
I. Die Dynamisierungsprozesse verbindende, übergreifende Leitaspekte 32
1. Gemeinwohlförderung unter den Bedingungen digitaler Mensch-Maschine-Interaktion 33
2. Datensouveränität 35
a) Realbefund 35
b) Schlussfolgerungen 36
3. Transnationalität 38
II. Datengestützte Erfüllung öffentlicher Aufgaben 39
1. Algorithmenkontrolle als Regulierungsaufgabe 42
a) Diskriminierungsverbote 45
b) Kontrollmechanismen 45
aa) Regulierungsansätze des unionalen Datenschutzrechts 45
bb) Algorithmenkontrolle im „Internet der Dinge“ 46
2. Smart Cities‘ Government: staatliche Infrastrukturaufgaben in der digitalen Welt 47
3. Social-Media-Monitoring durch die öffentliche Verwaltung 50
4. Mitgliedstaatliche Regelungsspielräume unter der Datenschutz-Grundverordnung 53
5. Das Once-only-Principle als datenschutzkonforme Strategie eines ebenenübergreifenden E-Governments? 56
6. Regelungsbedarf und rechtliche Grenzen elektronischer vollautomatisierter Verwaltungsverfahren 57
III. Digitale Sicherheitsarchitektur 59
1. Ein digitales Ordnungsrecht 60
2. Schutzmechanismen der digitalen Kommunikation 63
a) Vertrauen in die technische Infrastruktur als Schlüsselelement digitaler Entwicklungsperspektiven 64
b) Digitales Identitätsmanagement 65

IV. Öffentlich-private Kooperationsfelder im digitalen Raum 66
1. Kooperative eingebettete Systeme: Vernetzung der öffentlichen Verwaltung mit intelligenten Industrie 4.0-Umgebungen 67
2. Datenschutzrechtliche Verantwortungsstrukturen in komplexen Online-Akteursnetzwerken 70
V. Digital Public Management 72
1. Organisationsprinzipien des Mobile Government 74
2. IT-Inkubator öffentliche Verwaltung 76
3. Open-Innovation-Wettbewerbe der öffentlichen Hand – Bürger und Staat als kollaborative Gesellschaftsintrapreneure 79
4. Digital-transformationale Führung in der Netzwerkverwaltung 81

D. Personen 84
I. Senior Fellows 84
II. Forschungsreferenten 85

E. Erste Teilergebnisse 86
I. Im Jahr 2016 veröffentlichte Werke (geordnet nach Erscheinungsdatum) 86
II. Zur Veröffentlichung eingereichte, noch nicht erschienene Werke 88

F. Literaturverzeichnis 89

A. Transformationsimpulse des digitalen Wandels für die öffentliche Verwaltung und gesetzgeberische Regulierungsstrategien

Der digitale Wandel durchdringt unaufhaltsam alle Bereiche des gesellschaftlichen, wirtschaftlichen und politischen Lebens. Das Internet vernetzt Akteure, Objekte und Räume sowohl im privaten als auch im öffentlichen Raum; es eröffnet neue Kanäle für die individuelle sowie die kollektive Kommunikation. Längst erschöpft sich das Internet nicht mehr in einem Vermittlungskanal für E-Mails, einer digitalen Bibliothek und einer virtuellen Agora. Ganze Produktionsabläufe, Steuerungsvorgänge und Interaktionsmuster, die bislang notwendig in der realen Welt verortet waren, verlagern sich in ein „Internet der Dinge und Dienste“[2] sowie in die sozialen Medien des Web 2.0. Seit Jahrzehnten etablierte Geschäftsmodelle – vom Bankensystem über die Automobilindustrie bis hin zum Taxi- und Hotelgewerbe – rüttelt die Digitalisierung durcheinander, ja wälzt sie teilweise gleichsam wie eine Planierraupe nieder. Der digitale Paradigmenwechsel hat Dimensionen der Unumkehrbarkeit erreicht. Alles, was sich digitalisieren lässt, steht im Begriff auch digitalisiert zu werden.

I. Chancen technischer Entwicklungsdynamik

1. Ökonomische Dimension

Die wirtschaftliche Bedeutung der digitalen Revolution zu erkennen, braucht keine prophetische Gabe. Bereits der Blick auf die Forbes-Liste der weltweit wertvollsten Unternehmensmarken macht deutlich: Sechs von zehn Marken entstammen heute Unternehmen der Digitalwirtschaft

2 Engl.: Internet of Things (IoT). Vgl. zur Einführung etwa *Andelfinger/Hänisch*, Internet der Dinge, 2015; *Sprenger/Engemann* (Hrsg.), Internet der Dinge, 2015. Zum „Internet der Dienste“ etwa *Heuser/Wahlster* (Hrsg.), Internet der Dienste, 2011; *Raabe/Wacker/Oberle et al.*, Recht ex machina: Formalisierung des Rechts im Internet der Dienste, 2012, S. 33 ff.

– die meisten von ihnen sind erst wenige Jahre alt.[3] All diesen Unternehmen ist das Geschäftsmodell gemeinsam, Daten als den Rohstoff der Zukunft zu veredeln. Sie füllen ihre Datenarsenale mit atemberaubender Geschwindigkeit und haben diese zu wahren Goldspeichern ausgebaut.

Die weltweite Verknüpfung unterstützt den Ideenaustausch, die Verbreitung von Informationen sowie die Zusammenarbeit von Menschen und Unternehmen. Die damit verbundene drastische Reduktion von Transaktionskosten trägt wesentlich zu Innovationen sowie zur allgemeinen Wertschöpfung bei.[4]

2. Gesellschaftliche Dimension

Das Internet ist im Jahr 2016 in der Mitte der Gesellschaft angekommen. 58 % der deutschsprachigen Bevölkerung sind privat und/ oder beruflich täglich im Internet unterwegs (im Jahr 2012 waren es noch 38 %) – mehr als 78 % zumindest mehrfach pro Woche.[5] Damit geht auch ein geändertes Nutzungsverhalten in allen Altersgruppen einher: Zu beobachten ist insbesondere eine stärkere Verwendung von Smartphones und (damit korrespondierend) eine wachsende mobile Nutzungsdauer sowie ein aktiveres Verhalten in sozialen Netzwerken.[6] Der Anteil der Personen, die das Internet weder privat noch beruflich nutzen

---

3 Die wertvollsten Marken sind (in absteigender Reihenfolge): Apple, Google, Microsoft, Coca-Cola, Facebook, Toyota, IBM, The Walt Disney Company, McDonald‘s, General Electric. Facebook (2004) und Google (1997) sind erst wenige Jahre alt. Vgl. Forbes, Liste der wertvollsten Unternehmensmarken, http://www.forbes.com/pictures/mli45fflfg/1-apple/#25713ad97d28 (5.10.2016).

4 World Economic Forum, The Global Information Technology Report 2016, 2016, S. 40. Vgl. auch McKinsey Global Institute, Internet matters: The Net`s sweeping impact on growth, jobs, and prosperity, 2011, S. 16, 21, 22: Das Internet schafft insgesamt mehr Arbeitsplätze, als es überflüssig macht.

5 Deutsches Institut für Vertrauen und Sicherheit im Internet, DIVSI Internet-Milieus 2016: Die digitalisierte Gesellschaft in Bewegung, 2016, S. 15. Nach *Koch/Frees*, Media Perspektiven 2016, 418, 421, sogar 65,1 % täglich.

6 Deutsches Institut für Vertrauen und Sicherheit im Internet (Fn. 5), S. 15 ff. Ähnlich Initiative D21, Digital-Index 2016, 2016, S. 12 f. Zur Nutzungsdauer unterwegs siehe auch *Koch/Frees* (Fn. 5), 424.

(sog. „Offliner“, zu 85 % Rentner)[7] sank unterdessen von 20 % im Jahr 2012 auf 16 % im Jahr 2016.[8] Die Aufgeschlossenheit gegenüber den Vorteilen des Internets wächst weiterhin: Insgesamt 72 % der Deutschen sehen im Internet mehr Chancen als Risiken.[9] Der Gruppe der sog. „internetfernen Verunsicherten“ gehört nur noch eine kleine Minderheit der Bevölkerung an.[10]

Es zeichnet sich ab, dass in Zukunft ohne digitale Teilhabe auch nur eingeschränkt soziale Teilhabe möglich ist. Denn Kommunikation findet zunehmend über Messenger-Dienste (z. B. WhatsApp) und soziale Netzwerke statt.[11] Dies trifft nicht nur auf jüngere Menschen zu, die in der Altersgruppe der 14-29-Jährigen zu 95 % soziale Netzwerke nutzen. Insbesondere in der Altersgruppe der 30-64-Jährigen hat die Nutzung von Messenger-Diensten und sozialen Netzwerken seit 2012 stark zugenommen.[12]

---

7 Deutsches Institut für Vertrauen und Sicherheit im Internet (Fn. 5), S. 23.

8 Deutsches Institut für Vertrauen und Sicherheit im Internet (Fn. 5), S. 14. Ähnlich *Koch/Frees* (Fn. 5), 420: 16,2 % Offliner. Diese Zahl bedeutet jedoch nicht, dass diese Gruppe keinerlei Zugang zum Internet hätte: 83 % der „Offliner“ geben an, dass sie zumindest Internetrecherchen für sich durch andere Personen erledigen lassen, s. Deutsches Institut für Vertrauen und Sicherheit im Internet (Fn. 5), S. 24.

9 Deutsches Institut für Vertrauen und Sicherheit im Internet (Fn. 5), S. 20.

10 Deutsches Institut für Vertrauen und Sicherheit im Internet (Fn. 5), S. 70. Dieser Befund soll aber nicht darüber hinwegtäuschen, dass die fortschreitende Digitalisierung für viele Bürger (noch) eine Herausforderung darstellt. Kritisch sehen Studien insbesondere den Grad der Kompetenz im Umgang mit der Datenverarbeitung, der Sicherheit und im Umgang mit neuen Begrifflichkeiten, s. Initiative D21 (Fn. 6), S. 38 ff. 26 % der Bürger weisen nur einen niedrigen Digitalisierungsgrad auf („digital Abseitsstehende“), 43 % einen mittleren („Digital Mithaltende“) und nur 31 % einen hohen Digitalisierungsgrad („digital Vorreitende“), s. Initiative D21 (Fn. 6), S. 28 f.

11 Deutsches Institut für Vertrauen und Sicherheit im Internet (Fn. 5), S. 17; *Koch/Frees* (Fn. 5), 429.

12 Deutsches Institut für Vertrauen und Sicherheit im Internet (Fn. 5), S. 18.

3. Politisch-administrative Dimension

Nicht nur für das Leben und Arbeiten der Menschen, sondern auch für die Beziehungen zwischen Bürger und Verwaltung zeitigt das Internet disruptive Veränderungen. An die Stelle der papiergebundenen Antragsverwaltung mit persönlicher Vorsprache tritt immer stärker die elektronische Kommunikation, an die Stelle der Papierakte die E-Akte. Im Grundsatz ist das auch wünschenswert: Die Digitalisierung nimmt Staat, Gesellschaft und Privaten Transaktionskosten in substanziellem Umfang ab. Die neuen Möglichkeiten der Informationsgewinnung und Datenanalyse (Algorithmen, Netzwerkarchitektur etc.) verschaffen der Verwaltung neue Gestaltungsmöglichkeiten zur gemeinwohlorientierten Aufgabenerledigung. Bislang scheinbar wertlosen, unstrukturierten Daten hauchen Big-Data-Algorithmen durch intelligente Verknüpfung, das Aufspüren bislang unerkannter Muster und die Nutzung sich stetig verbessernder Prozessorleistungen neues Leben ein. Der damit verbundene Gemeinwohlnutzen erstreckt sich von der Planung und Steuerung öffentlicher Infrastrukturen über die Suche nach Partizipationsbedarf im digitalen Raum bis hin zur Vereinfachung bzw. (Voll-)Automatisierung von Verwaltungsverfahren. Nicht nur Wirtschaftsunternehmen, sondern auch Sicherheitsbehörden eröffnen sich im Internet ungeahnte Möglichkeiten der Begleitung und Steuerung gesellschaftlicher Vorgänge und individuellen Verhaltens – aber auch die informationelle Selbstbestimmung gefährdender Überwachung. Was früher umständlich unter Rückgriff auf menschliche Quellen, durch Observationen und Kommunikationsüberwachung zusammengetragen werden musste, lässt sich nun mit wenigen Klicks bündeln und zu einem detaillierten Persönlichkeitsprofil zusammenfügen. Es erschließen sich ganz neue Ermittlungsmethoden und Potenziale ebenenübergreifender Zusammenarbeit.

II. Herausforderungen und Steuerungsaufgaben

1. Rahmenbedingungen

a) Taktfrequenz erforderlicher Anpassungen

Die Uhr des digitalen Wandels tickt nicht nur schnell, sondern auch scheinbar unaufhaltsam. Längst haben *Bürger* und *Unternehmen* die technischen Neuerungen in ihren Alltag integriert.[13] Will die *öffentliche Hand* von der Faktizität der technischen und darauf aufbauenden sozialen Entwicklungen nicht überrollt werden und ihre Fähigkeit zur zielgerichteten gesellschaftlichen Steuerung nicht verlieren, muss sie binnen enger Zeitfenster funktionale Lösungen für die Erfüllung hoheitlicher Aufgaben bereitstellen. Die öffentliche Verwaltung muss auf neue technologische Entwicklungen und veränderte Bedürfnisse des *Homo digitalis* rechtzeitig reagieren. Sie sieht sich dabei einem ständigen Wettlauf ausgesetzt: Denn die technische Entwicklung eilt dem Recht und der es ausführenden öffentlichen Verwaltung in kaum einholbarer Geschwindigkeit voraus und schlägt dabei kaum vorhersehbare Haken. Sie lässt sich ihren Takt nicht durch Gesetzgeber und Exekutive vorgeben. Das Internet als zentrale Infrastrukturressource der digitalisierten Informationsgesellschaft gleicht insoweit – in den Worten von *Bill Gates* – einer Welle: „Entweder man lernt, auf ihr zu schwimmen, oder man geht unter."

Was zunächst der ungezwungenen Experimentier- und Innovationsfreude der Akteure überlassen war, entwickelt sich für den öffentlichen Sektor immer mehr auch zu einem Veränderungsdruck. Soll die Digitalisierung chancenreiche Transformationsimpulse (statt krisenhafter Anpassungsprozesse) für den Staat als Ordnungssystem und Institutionengefüge auslösen, bedarf es durchdachter, vernetzter sowie ebenenübergreifender Planungen und Entscheidungen. Nur mithilfe eines ganzheitlichen Ansatzes kann der öffentliche Sektor mit der digitalen Entwicklung Schritt halten und ihre Potenziale für das Gemeinwohl fruchtbar machen.

---

13 World Economic Forum (Fn. 4), S. 19: Deutschland belegt Platz 6 bzw. 18 von 139 Ländern hinsichtlich der unternehmerischen bzw. privaten Nutzung des Internets.

b) Reichweite des Anpassungsbedarfs

Die digitale Transformation fordert der öffentlichen Verwaltung mehr als nur partielle Modifikationen ab. Über alle Teilsysteme hinweg setzt sie Verwaltungsorganisation, Verwaltungsverfahren und -handeln einem nachhaltigen Innovations- und Umbildungsprozess aus. Neue Verwaltungsaufgaben entstehen, es bedarf grundlegender Verfahrensumgestaltungen und einer umfassenden Anpassung des geltenden Rechtsrahmens. In Rede steht dabei weniger eine punktuelle Weiterentwicklung als eine Zeitenwende in der öffentlichen Verwaltung. Dort, wo die digitale Transformation auf staatlich-institutionelle Kontinuitätssicherungsmechanismen, namentlich auf persistente Legitimations- und Funktionsgewährleistungen trifft, gilt es, funktionale Äquivalente zu identifizieren und ggf. zu entwickeln oder neue Wege der Aufgabenwahrnehmung zu gehen.

c) Unausgeschöpfte Potenziale des Status quo

Die Gestaltung der digitalen Verwaltung der Zukunft ist bereits seit geraumer Zeit ein zentrales Anliegen der Regierungen auf Bundes- und Landesebene[14] sowie der Europäischen Kommission[15]. Ihre Priorisierung folgt keinem Selbstzweck. So wie der Staat es einerseits vermeiden sollte, unbesehen jedem Trend zu folgen, ist er andererseits stets gefordert, gesellschaftliche Veränderungen im Blick zu behalten und sich veränderten Realitäten anzupassen. Die Adaption der Aufgaben und Verfahren an tatsächliche Verschiebungen, die sich im gesellschaftlichen Koordinatensystem vollziehen, ist Bestandteil des originären verfassungsrechtlichen Auftrages der Legislative und Exekutive.

Das Potenzial, das die Digitalisierung in sich trägt, schöpft die deutsche Verwaltung bislang nur ansatzweise aus.[16] Von einem standardmäßig digitalisierten Verfahren und der Regelnutzung elektronischer Verwaltungsangebote ist sie noch ein gutes Stück entfernt. (Nur) 45 %

---

14 Bundesregierung, Digitale Agenda 2014-2017, 2014, S. 19 ff.; Bundesregierung, Digitale Verwaltung 2020, 2014, S. 10 ff.; für die Länder siehe beispielsweise Hessische Landesregierung, Strategie Digitales Hessen, 2016, S. 16 ff.

15 Europäische Kommission, EU-eGovernment-Aktionsplan 2016-2020, COM(2016) 179 final, 2016, S. 2 ff.

16 Initiative D21, eGovernment Monitor 2016, 2016, S. 8.

der Deutschen nutzen E-Government-Angebote.[17] Der Kontakt mit einer digitalen Verwaltung erschöpft sich dabei weitgehend darin, Informationen einzuholen (z. B. Öffnungszeiten oder Checklisten), dient aber weniger dazu, konkrete Anträge zu stellen oder Verfahren vollständig abzuwickeln.

Das Bild Deutschlands, das internationale Vergleichsstudien zur E-Government-Weltliga zeichnen, ist unbefriedigend: Bei dem UN-E-Government Report 2016 kommt Deutschland nicht über Rang 15 von 193 Staaten hinaus.[18] Das Waseda-IAC International e-Government Ranking weist Deutschland Rang 19 unter 65 Staaten zu. Die Spitzenplätze nehmen Singapur (1), die USA (2), Dänemark (3) Korea (4), Japan (5) und Estland (6) ein.[19]

Auch im europäischen Vergleich bleibt Deutschland als wirtschaftliche Lokomotive der Union hinter seinen Möglichkeiten zurück: Der EU-Index für die digitale Wirtschaft und Gesellschaft (DESI) verortet die Bundesrepublik sub specie der digitalen Bereitstellung öffentlicher Dienste und Dienstleistungen[20] im europäischen Mittelfeld:[21] Während in der EU durchschnittlich 32 % der Bürger digitale Verwaltungsangebote umfangreich bedienen, insbesondere Formulare online einreichen, nutzen nur 19 % der Deutschen solche Angebote.[22] In keiner anderen

---

17 Initiative D21 (Fn. 16), S. 8, 12 f.

18 United Nations, UN E-Government Survey 2016, 2016, S. 111. Deutlicher noch World Economic Forum (Fn. 4), S. 19, 27: Platz 30 von 139 Ländern für die staatliche Nutzung des Internets.

19 Waseda University/International Academy of CIO, The 12th Waseda-IAC International e-Government Rankings Survey 2016 Report, 2016, S. 1.

20 Unter den Indikator „Digitale öffentliche Dienste/Dienstleistungen“ (Digital Public Services) fasst der DESI die Dimensionen „E-Government“ und „E-Health“. Diese untergliedern sich wiederum in die Indikatoren „E-Government Users“, „Pre-filled Forms“, „Online Service Completion“ und „Open Data“ auf der einen Seite sowie „Medical Data Exchange“ und „E-Prescription“ auf der anderen Seite, vgl. http://digital-agenda-data.eu/datasets/desi/indicators (28.11.2016).

21 Europäische Kommission, Digital Economy and Society Index – Country Profile Germany, 2016, S. 6.

22 Europäische Kommission (Fn. 21), S. 6. Auch auf die gesamte Nutzung digitaler Angebote bezogen (z. B. zu Informationszwecken) liegen Deutsche im Verhältnis zu anderen EU-Staaten zurück (45 % im Vergleich zu 74 % in Österreich), s. Initiative D21 (Fn. 16), S. 8.

Kategorie schnitt Deutschland bei dem „Digital Progress Report“ der EU-Kommission so schlecht ab wie im Bereich „Digital Public Services“.[23]

In der Tat machen die Deutschen von den vorhandenen Angeboten wenig Gebrauch. Eine Mehrzahl der Bürger (57 % der Befragten) kennt viele der Online-Angebote überhaupt nicht. 45 % der Menschen in Deutschland lehnen in Befragungen Online-Angebote grundsätzlich als zu komplex bzw. als in der Struktur nur schwer überschaubar ab.[24] Zudem erklärt fast die Hälfte der Befragten, dass sie Online-Angebote frühestens dann (intensiver) nutzen werden, wenn Verwaltungsverfahren sich umfänglich online abwickeln lassen.[25] Es zeigt sich: Die Verwaltung muss noch zahlreiche Hürden überwinden, bis sie das Potenzial der Digitalisierung vollständig ausschöpfen kann.[26]

So überrascht es auch nicht, dass der Nationale Normenkontrollrat der Bundesrepublik in einem Gutachten auf dem Weg der Digitalisierung der Verwaltung reichlich Optimierungspotenzial bescheinigt: Die Bundesrepublik setze bislang auf einzelne „Leuchtturmprojekte“ und webe einen digitalen Flickenteppich, der kaum nutzerfreundliche Angebote für seine Bürger bereithalte[27]; mangels ebenenübergreifender Digitalisierungsstrategien seien die gut gemeinten Angebote, welche die föderalen Einheiten hervorgebracht haben, als punktuelle Lösungen untereinander nur wenig kompatibel.[28] In dem komplexen System des deutschen Föderalismus sind die vorhandenen Insellösungen in der Tat kaum in der Lage, zu einer übergreifenden und flächendeckenden Digitalisierung der Verwaltung beizutragen.[29]

Gleichzeitig gilt es aber nicht zu verkennen: Deutschland hat in der Digitalisierung in den vergangenen Jahren auch substanzielle Fortschritte erzielt. Der IT-Staatsvertrag setzt (trotz seines Ausbaubedarfs

---

23 Europäische Kommission (Fn. 21), S. 6.

24 Initiative D21 (Fn. 16), S. 16.

25 46 % der Befragten, s. Initiative D21 (Fn. 16), S. 16.

26 Zu weiteren Barrieren (z. B. Datenschutz) s. Initiative D21 (Fn. 16), S. 16.

27 Zur mangelnden Nutzerfreundlichkeit etwa McKinsey&Company, E-Government in Deutschland, 2015, S. 11.

28 Nationaler Normenkontrollrat, E-Government in Deutschland: Wie der Aufstieg gelingen kann – ein Arbeitsprogramm (Kurzfassung), 2016, S. 17.

29 Nationaler Normenkontrollrat (Fn. 28), S. 17.

und aller Unzulänglichkeiten der föderalen Kooperation in der Praxis) einen verlässlichen Rechtsrahmen für eine künftige Zusammenarbeit zwischen Bund und Ländern. Die eID-Funktion des neuen Personalausweises ermöglicht einen rechtssicheren Identitätsnachweis. Der Grundstein für digitale Behördengänge ist gelegt.[30] Weitere Projekte, etwa die E-Rechnung,[31] hat der Bundestag bereits auf den Weg gebracht. Die Nutzerzahlen der digitalen Verwaltungsangebote steigen allmählich wieder, nachdem sie 2015 rückläufig waren.[32] Ebenso scheinen Nutzungsbarrieren, wie beispielsweise die Unkenntnis von Angeboten,[33] langsam zu verschwinden. Die jüngsten Entwicklungen nähren Hoffnung. Grund, sich selbstzufrieden zurückzulehnen, besteht aber nicht. Insbesondere sind die Herausforderungen, welche sich mit dem Prozess der Digitalisierung verbinden, nicht mit einfachen Hausrezepten zu bewältigen, sondern bedürfen einer komplexen Diagnostik. Die Zielmarken, an denen sich die Digitalisierungsstrategie des Staates messen lassen muss, stehen dabei mitunter in einem spannungsreichen Konflikt.[34]

---

30 Siehe hierzu etwa *Borges*, NJW 2010, 3334 ff.

31 Entwurf eines Gesetzes zur Umsetzung der Richtlinie 2014/55/EU über die elektronische Rechnungsstellung im öffentlichen Auftragswesen, BT-Drs. 18/9945; Bundesministerium des Innern, Umsetzung der Digitalisierung: Bundeskabinett beschließt E-Rechnungs-Gesetz, Pressemitteilung v. 13.7.2016.

32 Initiative D21 (Fn. 16), S. 8.

33 Initiative D21 (Fn. 16), S. 16: Im Vergleich zum Jahr 2014 sank die Zahl derer, welche die Unkenntnis von Online-Angeboten als Nutzungsbarriere nannten, um 19 Prozentpunkte auf 57 %.

34 Vgl. dazu auch S. 34.

2. Digitale Sicherheit

(Industrie-)Spionage, Cyber-Mobbing und Hacker-Attacken sind die Kehrseite der schönen neuen Internetwelt.[35] Durch Social Engineering täuschen Angreifer persönliche Beziehungen vor, um Informationen zu erlangen oder um das Opfer zu motivieren, einen Anhang mit Schadprogrammen zu öffnen. Täter verwenden Distributed-Denial-of-Service-Angriffe (DDoS-Angriffe), um Online-Dienste betriebsunfähig zu machen oder dies zumindest anzudrohen, um Unternehmen zu erpressen. Die Menge an Spam-Nachrichten mit angehängter Schadsoftware hat im ersten Halbjahr 2016 im Vergleich zum Jahr 2015 um 1270 % zugenommen.[36]

35 Zu den verschiedenen paradigmatisch aufgeführten Angriffsmitteln s. Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2016, 2016, S. 18 ff.

36 BSI, BSI veröffentlicht Bericht zur Lage der IT-Sicherheit in Deutschland 2016, Pressemitteilung v. 9.11.2016.

DIGITALE SICHERHEIT

- *Die Anzahl der auf crypto-style-Ransomware basierenden Attacken stieg in 2015 im Vergleich zum Vorjahr um 35 %.*[37]
- *Täglich werden ca. 380.000 neue Schadprogramm-Varianten gesichtet.*[38]
- *Infolge eines verheerenden Cyber-Angriffs musste der Deutsche Bundestag sein gesamtes internes Netzwerk für mehrere Tage abschalten, um zentrale Komponenten des IT-Systems neu aufzusetzen.*[39]
- *Eine Sicherheitsanalyse der zehn verbreitetsten internet of things -Geräte hat eine hohe Anzahl an Schwachstellen in jedem Gerät zu Tage gefördert.*[40]

Wer sich auf vernetzten Datenautobahnen bewegt, braucht verlässliche digitale Sicherheitsgurte. Der digitale Wandel macht Staat und Gesellschaft in einem bislang nicht gekannten Ausmaß verwundbar.[41] Digitale Technologien sind daher nur so gut, wie sie sicher sind.

Die Dynamik der technologischen Entwicklung spielt Cyber-Angreifern in die Hände: Neue Sicherheitslücken entstehen schneller, als alte geschlossen werden können.[42] Die Verfolgung der Täter entpuppt sich als Kampf gegen eine Hydra. Das macht eine konsistente, im Idealfall global abgestimmte präventive IT-Sicherheitsstrategie und einen verständlichen, sicheren und handhabbaren Verfügungs- und Schutzrahmen für digitale Datenflüsse erforderlich.

Auf die Frage, worin sie das größte Risikopotenzial der aktuellen digitalen Entwicklung sehen, geben IT-Experten denn auch eine klare Antwort: Es ist das enorme Sicherheitsdefizit infolge der exponentiell vergrößerten Angriffsflächen, welche die komplexe Vernetzung verschiedenster Geräte, Komponenten und Dienste in einem „Internet der Dinge“ mit sich bringt.[43]

---

37 Symantec, 2016 Internet Security Threat Report, 2016, S. 7.

38 Bundesamt für Sicherheit in der Informationstechnik (Fn. 35), S. 18.

39 BSI, Die Lage der IT-Sicherheit in Deutschland 2015, 2015, S. 26.

40 Hewlett Packard Enterprise, Internet of things research study, 2015, S. 3.

41 Der jährliche finanzielle Schaden durch digitale Wirtschaftsspionage, Datensabotage und Datendiebstahl beläuft sich Schätzungen zufolge in Deutschland auf rund 51 Milliarden Euro pro Jahr, vgl. BITKOM, Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter, 2015, S. 17. In der deutschen Industrie beklagte jedes zweite Unternehmen im Jahr 2014 einen digitalen Spionageangriff oder Verdachtsfall, vgl. *Corporate Trust*, Industriespionage 2014 – Cybergeddon der deutschen Wirtschaft durch NSA & Co.?, 2015, S. 13.

42 Vgl. World Economic Forum, Global Risks 2014, 2014, S. 10.

43 Vgl. McKinsey Global Institute, The Internet of Things: Five critical questions, Interview with leading industry experts, 2015. Dem Themenkomplex „Digitale Sicherheit“ wendet sich der Programmbereich insbesondere mit dem Kernforschungsthema „Digitale Sicherheitsarchitektur“ (C.III, S. 59 ff.) zu.

Ebenso wie alles, was digitalisiert werden kann, digitalisiert werden wird, wird auch alles, was digitalisiert ist, angegriffen werden.

Erst wenn es staatlichen Stellen, insbesondere der öffentlichen Verwaltung gelingt, geeignete Sicherheitsstrategien zu entwickeln und umzusetzen, kann es ein Gemeinwesen verantworten, die Aufgabenerfüllung der öffentlichen Verwaltung auf den digitalen Modus umzuschichten. Nur integre IT-Lösungen schaffen insbesondere die notwendige Vertrauensgrundlage, um gemeinsame Information, Koordination und Entscheidung großflächig auf digitalisiert agierende Entitäten auszulagern. Die bereits durchgeführten oder angedachten Projekte (z. B. die Einrichtung des Nationalen Cyber-Abwehrzentrums oder die Erarbeitung von IT-Sicherheitsrichtlinien für Behörden)[44] können dabei nur den Anfang in einer Kette von Maßnahmen bilden. Entsprechende Gesetzgebungs-, Umsetzungs- und Aufsichtsmaßnahmen sind Ausfluss der grundrechtlichen Schutzpflicht des Staates gegenüber den Grundrechten der Bürger, insbesondere dem Allgemeinen Persönlichkeitsrecht (v.a. in seiner Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG).

3. Persönlichkeitsschutz

Die algorithmische Einhegung von Entscheidungsabläufen eröffnet im Big-Data-Universum tiefe Einblicke in unser digitales Alter Ego und perfektioniert die Berechenbarkeit menschlichen Verhaltens. Unser digitaler Zwilling hinterlässt massenhaft Datenspuren, die sich leicht nachzeichnen lassen: Datenkollektoren eröffnet das die Möglichkeit, die engere persönliche Lebenssphäre des Einzelnen auszuforschen und dadurch eine bislang nie dagewesene Deutungshoheit über Personen zu erlangen.[45] Wer aber sich unter Überwachung wähnt, ändert sein

---

44 Zu einer Auswahl von Projekten des Bundes s. beispielsweise Bundesamt für Sicherheit in der Informationstechnik (Fn. 35), S. 42 ff.

45 Zur Algorithmensteuerung unter Big-Data-Bedingungen etwa *Bächle*, Mythos Algorithmus, 2015; Centre for Internet and Human Rights, Ethics of Algorithms: from radical content to self-driving cars, 2015; *Martini*, DVBl. 2014, 1481 ff. m. w. N.; *O`Reilly*, Open Data and Algorithmic Regulation, in: Goldstein/Dyson (Hrsg.), Beyond Transparency, 2013, S. 289 ff.; *Pasquale*,

Verhalten.[46] Das Gefühl, unter ständiger Beobachtung zu stehen, schnürt der freien Persönlichkeitsentfaltung die Luft ab.[47] Zu tiefgehende Einblicksmöglichkeiten staatlicher und privater Stellen in die Privatsphäre von Internetnutzern beeinträchtigen sowohl die freie Meinungsäußerung des Einzelnen als auch den ungestörten kollektiven Diskurs als Lebenselixier einer pulsierenden Demokratie.

The black box society, 2015, S. 1 ff.; *Tufekci*, Colorado Technology Law Journal 2015, 203 ff.

46 Neuere empirische Erkenntnisse – aufgezeigt am Beispiel der NSA-Überwachung – stützten die These, dass Internetnutzer ihr Verhalten beim Verdacht möglicher staatlicher Überwachung verändern, vgl. *Marthews/Tucker*, Government Surveillance and Internet Search Behavior, 2015; *Penney*, Berkeley Technology Law Journal 31 (2016), 117 ff.

47 Deutlich auch das BVerfG, Beschl. v. 13.10.2016 – 2 BvE 2/15, BeckRS 2016, 54271 Rn. 153: „Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland“.

DIGITALER DATENSCHUTZ

- *Nur 3% der Internetnutzer in Deutschland ist es gleichgültig, was mit ihren personenbezogenen Daten im Internet geschieht.*[48]
- *Die Anzahl der gestohlenen Identitäten ist im Jahr 2015 im Vergleich zum Vorjahr um 23 % gestiegen.*[49]
- *Das BSI informierte im Jahr 2014 über einen großflächigen Identitätsdiebstahl mit 18 Millionen betroffenen E-Mail-Adressen.*[50]

Der Schutz der Privatheit und informationellen Selbstbestimmung sieht sich unter den Bedingungen ubiquitärer Datenverarbeitung einerseits enormen Herausforderungen ausgesetzt. Die Vitalität und Produktivität der digitalen Welt hängt andererseits am Tropf der Produktion und der Verfügbarkeit von Datenströmen, ihrer Interoperabilität sowie den Schnittstellen zwischen öffentlichen und privaten Daten. Politische und regulatorische Maßnahmen zur Etablierung eines verständlichen, sicheren und handhabbaren Verfügungs- und Schutzrahmens für Daten beflügeln unter diesen Rahmenbedingungen im Idealfall die Entwicklung eines vertrauenswürdigen „Internets der Dinge".

Mit der Datenschutz-Grundverordnung (DSGVO) unternimmt die EU den Versuch, ein einheitliches Datenschutzniveau in allen Mitgliedstaaten zu etablieren – und setzt mit seinem Marktortprinzip und den Vorschriften für die Übertragung von Daten in Drittstaaten auch global wirksame Maßstäbe.[51]

4. Technologische Abhängigkeiten

a) Abhängigkeiten der Verwaltung von privaten Dienstleistern

Das geistige Eigentum an digitalen Technologien liegt fast ausschließlich in privater Hand. Bei der Auswahl von Hard- und Software läuft der Staat daher schnell Gefahr, IT-Lösungen einzukaufen, die er nicht selbst

---

48 BITKOM, Datenschutz in der digitalen Welt, 2015, S. 2.

49 Symantec (Fn. 37), S. 8.

50 BSI, Neuer Fall von großflächigem Identitätsdiebstahl: BSI informiert Betroffene, Pressemitteilung v. 7.4.2014.

51 Insbesondere mit den Projekten „Mitgliedstaatliche Regelungsspielräume unter der Datenschutz-Grundverordnung (C.II.4, S. 53 ff.) und „Datenschutzrechtliche Verantwortungsstrukturen in komplexen Online-Akteursnetzwerken" (C.IV.2, S. 70 ff.) nimmt sich der Programmbereich zentralen Fragestellungen eines modernen, funktionalen und technikgestützten Datenschutzrechts an.

nachvollziehen, geschweige denn kontrollieren kann. Er ist auf Support, Updates und Know-how von außen angewiesen; nutzt er proprietäre Lösungen, kann er zwar das Front-End konfigurieren, ein Einblick in den Programmcode als der Herzkammer der Kommunikations- und Informationstechnologie ist ihm in der Regel jedoch verwehrt.[52] Daraus ergeben sich Herausforderungen nicht nur für die IT-Sicherheit, insbesondere bei kritischen Infrastrukturen und vertraulichen Verarbeitungsvorgängen, sondern auch für die Rechtsstaatlichkeit. Sie münden in die Grundfrage: Wie lässt sich öffentliche Kontrolle über – durch Betriebsgeheimnisse geschützte – Hard- und Software gewährleisten, wenn die demokratisch legitimierten Kontrollinstanzen immer weitreichendere Arbeitsschritte auf diese auslagern?[53]

b) Abhängigkeit des Individuums von digitalen Angeboten als Teilhabevoraussetzung

Online-Ressourcen sind in einer digitalen Welt die Nabelschnur gesellschaftlicher Teilhabe. Die Personalisierung (in der öffentlichen Verwaltung gleichermaßen wie bei privaten Dienstleistern) eingesetzter Online-Angebote zeitigt Auswirkungen auf die Wahrnehmung der individuellen Informationsfreiheit und den Persönlichkeitsschutz.[54]

Nur geeignete Schutzmaßnahmen der individuellen Kommunikation sowie ebenenübergreifende Regelungsansätze, Organisationsstrukturen und sichere Informations- und Kommunikationsnetze[55] immunisieren den einzelnen Bürger hinreichend gegen die Risiken und Abhängigkeiten digitaler Technologien. Im digitalen Zeitalter ist daher nicht nur der Persönlichkeitsschutz eine zentrale Infrastrukturvorgabe. Auch die Qualität der Datenverarbeitung und Funktionsfähigkeit technischer Systeme

---

52 Zu den Möglichkeiten von Open-Source-Lizenzierungen und offenem Quelltext vgl. *Auer-Reinsdorff/Kast*, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 2. Aufl., 2016, § 9, insbesondere Rn. 11.

53 Zur Nutzung von Open-Source-Lösungen in der Verwaltung etwa *Martens*, KommJur 2007, 94 ff.; *Demmel/Herten-Koch*, NZBau 2004, 187 ff.

54 Vgl. *Pariser*, The Filter Bubble, 2011. Gerade nach der US-Präsidentschaftswahl im November 2016 hat die Diskussion um den Einfluss sozialer Netzwerke auf die Meinungsbildung erneut Fahrt aufgenommen, vgl. etwa *Zastrow*, Wie Trump gewann, FAS vom 11.12.2016, S. 2 f.

55 Zum objektiv-rechtlichen Schutzgehalt des Grundrechts auf Integrität und Vertraulichkeit informationstechnischer Systeme grundlegend *Hoffmann-Riem*, JZ 2014, 53 (57 ff.).

entwickelt sich immer sichtbarer zu einer wichtigen Quelle selbstbestimmter Kommunikation und ökonomischer Wertschöpfung.

VERTRAUEN IN UND DURCH DIE DIGITALE VERWALTUNG

Noch immer sehen 31 % der Deutschen im mangelnden Vertrauen in die Arbeit der Behörden insgesamt eine Barriere für die intensivere Nutzung von Online-Behördendiensten.[56]

Vertrauen ist Voraussetzung für ein funktionierendes Zusammenspiel zwischen Bürgern, Wirtschaft und Verwaltung. Die Digitalisierung des Verfahrens und der Leistungen generiert insbesondere nur dann die möglichen und anvisierten Effizienzsteigerungen, wenn die Adressaten die digitalen Angebote auch tatsächlich annehmen.

Vertrauen gegenüber technischen Innovationen setzt gleichzeitig eine ausreichend ausgebildete Kompetenz im Umgang mit digitalen Technologien voraus. Eine wichtige Aufgabe des Staates ist es daher, das Bewusstsein der gesellschaftlichen Akteure dafür zu schärfen, wie sie zum Schutz eigener Daten und IT-Infrastruktur durch Präventions- und Sicherheitsmaßnahmen beitragen können („digital awareness“)[57].

56 Initiative D21 (Fn. 16), S. 17, wobei dieser Wert zum Vergleichsjahr 2014 deutlich (um 26 Prozentpunkte) gesunken ist. Für das Jahr 2015 (50 %) s. Initiative D21, eGovernment Monitor 2015, 2015, S. 14.

57 Diesem Gesichtspunkt geht der Programmbereich insbesondere im Rahmen des Projekts „Schutzmechanismen der digitalen Kommunikation“ (C.III.2, S. 63 ff.) nach.

5. *Digitale Infrastruktur*

DIGITALE VERNETZUNG

- *Deutschland liegt beim Ausbau schneller und ultraschneller Breitbandanschlüsse mit über 30 Mbit/s im EU-Vergleich nur auf Platz 21.*[58]
- *2020 werden Schätzungen zufolge 25 bis 30 Milliarden Objekte im „Internet der Dinge" vernetzt sein.*[59]

DIGITALE INTEROPERABILITÄT

Das EGovG des Bundes und die EGov-Gesetzgebung der Länder setzen mit ihren Vorgaben zur elektronischen Behördenkommunikation und dem Datenaustausch eine qualifizierte IT-Vernetzung über Behördengrenzen und Verwaltungsebenen voraus.

Die flächendeckende Bereitstellung einer leistungsfähigen und sicheren Breitbandinfrastruktur ist nicht nur Voraussetzung dafür, Online-Verwaltungsdienstleistungen im gesamten Land anzubieten. Sie ist – zusammen mit einer flächendeckenden Versorgung mit mobilem Internet – auch die technische Grundlage für die praktische Implementierung des „Internets der Dinge": Dessen Funktionalität hängt von einem schnellen und verzögerungsfreien Datenfluss ab. Mit Blick auf die digitale Vernetzung von Objekten ist außerdem die Definition und Verfügbarkeit von Datenbankschnittstellen für die öffentliche Hand elementar, damit sie die damit verbundenen Ordnungsaufgaben wahrnehmen und eine gemeinwohldienliche staatliche Teilhabe an Objektdaten gewährleisten kann.[60]

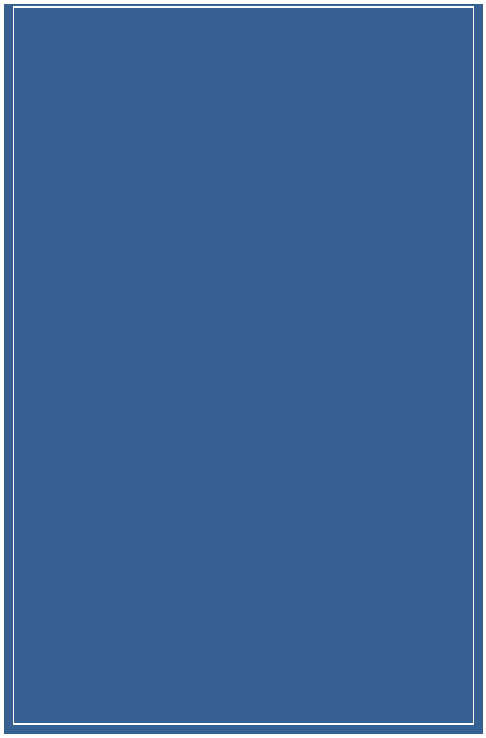
Die ebenenübergreifende Vernetzung der IT-Systeme der Bundes-, Landes- und Kommunalverwaltungen bzw. die Integration mehrerer IT-Systeme in eine einheitliche (europäische) Infrastruktur erfordert es, alle relevanten Interoperabilitätsfragen mitzudenken und große Anstrengungen zu ihrer Gewährleistung zu unternehmen. Dem sind auf Bundesebene insbesondere die Vorhaben „Aktionsplan E-Akte" und „Gemeinsame und integrierte Prozessoptimierung", im föderalen Bereich etwa

---

58 Europäische Kommission, Implementation of the EU regulatory framework for electronic communication - 2015, 2015, S. 6.

59 Gartner, Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015, Pressemitteilung v. 11.11.2014; EMC, The Digital Universe of Opportunities, 2014, S. 5.

60 Hierauf richtet der Programmbereich insbesondere mit den Projekten „Smart Cities' Government: staatliche Infrastrukturaufgaben in der digitalen Welt" (C.II.2, S. 47 ff.) und „Kooperative eingebettete Systeme: Vernetzung der öffentlichen Verwaltung mit intelligenten Industrie 4.0-Umgebungen" (C.IV.1, S. 67 ff.) sein besonderes Augenmerk.



die Standardisierungsagenda[61] und xDomea[62] sowie auf kommunaler Ebene das Vorhaben „Modellkommune“ verschrieben.[63] Ziel sollte eine Ausweitung der föderalen Schlagkraft des IT-Planungsrates und ein Ausbau der bisherigen Angebote hin zu einem bundesweiten Portalverbund[64] mit gemeinsamen Servicestandards sein[65]. Gelingt das, entsteht eine neue Kultur der ebenenübergreifenden (IT-)Kooperation, welche dem Online-Angebot der Verwaltung einen Quantensprung ermöglicht.

Neben den operativen Bemühungen um Interoperabilität lohnt es sich auch, die Potenziale junger technischer Innovationen – etwa der Distrubuted-Ledger- bzw. Blockchain-Technologie –für die verteilte Datenverarbeitung im Bundesstaat frühzeitig in den Blick zu nehmen und zu erschließen.[66]

---

61 Vgl. Koordinierungsstelle für IT-Standards (KoSIT), Standardisierungsagenda, 2015.

62 XDOMEA ist der Datenaustauschstandard der Verwaltung zwischen Daten unterschiedlicher Systemen.
Vgl. www.xoev.de/detail.php?gsid=bremen83.c.11406.de (15.9.2016).

63 Siehe hierzu Bundesregierung (Fn. 14), S. 25 ff., 44 f., 97 f.

64 IT-Planungsrat, Projektsteckbrief Portalverbund, 2016.

65 Dazu etwa Nationaler Normenkontrollrat, E-Government in Deutschland: Wie der Aufstieg gelingen kann - ein Arbeitsprogramm (Langfassung), 2016, S. 17 ff: „Der ‚Digitale Servicestandard für Deutschland‘ (DSD) definiert die Rahmenbedingungen für den Erfolg des nutzerorientierten E-Governments, sodass dieses anhand seiner Wirkungen, seiner Akzeptanz sowie seiner Nutzung messbar wird. ‚Digital-by-Default‘ wird in Übereinstimmung mit den unterschiedlichen Nutzeranforderungen und unter Berücksichtigung von Datenschutz und Barrierefreiheit sukzessive eingeführt.“

66 *Rehfeld*, Die Blockchain, in: Fadavian (Hrsg.), Transparente Staatstätigkeit, 2016, S. 25 ff.; *Blocher*, AnwBl 2016, 612 ff.; *Walport*, Distributed Ledger Technology, 2016; *Kaulartz*, CR 2016, 474 ff.; *Kolain/Wirth*, Speed Dating on Smart Contracts, in: Parycek/Edelmann (Hrsg.), CeDEM16, 2016, S. 201 ff. In dem Symposium „Anwendung der Blockchain-Technologie auf die öffentliche Verwaltung“ hat sich der Programmbereich bereits am 3./4.11.2016 mit diesem Thema auseinandergesetzt, siehe dazu *Kolain*, Verwaltung und Management 2016, 328 ff.

6. *Benutzerfreundlichkeit*

DIGITAL USABILITY

- *Nach wie vor bewegen sich die sog. Silversurfer der Altersgruppe 70+ und Bürger mit geringer formaler Bildung deutlich weniger souverän im digitalen Raum als die medienkompetenteste Nutzergruppe der formal hoch gebildeten 14-29-Jährigen.*[67]
- *Für 45 % der Deutschen errichtet die mangelhafte Benutzerfreundlichkeit von Online-Behördendiensten eine Nutzungsbarriere.*[68]
- *73 % der deutschen Internetnutzer äußern, dass Online-Dienste nicht infolge überzogener Datenschutzregeln umständlicher zu bedienen sein sollten.*[69]

Die digitale Gesellschaft ist (weiterhin) von soziologisch bedingten Zugangs- und Teilhabegräben durchzogen. Um damit einhergehende sozial selektive Nutzungshürden für staatliche Online-Angebote so niedrig wie möglich zu halten, kommt der einfachen, intuitiven Handhabung und niedrigschwelligen, barrierefreien sowie sprachlich verständlichen Gestaltung von E-Government-Diensten eine zentrale Bedeutung zu. Dazu gehören auch technische Lösungen, die den Nutzern helfen, ihre Daten wirksam zu schützen und die Sicherheit ihrer IT zu erhöhen.

„Usability" ist ein Passepartout für die Gewährleistung digitaler Teilhabe und den souveränen Umgang mit personenbezogenen Daten. Gerade im Bereich der Verschlüsselungstechnologien, denen eine zentrale Rolle beim *Datenschutz durch Technik* zukommt (vgl. auch Art. 25 Abs. 2 DSGVO), fehlt es aber bislang oftmals an einfach zu benutzenden, massentauglichen Lösungen.[70]

---

67 Initiative D21 (Fn. 6), S. 28 ff. Ähnlich Deutsches Institut für Vertrauen und Sicherheit im Internet (Fn. 5), S. 70 ff.

68 Initiative D21 (Fn. 16), S. 16 f.

69 BITKOM, Internetnutzer gehen pragmatisch mit Datenschutz um, Pressemitteilung v. 22.9.2015.

70 Aspekte der Benutzerfreundlichkeit als Entwicklungsvorgabe für digitale Verwaltungsangebote untersucht der Programmbereich insbesondere im Rahmen der Projekte „Mitgliedstaatliche Regelungsspielräume unter der Datenschutz-Grundverordnung (C.II.4, S. 53 ff.), „Schutzmechanismen der digitalen Kommunikation" (C.III.2, S. 63 ff.), „IT-Inkubator öffentliche Verwaltung" (C.V.2, S. 76 ff.) und „Open-Innovation-Wettbewerbe der öffentlichen Hand – Bürger und Staat als kollaborative Gesellschaftsintrapreneure" (C.V.3, S. 79 f.).

DIGITALE MOBILITÄT

- *Mehr als die Hälfte der Deutschen nutzt Mobilfunknetze für den Internetzugang.*[71]
- *Das Datenvolumen des mobilen Internets ist im Jahr 2015 im Vergleich zum Vorjahr um 74 Prozent gestiegen.*[72]
- *Die Nutzung von E-Government Angeboten durch mobile Endgeräte hat einen enormen Zuwachs erfahren und wird weiterhin rasant zunehmen.*[73]

Die standortunabhängige Vernetzung von Personen und die Erreichbarkeit von Online-Diensten (digitale Mobilität) zählen zu den fünf Schlüsselkomponenten moderner IT.[74] Fortschrittliches E-Government ist im Außenkontakt zum Bürger daher durch mobil erreichbare Zugänge zu Verwaltungsleistungen gekennzeichnet. Dafür braucht es ein mobiles Webangebot, Kompetenz in der Herstellung von Apps und mobile Verwaltungsdienste. Verwaltungsintern erfordert das eine Ausstattung der Verwaltung mit mobiler IT (VPN-Schnittstellen, mobile Geräte und Anwendungen, ID-Lösungen für den Fernzugriff u. a.), eine – insbesondere auch sicherheitssensibilisierende – Personalschulung für den Umgang mit mobilen Anwendungen sowie ein Mobile Device Management.[75]

---

71 Initiative D21 (Fn. 16), S. 26.

72 Cisco, Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020, 2016, S. 1.

73 Nur noch 18 % der Bürger lehnen die mobile Nutzung von E-Government-Angeboten auch für die Zukunft kategorisch ab, s. Initiative D21 (Fn. 16), S. 26 f.

74 Deloitte NASACT, Digital Government Transformation Survey, 2015, S. 4.

75 Die damit verbundenen verwaltungswissenschaftlichen Fragestellungen greift der Programmbereich in dem Projekt „Organisationsprinzipien des Mobile Government“ (C.V.1, S. 74 f.) auf. Vgl. auch die Darstellung der verschiedenen Architekturebenen bei U.S. Federal CIO Council, Government Use of Technology – Barriers, Opportunities, and Gap Analysis, 2012, S. 10.

7. *Digitale Automatisierung und Autonomisierung*

DIGITALE AUTOMATISIERUNG UND AUTONOMISIERUNG

- *Das kognitive IBM-Computersystem Watson ist nicht nur in der Lage, die Quizshow Jeopardy! zu gewinnen, sondern auch Gourmet-Kochrezepte zu kreieren, Krebstherapien zu entwickeln und Versicherungsberatern zu assistieren.*[76]
- *Mehr als ein Drittel der EU-Bürger nimmt an, dass in Zukunft ein Roboter ihre beruflichen Aufgaben zumindest teilweise erledigen kann.*[77]
- *Die Hälfte der Automobilindustrie und Marktanalysten geht davon aus, dass bis 2030 vollautonomes Fahren den Durchbruch geschafft hat.*[78]
- *Dem Google-Tochterunternehmen „DeepMind" ist es gelungen, eine künstliche Intelligenz ohne Vorprogrammierung Computerspiele erlernen und spielen zu lassen.*[79]

Jüngste Big-Data-getriebene Entwicklungen im Bereich künstlicher Intelligenz nähren auch im öffentlichen Sektor die Hoffnung, das Verwaltungspersonal durch bzw. den Einsatz (teil-)autonom entscheidender Expertensysteme entlasten zu können. Der Einsatz solcher „Entscheidungsmaschinen" geht allerdings mit weitreichenden verfahrensrechtlichen sowie verfassungs- und grundrechtsrelevanten Herausforderungen einher.

Ähnliches gilt für den Einsatz wissensbasierter Systeme, Mustererkennungs-/Mustervorhersageverfahren und Roboter durch Private. Gesetzgeber und Behörden sind insoweit gefordert, die Auswirkungen einer zunehmenden technischen Automatisierung und Autonomisierung bestimmter erlaubnis- oder zulassungspflichtiger Tätigkeiten (wie z. B. Personenbeförderung, Wertpapierhandel, Kreditvermittlung, Versicherungsberatung, Patientenpflege, Rechtsberatung) auf die Sicherheit des betroffenen Verkehrsbereichs (Straße, Finanzmarkt, Versicherungswesen, Kliniken, Rechtsverkehr usw.) im Rahmen ihrer Zuständigkeit zu beobachten und ggf. Anpassungsbedarfe erlaubnis- und haftungsrechtlicher Vorschriften zu eruieren.[80]

---

76 *Rauner/Schröder*, Zeit Wissen 2015, 64; siehe zu den technischen Hintergründen des Sieges bei „Jeopardy!" *Tesauro/Gondek/Lencher et al.*, JAIR 2013, 205; zum Einsatz in der Onkologie *Leiner*, Im Fokus Onkologie 2016, 12.

77 Europäische Kommission, Autonomous Systems Report, 2015, S. 27.

78 BITKOM, Jedes zweite Automobilunternehmen erwartet Durchbruch für autonomes Fahren bis 2030, Pressemitteilung v. 8.9.2015.

79 *Silver/Huang/Maddison et al.*, Nature 2016, 484 ff.

80 Die offenen Fragen digitaler Automatisierung und Autonomisierung sind insbesondere Gegenstand der Projekte „Algorithmenkontrolle als Regulierungsaufgabe" (C.II.1, S. 42 ff.) und „Regelungsbedarf und rechtliche Grenzen elektronischer vollautomatisierter Verwaltungsverfahren" (C.II.6, S. 57 ff.).

8. Digitale Organisationskultur

DIGITALE ORGANISATIONSKULTUR

Der Transparenzgrad der öffentlichen Verwaltung in Deutschland erfüllt die EU-Top-Level-Benchmark nur zu 60 % und liegt damit im EU-Vergleich nur im Mittelfeld.[81]

Der zunehmende IT-Einsatz in der öffentlichen Verwaltung und die Digitalisierung von Verwaltungsvorgängen und -verfahren verändert nicht nur die behördliche Prozess- und Sachorganisation. Er wirkt sich ebenso nachhaltig auf die Arbeitsbedingungen des Personals und die damit verbundene Führungsverantwortung aus. Die Digitalisierung stellt überkommene verwaltungsinterne Handlungsmuster, Informationsflüsse sowie Kooperationsgrenzen in Frage. Sie öffnet bislang verschlossene Wissenssilos, lässt dadurch neue Kompetenz- und Rollenprofile entstehen und impliziert politische und öffentliche Erwartungen an die Außenkommunikation. Ein grundlegender Wandel des Verwaltungsselbstverständnisses ist die Folge. Für Fach- und Führungskräfte des öffentlichen Sektors eröffnet sich ein bedeutendes Lern- und Handlungsfeld. Brechen Hierarchien und Dienstwege zugunsten organisatorischer und informationeller Flexibilität auf, braucht es neben substituierenden verantwortungs- und legitimationssichernden Strukturen einen damit korrespondierenden Kulturwandel.[82] Behördenleitungen sind gefordert, offene Prozesse anzuregen, Informationsflüsse innerhalb der Verwaltung transparent zu gestalten und ein integratives Ideen- und Lösungsmanagement zu betreiben.[83] Hierauf sind insbesondere die Personalauswahl- und -entwicklungskonzepte, aber auch die Ausgestaltung der internen Kommunikations- und Wissensmanagementsysteme (z. B. in Form eines Social Intranet) auszurichten.[84]

---

81 Europäische Kommission, eGovernment Benchmark 2016 – Country Factsheet Germany, 2016, S. 1.

82 Vgl. dazu auch die Ausführungen in der Open Government-Vision der Europäischen Kommission Directorate-General for Communications Networks, Content and Technology, A vision for public services, 2013, S. 10.

83 Vgl. auch *Hill*, Verwaltung und Management 2016, 241 (243 ff.).

84 Mit den damit zusammenhängenden Fragen beschäftigt sich das Projekt „Digital-transformationale Führung in der Netzwerkverwaltung“ (C.V.4, S. 81 ff.).

B. Zielmarken digitaler Staatlichkeit und ihrer wissenschaftlichen Begleitung

So groß die Chancen der digitalen Transformation sind, so gewaltig sind auch die Herausforderungen, die damit auf die öffentliche Verwaltung einströmen. In diesem Prozess kann der Wissenschaft die hilfreiche Funktion zuwachsen, die Auswirkungen digitaler Technologien auf Staat und Gesellschaft nicht nur kritisch zu evaluieren, sondern sie auch mit reflektiertem Weitblick zu antizipieren. Sie vermag es, Anpassungsbedarfe für den Aufgabenzuschnitt und die Aufgabenwahrnehmung öffentlicher Stellen abzuleiten und Lösungen dafür zu entwickeln, wie – angesichts sich überschlagender Entwicklungsdynamiken – eine innovationsoffene Risikosteuerung durch und mit der öffentlichen Verwaltung möglich ist. Potenziale der Kooperation von Staat und Wirtschaft im digitalen Morgenland vorzudenken und anzuregen, die Öffnung der Verwaltungsverfahren für die Chancen der Digitalisierung zu begleiten und ihren Gefahren durch wirksame Regulierungs- und Organisationsempfehlungen entgegenzuwirken, gehört zu den Kernaufgaben verwaltungswissenschaftlicher Digitalisierungsforschung.

I. Leitbild der Staats- und Verwaltungstransformation durch digitalen Wandel

Als interdisziplinär angelegter Forschungsverbund, der verschiedene verwaltungsbezogene Fachdiskurse zusammenführt, bekennt sich der Programmbereich „Digitalisierung“ zu dem Leitbild einer durch den digitalen Wandel veranlassten Staats- und Verwaltungstransformation.[85] Dieses Leitbild bildet die Hintergrundfolie aller Forschungsbemühungen und den Ausgangspunkt für die Identifikation übereinstimmender Aufmerksamkeitsfelder.

85 Zu den koordinativen Funktionen von Leitbildern in interdisziplinären Forschungszusammenhängen vgl. statt vieler *Voßkuhle*, § 1 – Neue Verwaltungsrechtswissenschaft, in: Hoffmann-Riem/Schmidt-Assmann/ Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. I, 2. Aufl., 2012, Rn. 40 ff. m. w. N.

II. Selbstverständnis des Programmbereichs

Oftmals fehlen der Verwaltung im Alltagsgeschäft hinreichende eigene Zeitressourcen, um sich mit übergreifenden Zukunftsfragen der Regulierung und Normanwendung vertieft zu beschäftigen. Umgekehrt befruchten Rückmeldungen und Impulse aus der Erfahrungswelt der Praxis die wissenschaftliche Arbeit: Sie tragen zur Erweiterung des Forschungshorizonts, zur Schärfung des analysierenden Blicks und zu deren gesellschaftlichen Rückbindung nachhaltig bei. Viele Forschungsfragen erlangen erst durch die Anwendung von Konzepten und Handlungsempfehlungen in der Verwaltungspraxis klare Konturen, viele wissenschaftliche Herausforderungen werden erst im Zuge der Vorbereitung und Durchführung von konkreten Rechtsvorschriften und organisatorischen Konzepten sichtbar.

Auch wenn der Programmbereich die verwaltungswissenschaftliche Grundlagenforschung als seine Kernaufgabe versteht, verliert er die Relevanz seiner Ergebnisse für die Verwaltungspraxis dabei nicht aus dem Blick, sieht sich insbesondere dem Anspruch verpflichtet, die Ergebnisse bis zur Anwendungsebene zu Ende zu denken. Ein zentrales Augenmerk liegt deshalb auf der praktischen Verwertbarkeit der ausgewählten Forschungserträge für die Träger des Instituts. In seiner synergetischen Zusammenführung der Verwaltungswissenschaften und der Verwaltungspraxis bewegt sich der Programmbereich ganz in der Tradition des Forschungsstandorts Speyer.[86] Er beleuchtet die Chancen und Risiken der Gestaltungsaufgabe „digitaler Wandel“ daher nicht nur abstrakt. Vielmehr ist es ihm darum bestellt, die Fragen in angemessener Form auch auf die konkreten Bedürfnisse der Verwaltung herunterzubrechen und bei wissenschaftlichen Ergebnissen und Empfehlungen nach Möglichkeit auch die Kriterien der Machbarkeit, Umsetzbarkeit und Finanzierbarkeit zu berücksichtigen.

---

86 Vgl. dazu *Amos*, Zur Geschichte des Forschungsinstituts für öffentliche Verwaltung bei der (Deutschen) Hochschule für Verwaltungswissenschaften Speyer 1956/1962–2001, 2002.

III. Aus dem Erkenntnisinteresse und identifizierten Forschungsthemen abgeleitete übergreifende Forschungsfrage des Programmbereichs

1. Identifizierung und Auswahl der Forschungsthemen

So breit die Streuwirkung von Digitalisierungsprozessen ist, so vielfältig sind auch die Themen, welche die Staats- und Verwaltungstransformation auf die wissenschaftliche Agenda setzt. Anders als bei anderen Forschungsthemen handelt es sich bei der Digitalisierung um keinen konsistenten und in sich abgeschlossenen Forschungsgegenstand, der sich mit einer detailscharfen Forschungsfrage umreißen ließe – vielmehr setzt sie nahezu alle Lebensbereiche einem umfassenden Umbruchsprozess aus, der Ausstrahlungen in nahezu alle Wissenschaftsdisziplinen zeitigt.

Die Fülle der Digitalisierungsthemen macht es auch notwendig, eine Auswahl aus der Melange denkbarer Forschungsprojekte zu treffen.[87] Einem innovations- und zugleich praxisorientierten Forschungsprogramm, das sowohl an zentralen Punkten des wissenschaftlichen Diskurses Grundlagenforschung betreibt als auch zukunftsweisende, praxisgerechte Konzepte vordenken möchte, ist umgekehrt eine zu enge Eingrenzung des Forschungsvorhabens nicht sachdienlich. Der Auswahl der Forschungsprojekte ist vor diesem Hintergrund zwangsläufig ein gewisses Maß an Selektivität und Dynamik[88] eigen: Was konsistent im Hinblick auf die Forschungsfrage ist, ist unter Umständen für die politische und administrative Praxis von geringem Interesse – und umge-

87 Im Einklang mit den Bedürfnissen der Träger des Instituts, insbesondere ihrer (Ministerial-)Verwaltungen, legt der Programmbereich einen besonderen Schwerpunkt auf die regulatorischen Fragen der Digitalisierung.

88 Die Dynamik der Forschungsfelder bringt es notwendig mit sich, dass im Laufe des Bearbeitungsprozesses neue Forschungsthemen erkennbar werden, die sich zum Zeitpunkt des Programmstarts noch nicht abgezeichnet haben. Den Sachgesetzlichkeiten des erforschten Sachbereichs und den Erfordernissen innovativer Forschung wird der Programmbereich dadurch Rechnung tragen, dass er sich neuer Themen zeitnah (auch während seiner Laufzeit) stellt und die Prioritäten in seiner Feinsteuerung anpasst – ohne dabei jedoch die Fokussierung auf die Kernforschungsthemen infrage zu stellen. Das Design der übergreifenden Forschungsfrage lässt hierfür (bewusst) ausreichend Freiraum.

kehrt. Bei der Formulierung einer übergreifenden Forschungsfrage setzt der Programmbereich auf eine ausbalancierte Harmonie des Dreiklangs aus

- einer konsistenten Forschungsprogrammatik zu Digitalisierungsthemen im Kompetenzradius der beteiligten Forscher,
- der Aufgeschlossenheit gegenüber den Impulsen aus der politischen und administrativen Praxis sowie
- einem feinen Spürsinn für Innovations- und (interdisziplinäre) Kooperationsimpulse.

2. Umwälzungsprozesse der Digitalisierung und ihre Herausforderungen für Staat und Verwaltung

Das Leitbild der Staats- und Verwaltungstransformation durch digitalen Wandel impliziert die Hypothese: Der Staat als gesellschaftliches Ordnungssystem und Institutionenordnung wird sich im Zuge fortschreitender Digitalisierung in seiner äußeren und inneren Form[89] (weiter) umgestalten und eine Assimilation an die digitalisierten Lebens- und Funktionswelten seiner Bürger und gesellschaftlichen Teilsysteme erfahren.[90] Diese Präsumtion findet ihre Stütze sowohl in empirischen Befunden (in Gestalt von Meinungsführer- und Entscheiderstudien[91], Zukunfts-[92],

---

89 Zur Unterscheidung äußerer und innerer Grenz- und Formverschiebungen und den insoweit wirksamen Akteursgruppen und Veränderungsmechanismen vgl. *Benz*, Leviathan 40 (2012), 223 ff.

90 Die formale Digitalisierung staatlicher Aufgabenerfüllung im Sinne von E-Government-Projekten ist dabei nur *ein* Faktor des durch politische, wirtschaftliche und technische Variablen angetriebenen und definierten institutionellen Wandels und deshalb für sich genommen nicht mit staatlicher Transformation gleichzusetzen, vgl. *Gascó*, Social Science Computer Review 21 (2003), 6 ff.

91 Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI), Meinungsführer-Studie: Wer gestaltet das Internet?, 2012, S. 17 ff.; Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI), Entscheider-Studie zu Vertrauen und Sicherheit im Internet, 2013, S. 63 ff.

92 Codagnone/Wimmer (Hrsg.), Roadmapping eGovernment Research, 2007; IBM Corporation, Towards 2025: Delivering public sector digital transformation in Australia, 2013; Institute for Prospective Technological Studies (IPTS), Envisioning Digital Europe 2030, 2010, S. 61 ff.; Internet & Gesellschaft Collaboratory, Smart Country – Digitale Strategien für Regionen. Inter-

Trend-[93] und Innovationspotenzialanalysen[94]) als auch in politischen[95] und normativen Bedarfsprognosen[96].

Die Arbeitshypothese wachsender digitaler Assimilierung der Verwaltung an digitale Arbeits- und Lebenswelten fordert eine Analyse der Rahmenbedingungen, denen die Digitalisierung für das Handeln des Staates und der Verwaltung unterliegt – und daran anknüpfend die Suche nach Handlungsanleitungen, unter denen der Staat die Chancen dieses Veränderungsprozesses nutzen kann, ohne seine Strukturprinzipien und sein demokratisches Selbstverständnis zu gefährden. Ausgehend von dem empirischen Befund, dass sich das Handlungsumfeld des Staates und der Gesellschaft in einer digitalisierten Gesellschaft gegenwärtig radikalen Wandlungen ausgesetzt sieht, gilt es nach den Rahmenbedingungen zu fahnden, die den Aktionsradius der Gesellschaft und des Staates (insbesondere der öffentlichen Verwaltung) in einer digitalisierten Gesellschaft in Zukunft als Steuerungsfaktoren nachhaltig prägen: **Wie wird also die Digitalisierung das Handeln des Staates, insbesondere der Verwaltung, verändern?**

Der empirische Ausgangsbefund, insbesondere die sich abzeichnenden und zu erwartenden technischen Entwicklungen hin zu einer (nahezu) vollständig digitalisierten Gesellschaft (und Verwaltung), rufen die

---

aktiver Hintergrundbericht, https://smartcountry.collaboratory.de/ecm-politik/colab/de/home/beteiligen/draftbill/44586/13 (24.9.2015), Kap. 1; *Zweck/Holtmannspötter/Braun et al.*, Gesellschaftliche Veränderungen 2030, 2015; *Zweck/Holtmannspötter/Braun et al.*, Forschungs- und Technologieperspektiven 2030, 2015.

93 Vgl. etwa *Fromm/Weber*, ÖFIT-Trendschau: Öffentliche Informationstechnologie in der digitalisierten Gesellschaft, 2014.

94 *Markl/Hoeren/Krcmar*, Innovationspotenzialanalyse für die neuen Technologien für das Verwalten und Analysieren von großen Datenmengen (Big Data Management), 2013.

95 OECD Public Governance and Territorial Development Directorate, Recommendation of the Council on Digital Government Strategies, 2014; *Singer*, White House Proposes Broad Consumer Data Privacy Bill, New York Times vom 27.2.2015, http://www.nytimes.com/2015/02/28/business/white-house-proposes-broad-consumer-data-privacy-bill.html?_r=0 (20.3.2015); The White House, Big Data: Seizing Opportunities, Preserving Values, 2014. Zu deutschen und EU-weiten Programmen siehe bereits Fn. 14.

96 Siehe bspw. *Hill*, Wandel von Verwaltungskultur und Kompetenzen im digitalen Zeitalter, in: Hill/Martini/Wagner (Hrsg.), Transparenz, Partizipation, Kollaboration, 2014, S. 125 ff.; *Tumin/Fung*, From Government 2.0 to Society 2.0, 2011.

Kernfrage nach den daraus zu ziehenden Schlussfolgerungen auf den Plan: Die digitale Transformation löst nicht nur einen hohen Anpassungsdruck auf die bestehende gesellschaftliche Ordnungsstruktur aus; es stellt sich insofern nicht nur die Frage nach dem „Wie“ der Anpassung an die neuen technologischen Möglichkeiten und Erfordernisse. Der digitale Wandel wirft vielmehr auch die Frage nach dem „Wohin“ auf. Im Fokus wissenschaftlicher Aufmerksamkeit müssen deshalb auch die Konsequenzen stehen, die sich mit der Staats- und Verwaltungstransformation verbinden: Wie sieht ein digitaler, demokratischer Rechtsstaat auf dem Boden des Grundgesetzes aus? Wie lösen wir in 50 Jahren unsere Konflikte, wie verteilen wir die Güter, wenn Roboter menschliche Arbeitskraft in immer stärkerem Umfang ersetzen können, wie wirtschaften und arbeiten wir? Auch diese Fragen harren einer wissenschaftlichen Aufarbeitung.

Die denkbaren Handlungsanleitungen bewegen sich in einem Spannungsbogen zwischen dem wirtschaftlichen Wertschöpfungspotenzial und gemeinwohlorientierten Entwicklungsmöglichkeiten auf der einen Seite sowie Risiken für den Persönlichkeitsschutz und die Funktionsbedingungen eines demokratischen Rechtsstaats auf der anderen Seite. Die entscheidende Frage ist daher: **Wie kann der Staat, insbesondere die Verwaltung, die Chancen der Digitalisierung nutzen, ohne Grundprinzipien eines demokratischen Rechtsstaats und des Persönlichkeitsschutzes zu gefährden?**

Das Leitbild des Programmbereichs und die damit verbundenen Herausforderungen für die öffentliche Verwaltung stellen damit zugleich auch die Tauglichkeit der Steuerungsressourcen „Recht, Verfahren und Organisation“ in der digitalen Gesellschaft und die notwendigen binnenorganisatorischen Umformungen des Staates, insbesondere der öffentlichen Verwaltung, auf die Probe.

C. Transformationsdynamiken einer standardmäßig digital agierenden Verwaltung (Kernforschungsthemen)

Dass sich staatliche Stellen nicht auf ein Mindestmaß elektronisch verfügbarer Verwaltungsleistungen beschränken, sondern ihre Dienste flächendeckend und proaktiv in digitaler Form über das Internet bereitstellen sollten, darüber besteht politische Einigkeit. Denn die Digitalisierung der gesamten Leistungs- und Ordnungsverwaltung ist ein wichtiges Fundament der Organisations- und Leistungsfähigkeit moderner Informationsgesellschaften. Mit Hilfe von Informations- und Kommunikationstechnologien kann die öffentliche Verwaltung ihre Aufgaben zielgenau, insbesondere entkoppelt von Zeit und Raum, dort anbieten, wo die Bürger sich in ihrem digitalisierten Alltag aufhalten.[97] Digitale, in effizienter Weise miteinander vernetzte Verwaltungsleistungen sind ein wichtiger Schlüssel, um Bürgern sowie Unternehmen Kosteneinsparungen, beispielsweise bei der Informationseinholung, in Zulassungs- und Genehmigungsverfahren oder im Abgabenwesen, zu ermöglichen.[98]

Soll die standardmäßige Verfahrensdigitalisierung („*digital by default*“) zugleich dazu beitragen, den öffentlichen Verwaltungsaufwand zu reduzieren, setzt dies jedoch grundsätzlich eine vollständige Online-Migration des Verwaltungsangebots voraus. Erst wenn der Staat seine digitalisierten Verwaltungsleistungen zumindest vorrangig und medienbruchfrei elektronisch anbietet und der Bürger diese, ohne allzu

---

97 Eine teilweise bzw. vollständige Umstellung auf digitale Angebote setzt aber unter anderem voraus, dass die Bürger die entsprechenden Kompetenzen (z. B. sub specie Datenverarbeitung sowie Umgang mit Begrifflichkeiten der Digitalisierung) besitzen, um Online-Angebote tatsächlich sinnvoll zu nutzen. Skeptisch dazu allgemein Initiative D21 (Fn. 6), S. 38 ff.: Demnach hat die Kompetenz im Umgang mit digitalen Angeboten im Jahresvergleich von 2015 auf 2016 mit der fortschreitenden Digitalisierung sogar abgenommen. So sehen 47 % der Bürger bei sich keine oder nur geringe Kompetenzen, eine Online-Überweisung vorzunehmen. Diese Entwicklung ist zugleich ein Spiegel der wachsenden Komplexität und Risikoanfälligkeit digitaler Angebote. Auf absehbare Zeit besteht auch deshalb die Notwendigkeit, Online-Verfahren im Grundsatz auch analog vorzuhalten.

98 Bürger in Deutschland bewerten vor allem Öffnungszeiten der Behörden (+ 0,73 auf einer Skala von - 2 bis + 2) und Wartezeiten bei Behördengängen (+ 0,82) als eher durchschnittlich, s. Statistisches Bundesamt, Zufriedenheit der Bürgerinnen und Bürger in Deutschland mit behördlichen Dienstleistungen, 2015, S. 10.

hohe Zugangshürden überwinden zu müssen, erreichen kann, lassen sich öffentliche Ausgaben in dem erhofften Umfang einsparen.[99]

Mit dem Konzept eines digitalen Verwaltungsstandards verbindet sich die Erwartung und Hoffnung, dass die Bürger die elektronischen Servicekanäle tatsächlich nutzen und mit der Verwaltung grundsätzlich auf elektronischem Wege kommunizieren.[100] Das setzt einfach zu bedienende, schnelle, effiziente und effektive Dienste für Bürger und Unternehmen voraus. Standardmäßig digitale Dienste sind so benutzerfreundlich zu gestalten, dass sich die Bürger aufgrund des erkennbaren Mehrwerts für ihre Nutzung entscheiden und möglichst wenige Personen dabei auf eine Assistenz oder den Rückgriff auf Papier- oder Präsenzkommunikation angewiesen sind.[101] Nur so lassen sich die technischen Innovationen mit den Leistungen und Gewährleistungen der öffentlichen Verwaltung funktionell verzahnen.

Gleicht man den Status quo mit den Zielvorstellungen eines Rechtsstaates in einer digitalen Welt ab, kristallisieren sich thesenartig erste digitale Handlungsgebote heraus:

---

99 Die Europäische Kommission schätzt das Einsparpotenzial auf EU-Ebene bei schrittweiser Umsetzung der Digital-by-Default-Strategie über einen Vier-Jahres-Zeitraum auf jährlich rund 6,5 Milliarden Euro und bei konzentrierter, schneller Realisierung des digitalen Verwaltungsstandards nach dem Vorbild des Vereinigten Königreichs auf jährlich bis zu 10 Milliarden Euro, vgl. Europäische Kommission, Study on eGovernment and the Reduction of Administrative Burden, 2014, S. 24 f.

100 Die Schubwirkung eines solchen Ansatzes hat jüngst die Arbeitsgruppe „Attraktivität des E-Government" des IT-Planungsrats in ihrem Abschlussbericht hervorgehoben: In Deutschland ist denjenigen E-Government-Angeboten besonderer Erfolg beschieden, deren Benutzung die öffentliche Verwaltung rechtlich und zielgruppenorientiert vorgibt und steuert, wie z. B. ELSTER (vgl. IT-Planungsrat, Entscheidungsniederschrift zur 18. Sitzung des IT-Planungsrats am 1. Oktober 2015 in Berlin, S. 4).

101 Vgl. dazu Europäisches Parlament, eGovernment – Using technology to improve public services and democratic participation, 2015, S. 4. Für vergleichbare Digital-by-Default-Strategien außerhalb der EU vgl. etwa die *Digital by Default Declaration* des australischen Bundesstaates South Australia vom November 2014, abrufbar unter http://digital.sa.gov.au/sites/default/files/content_files/declarations/Digital-by-Default-Declaration.pdf (30.11.2016).

- **These 1**: Die digitale Bereitstellung von Verwaltungsleistungen anstelle papierbasierter Verwaltungsverfahren birgt enormes Einsparpotenzial für die öffentlichen Haushalte – aber auch für die Wirtschaft und die Bürger.[102]
- **These 2**: Der öffentliche Sektor muss stärker datenbasiert und datengestützt agieren, wenn er an das digitale Ökosystem anschlussfähig sein will.[103]
- **These 3**: Der Staat der digitalen Gesellschaft ist durch neue Formen der netzwerkartigen Zusammenarbeit von öffentlichen (Politik, Verwaltung) und nicht-öffentlichen Stakeholdern (Wirtschaft, Zivilgesellschaft) im digitalen öffentlichen Raum gekennzeichnet.[104]
- **These 4**: Die veränderte digitale Handlungsumwelt sollte sich auch in der Binnenorganisation der Verwaltung abbilden. Für die netzwerkaffine Tätigkeit geeignete Organisationsprinzipien (bspw. Offenheit, Vertrauen, Flexibilität und Kollaboration) sollte sie adaptieren und den damit einhergehende Kulturwandel als Führungsaufgabe[105] begreifen.

Verdichtet man diese kognitiven und normativen Befunde, weist das Leitbild der digitalen Verwaltung vier Transformationsdynamiken für die öffentliche Verwaltung aus; sie bilden zugleich das Dach für die Architektur, unter der der Programmbereich seine Kernforschungsthemen bündelt:

---

102 Vgl. Europäische Kommission, A Digital Single Market Strategy for Europe - Analysis and Evidence, 2015, S. 75.

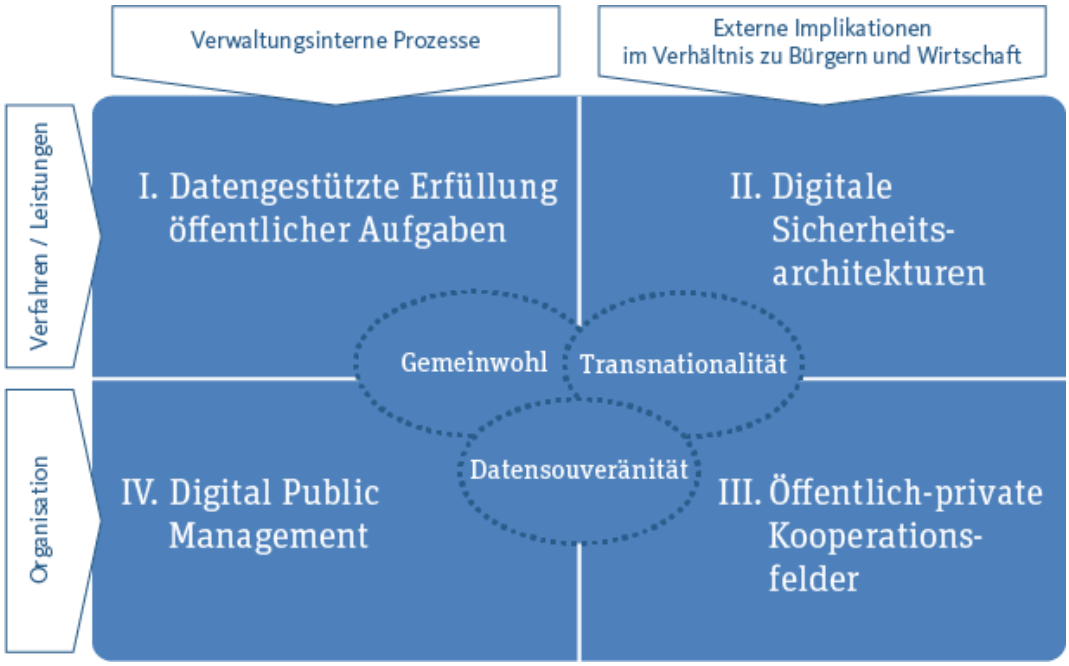
103 Vgl. dazu C.II, S. 39 ff.

104 Vgl. dazu etwa Nationale Plattform Zukunftsstadt, Die Zukunftsstadt – CO2-neutral, energie-/ressourceneffizient, klimaangepasst und sozial, 2015, S. 37; *Zweck/Holtmannspötter/Braun et al.* (Fn. 92), S. 186.

105 Vgl. *Tumin/Fung* (Fn. 96), S. 5 u. 13.

Die digitale öffentliche Verwaltung…

- …setzt für effizientes und informiertes Handeln verstärkt Big-Data-Anwendungen ein (Kernforschungsthema I.; S. 39 ff.).
- …ist dafür auf eine sichere digitale Infrastruktur und neue Methoden der Erkenntnisgewinnung angewiesen (Kernforschungsthema II.; S. 59 ff.).
- …kooperiert bei der digitalen Leistungserbringung in neuen Formen mit der Digitalwirtschaft (Kernforschungsthema III.; S. 66 ff.).
- …gestaltet ihre Aufbau- und Ablauforganisation nach Vorgaben der Organisationslogik von Netzwerken um und durchläuft dabei auch einen organisationskulturellen Wandel (Kernforschungsthema IV.; S. 72 ff.)



I. Die Dynamisierungsprozesse verbindende, übergreifende Leitaspekte

Die Kernforschungsthemen des Programmbereichs haben in unterschiedlicher Kombination und Tiefe verwaltungsinterne Prozesse oder externe Wechselwirkungen sowie Verfahrens- oder Organisationsgesichtspunkte zum Gegenstand. Miteinander verzahnt sind sie durch drei Leitaspekte, die den Weg in eine neue Daten- und Kommunikationsordnung ebnen und an denen sich jegliche digitale Entwicklung messen lassen muss: Gemeinwohlförderung (1.), Datensouveränität (2.) sowie Transnationalität (3.)

1. Gemeinwohlförderung unter den Bedingungen digitaler Mensch-Maschine-Interaktion

Als übergreifender Leitmaßstab jeglichen staatlichen Handelns nimmt das Gemeinwohlprinzip auch das digitale staatliche Handeln in die Pflicht.[106]

Das Grundgesetz[107] erwähnt das Gemeinwohl als verfassungsrechtlichen Grundwert zwar nur sporadisch. Es hebt die Gemeinwohlbindung aber in zahlreichen wichtigen normativen Bekenntnissen besonders hervor – insbesondere sub specie der Eigentumsfreiheit (als Richtschnur für Inhalts- und Schrankenbestimmungen [Art. 14 Abs. 2 S. 2 GG] auf der einen Seite und als Voraussetzung einer Enteignung [Art. 14 Abs. 3 S. 1 GG] auf der anderen Seite) sowie für die Amtseide des Bundespräsidenten (Art. 56 S. 1 GG), des Bundeskanzlers und der Bundesminister (Art. 64 Abs. 2 GG i. V. m. Art. 56 S. 1 GG).[108] Die dienende Funktion des Staates als eine treuhänderisch dem Allgemeininteresse verschriebene Einheit deutet auch das Republikprinzip des Art. 20 Abs. 2 GG an.[109] Im EUV scheint der Gemeinwohlgedanke in Art. 3 Abs. 1 besonders hell auf: Die Union verfolgt das Ziel, „das Wohlergehen ihrer Völker“ zu fördern. Im Geiste dieser Zielsetzung stellt die

---

106 BVerfGE 128, 226 (244). Siehe auch BVerfGE 42, 312 (332): „Das Grundgesetz hat nicht eine virtuell allumfassende Staatsgewalt verfaßt, sondern den Zweck des Staates materialiter auf die Wahrung des Gemeinwohls beschränkt, in dessen Mitte Freiheit und soziale Gerechtigkeit stehen.“

107 Auch die Landesverfassungen verpflichten alle staatlichen Akteure – in unterschiedlichen Ausprägungen – auf das Gemeinwohlprinzip. Beispielsweise gibt Art. 1 Abs. 2 RhPfVerf dem Staat auf, das Wohlergehen des einzelnen und der innerstaatlichen Gemeinschaften durch die Verwirklichung des Gemeinwohls zu fördern. Zusammenfassend *Martini*, Der Markt als Instrument hoheitlicher Verteilungslenkung, 2008, S. 221 f.

108 *Martini* (Fn. 107), S. 219 f. mit weiteren Beispielen. Der Verweis auf das Gemeinwohl schwört die Inhaber der Ämter nicht nur auf die Legalität ihres Tuns ein, sondern in seinen moralischen Bezügen auch darauf, das Wohl der Bürger mit ihrem ganzen Handeln integrativ zu verwirklichen. Vgl. etwa *Isensee*, § 71 Gemeinwohl im Verfassungsstaat, in: Isensee/Kirchhof (Hrsg.), HdbStR IV, 3. Aufl., 2006, Rn. 59.

109 *Anderheiden*, Gemeinwohl in Republik und Union, 2006, S. 267 ff.; *Martini* (Fn. 107), S. 220.

DSGVO als sekundärrechtliche Magna Charta des Persönlichkeitsschutzes die Verarbeitung personenbezogener Daten in den Dienst der Menschheit (Erwägungsgrund Nr. 4 S. 1 DSGVO).

Wiewohl nahezu alle Verfassungen die Verpflichtung des Staates auf das Gemeinwohl formulieren, halten sie sich im Hinblick auf die Konturierung seines Inhalts weithin bedeckt: Weder das Primärrecht der Union noch das Grundgesetz legen fest, was sie unter Gemeinwohl verstehen.[110] Das allgemeinste aller Staatsziele ist ohnehin nicht abschließend definierbar; möglich ist nur eine Annäherung an den Begriff via positiver und negativer Beschreibungsformeln.[111] Universales Kernelement des Gemeinwohlverständnisses ist eine Verpflichtung des Staates auf eine uneigennützige Aufgabenerledigung, welche das Wohlergehen seiner Bürger und der Allgemeinheit als solcher (der *res publica* im Sinne Ciceros) – in Abgrenzung zu den Partikularinteressen seiner Mitglieder – in den Mittelpunkt aller seiner Bemühungen stellt.[112] Auch und gerade in einem digitalen Kosmos ist das Gemeinwohl das Produkt einer Abwägung widerstreitender Interessen: Wirtschaftliche Wertschöpfung, Freiheitsrechte (insbesondere Persönlichkeitsschutz) und Sicherheit stehen als Zielgrößen der digitalen Entwicklung regelmäßig in einem Spannungsverhältnis. So entstehen Unternehmen bspw. zwangsläufig Kosten, wenn sie Datenschutzbeauftragte nach § 4f BDSG installieren müssen, um ein angemessenes Datenschutzniveau zu garantieren. Datenschutz gilt vielen daher häufig als Sand im Getriebe wirtschaftlicher Wertschöpfung. Gleiches gilt für die Datensicherheit: Ihrem Wesen nach errichtet sie Zugangshürden, die nicht nur den widerrechtlichen, sondern typischerweise auch den rechtmäßigen Nutzer treffen. Umgekehrt können sich die Interessen des Datenschutzes und der Datensicherheit auf der einen Seite und der wirtschaftlichen Wertschöpfung auf der anderen Seite auch ergänzen – etwa wenn ein hohes Datenschutzniveau eines Unternehmens die Bürger erst motiviert, diesem

---

110 *Anderheiden* (Fn. 109), S. 49, 52. Anders teilweise die Landesverfassungen: So bietet die Bayerische Verfassung in ihrem Art. 151 Abs. 1 eine Teildefinition, nach der das Gemeinwohl insbesondere ein menschenwürdiges Dasein und die Erhöhung des Lebensstandards umfasst.

111 Vgl. etwa *Isensee* (Fn. 108), Rn. 3; *Martini* (Fn. 107), S. 222 f., 233.

112 *Isensee* (Fn. 108), Rn. 36; *Kirchhof*, Das Wettbewerbsrecht als Teil einer folgerichtigen und widerspruchsfreien Gesamtrechtsordnung, in: ders. (Hrsg.), Gemeinwohl und Wettbewerb, 2005, S. 1 (7 f.); *Martini* (Fn. 107), S. 220.

ihre Daten zu offenbaren.[113] Der grundsätzliche Zielkonflikt und die besondere Herausforderung, die konkurrierenden Interessen zu einem sachgerechten Ausgleich zu bringen, bleibt dennoch bestehen. Gemeinwohlfindung ist in der digitalen ebenso wie in der analogen Welt ein Balanceakt. So versteht sich das Gemeinwohl in der digitalen Welt als Suchauftrag an den Staat und alle gesellschaftlichen Akteure, zwischen den Zielkoordinaten einer den Wertvorstellungen des Gemeinwesens entsprechenden digitalen Ordnung praktische Konkordanz herzustellen – ohne die Kunst des Kompromisses ist das nicht möglich.

2. Datensouveränität

Im Datenökosystem der digitalen Gesellschaft kommt den Grundwerten „Datenschutz“ und „Datensouveränität“ als Teilaspekten des Gemeinwohls eine herausragende Bedeutung zu. Sie sind Voraussetzung für die gesellschaftliche Verträglichkeit und Akzeptanz digitaler Innovationen.

a) Realbefund

Die Welt von morgen ist gespickt mit Sensoren. Sie begleiten den Einzelnen auf dem Weg zur Arbeit, in der U-Bahn, im Auto, im Supermarkt sowie beim Sport und fungieren damit als digitale Schnittstelle zum analogen Kosmos.[114] Mit der massierten Datengenerierung verknüpft sich die Möglichkeit, vorhandene Informationen in einer bisher nicht bekannten Tiefe auszuwerten.

Dem damit hebbaren enormen wirtschaftlichen Potenzial stehen Risiken für die Selbstentfaltung des Einzelnen gegenüber: In Zeiten ubiquitärer Datensammlung und -auswertung verliert der Internetnutzer mehr und mehr die Verfügungsgewalt über die eigenen digitalen Fußspuren. In der digitalen Welt ist Datenautonomie dadurch immer weniger erfahrbar – ebenso wie die Grenzen zwischen Privatem und Öffentlichem immer durchlässiger werden: Alltagsgegenstände mutieren zu Bewegungsmeldern, die viel über die Lebensgewohnheiten ihrer Nutzer zu erzählen wissen. Geräte wie das Smartphone oder der Smart Car,

---

113 The Boston Consulting Group, Earning Consumer Trust in Big Data: A European Perspective, 2015, S. 4 ff.

114 *Martini*, Wie werden und wollen wir morgen leben?, in: Hill/Martini/Wagner (Hrsg.), Die digitale Lebenswelt gestalten, 2015, S. 9 ff.

mit denen die Menschen die Hoffnung verbinden, sie trügen die digitale Freiheit in sich, mutieren schnell zur digitalen Fußfessel.[115] Die eigene Wohnung, einst Refugium individueller Entfaltung, leuchtet nun als Smart Home den digitalen Schatten aus, den der Bewohner an seine Wände wirft.[116] Die Smart Factory perfektioniert die alltägliche Überwachung des Mitarbeiters im Interesse einer Erhöhung seiner Produktivität. Die hochentwickelten Sensoren und Aktoren zur Optimierung von Arbeitsabläufen entwickeln sich zum Seismographen jeder menschlichen Regung.[117] Sie machen das Leben erfass-, entschlüssel- und berechenbar.[118] In den smarten Lebenswelten der Zukunft bleibt so kaum mehr etwas geheim.[119]

Die Geschäftsmodelle der digitalen Ökosysteme kommen dabei zumeist nur vordergründig als kostenlos daher. Die zahlreichen Annehmlichkeiten, mit denen sie das Leben versüßen, erkaufen sich die Nutzer zum Preis lückenloser Speicherung und Auswertung ihres Verhaltens sowie eines Kontrollverlustes über die autonome Verwendung personenbezogener Daten. Der Nutzer ist nicht länger nur der Kunde, er ist auch das Produkt, das der Anbieter zu verwerten trachtet.[120]

b) Schlussfolgerungen

Die widerstreitenden Interessen – wirtschaftliche Innovationskraft und Informationsgewinnung einerseits sowie Schutz bzw. Gewährleistung der Persönlichkeitsrechte des Einzelnen andererseits – mit technischem wie normativem Augenmaß auszubalancieren, ist Aufgabe eines zeitgemäßen Persönlichkeitsschutzes.[121]

---

115 *Martini* (Fn. 114), S. 27.

116 *Martini* (Fn. 114), S. 27 f.

117 Zur Funktionsweise neuronaler Netze und den Grundlagen künstlicher Intelligenz *Schlieter*, Die Herrschaftsformel, 2015, Kap. 7 bis 9, S. 47 ff.

118 Populärwissenschaftlich beschäftigen sich mit dem Themenkreis etwa *Albrecht*, Finger weg von unseren Daten!, 2014; *Aust/Ammann*, Digitale Diktatur, 2016; *Drösser*, Total berechenbar?, 2016; *Morgenroth*, Sie kennen dich! Sie haben dich! Sie steuern dich!, 2016; *Welzer*, Die smarte Diktatur, 2016.

119 *Martini* (Fn. 114), S. 27 f.

120 Dazu bspw. *Martini* (Fn. 114), S. 29 ff. m. w. N.

121 Siehe auch *Hill*, Verwaltung und Management 2016, 1 ff.; zur Innovationskraft im öffentlichen Sektor auch *Hill*, DÖV 2016, 493 ff.

Nur ein Individuum, das sowohl bei der Bereitstellung als auch im Umgang mit personenbezogenen Daten und Datenspuren selbstbestimmt agiert, ist den Herausforderungen der digitalen Welt gewachsen und kann ihre Potenziale für eigene Interessen entfalten. Ist digitale Aktivität demgegenüber von einem Gefühl des Kontrollverlustes über die eigenen Datenspuren und einer panoptischen Überwachung überschattet, erzeugt das ein um sich greifendes Misstrauen und ein diffuses Gefühl des Überwachtwerdens, von dem Abschreckungseffekte ausgehen.[122] Digitale Souveränität gehört daher zu den Leitideen guter digitaler Verwaltung und guter digitaler Staatlichkeit.

Der Staat ist in seiner Funktion als Schöpfer und Lenker der Institutionenordnung aufgerufen, klare Zuordnungen von Verfügungs- und Zugriffsrechten auf (Sach-)Daten und Datenflüsse Privater sowie der öffentlichen Hand vorzunehmen – insbesondere in der Smart City,[123] bei eingebetteten Systemen[124] und im „Internet der Dinge“[125]. Dazu gehört auch die Sicherung und Förderung der Kompetenzentwicklung zum souveränen Umgang mit datengestützten Verwaltungsvorgängen und Datenanalysen – sowohl bei Nutzern als auch bei den Mitarbeitern des öffentlichen Dienstes.[126]

---

122 Vgl. Fn. 46.

123 Siehe dazu im Einzelnen das Projekt „Smart Cities‘ Government: staatliche Infrastrukturaufgaben in der digitalen Welt“ (C.II.2, S. 47 ff.).

124 Damit beschäftigt sich das Projekt „Kooperative eingebettete Systeme: Vernetzung der öffentlichen Verwaltung mit intelligenten Industrie 4.0-Umgebungen“ (C.IV.1, S. 67 ff.).

125 Damit beschäftigt sich das Projekt „Algorithmenkontrolle als Regulierungsaufgabe“ (C.II.1, S. 42 ff.) im Unterprojekt „Algorithmenkontrolle im Internet der Dinge“ (C.II.1.b)bb), S. 46 f.).

126 Dazu das Projekt „Digital-transformationale Führung in der Netzwerkverwaltung“ (C.V.4, S. 81 ff.).

3. Transnationalität

In einer global vernetzten Datenwelt, deren Verarbeitungsvorgänge von Raum und Zeit weitgehend entkoppelt sind, lassen sich digitale Entwicklungen nicht alleine durch die Brille des Nationalstaats betrachten.[127] Dies zeigt bereits das exponentielle Wachstum des grenzüberschreitenden Datenaustausches: Weltweit hat er sich von 2005 bis 2014 um das 45-fache erhöht. Prognosen sagen bis 2021 eine Steigerung (im Vergleich zum Jahr 2005) um das 380-fache Voraus.[128] Der kometenhafte wirtschaftliche Aufstieg digitaler Global Player, wie Amazon, Google oder Facebook macht sie zum Abbild und Profiteur dieser Entwicklung.[129]

Angesichts der transnationalen Sphären, in denen sich die digitale Entwicklung bewegt, büßen nationale Rechtsordnungen immer stärker an Steuerungskraft ein.[130] Die digitale Transformation muss viel mehr als die analoge Welt in das Konzert des internationalen Rechts eingebunden und als Teil seiner Gesamtsymphonie gedacht werden. Das gilt nicht nur für den Inhalt der Regelungen, sondern auch für ihre Durchsetzbarkeit. Schon deshalb lassen sich Regulierungsideen nicht mehr alleine national denken; ein Vermeidungsverhalten der – teilweise sehr wirkmächtigen – Unternehmen lässt sich durch nationale Alleingänge kaum verhindern.[131] Es kommt zu einem Wettbewerb der Marktordnungen unter konkurrierenden Grundvorstellungen von Persönlichkeitsschutz. Die Pole seiner Erscheinungsformen bewegen sich zwischen digitalem Imperialismus und etatistischer Werte-Hegemonie.

Die Bedeutung der Transnationalität rückt zusehends in das Bewusstsein der politischen Entscheidungsakteure. Nicht nur die Regelungen der DSGVO zur Koordinierung der nationalen Aufsichtsbehörden

---

127 World Economic Forum (Fn. 4), S. 40.

128 McKinsey Global Institute, Digital Globalization: The new era of global flows, 2016, S. 31.

129 Der grenzüberschreitende direkte Handel ausländischer Unternehmen mit Verbrauchern über digitale Plattformen nimmt rasant zu. Das McKinsey Global Institute (Fn. 128), S. 35, geht von einem jährlichen Zuwachs des grenzüberschreitenden Handels zwischen Unternehmern und Verbrauchern von ca. 27 % aus.

130 *Martini* (Fn. 114), S. 39.

131 *Martini* (Fn. 114), S. 39 f.

machen das beispielhaft deutlich.[132] Auch das Marktortprinzip der neuen Magna Charta des Persönlichkeitsschutzes (Art. 3 Abs. 2 DSGVO)[133] dehnt den Anwendungsbereich des europäischen Datenschutzrechts auf alle Anbieter aus, die Personen in der Union Waren oder Dienstleistungen anbieten oder deren Verhalten in der Union beobachten – unabhängig davon, wo sich der Sitz des verarbeitenden Unternehmens befindet bzw. an welchem Ort es die Daten verarbeitet.[134] Mit diesen normativen Maßstäben reklamiert die Union als größter überstaatlicher Binnenmarkt der Welt für sich den Anspruch, ihre Bürger in einer entterritorialisierten Welt unter Rückgriff auf die Wirkmacht ihres Marktes wirksam vor einer Unterwanderung der Schutzstandards der Wertegemeinschaft zu bewahren.

II. Datengestützte Erfüllung öffentlicher Aufgaben

Daten sind der Treibstoff der Digitalisierung. Der sprunghaft von Tera- auf Zettabytes gestiegene jährliche Informationszuwachs und die umwälzenden technologischen Fortschritte bei der Datenspeicherung, -verarbeitung, -zusammenführung und -analyse erklimmen eine neue Evolutionsstufe der Informationsgesellschaft.

Während im privatwirtschaftlichen Bereich der ökonomische Nutzen der Massendatenauswertung im Vordergrund des Interesses steht, zielen Überlegungen zum Einsatz von Data Mining und Data Analytics im öffentlichen Sektor sowohl auf die gemeinwohlorientierte Optimierung

---

132 S. dazu *Kühling/Martini*, EuZW 2016, 448 (452 f.).

133 In seiner Google-Spain-Entscheidung (EuGH, Urt. v. 13.5.2014, Rs. C-131/12, ECLI:EU:C:2014:317 – Google) hat der EuGH dieses Prinzip in einer rechtspolitisch wünschenswerten, dogmatisch aber angreifbaren Weise dem Unionsrecht – bereits vor Verkündung der DSGVO – unterlegt. Ausführlich zum Urteil bspw. *Kühling*, EuZW 2014, 527 (527 ff.): Er sieht in dem Urteil ein „klares Signal" für den Datenschutz gegenüber Unternehmen aus Nicht-EU-Staaten. Vgl. auch die Safe-Harbor-Entscheidung des EuGH (EuGH, Urt. v. 6.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650): Die in Art. 7 und Art. 8 GrCh gewährleisteten Grundrechte auf Achtung des Privatlebens und Schutz personenbezogener Daten implizieren nach der Erkenntnis des Gerichts ein hohes Schutzniveau, das sich im Datenaustausch mit Drittländern vor allem in einem wirksamen und angemessenen Datenschutz widerspiegeln müsse.

134 Die Entgeltlichkeit ist nach dem Wortlaut des Art. 3 Abs. 2 DSGVO keine Voraussetzung, sodass grundsätzlich auch Suchmaschinen und soziale Netzwerke darunter fallen.

von Entscheidungsprozessen als auch auf eine effizientere Gestaltung von Verwaltungs- bzw. Fachverfahren. Das Potenzial, das im Big-Data-Universum steckt, ist beträchtlich.[135] Beispielsweise versprechen die Datenanalyse der Energiedaten von Smart Grids[136] und die Auswertung der Verkehrsdaten in Smart Cities ein verbessertes Bedarfs- und Risikomanagement der infrastrukturellen Daseinsvorsorge. Data-Mining-Anwendungen und auf Algorithmen gestützte Entscheidungsassistenten erleichtern die Bearbeitung und Bescheidung von Anträgen und unterbreiten automatisiert Entscheidungsvorschläge. Mittels Social-Media-Monitoring können Behörden Trendverläufe, Stimmungsbilder und Meinungsführer in sozialen Netzwerken ermitteln und dieses Wissen für das Risikomanagement von Großveranstaltungen, die Kriminalitätsbekämpfung oder die nachfrageorientierte Bürgerbeteiligung fruchtbar machen. Nach Meinung mancher erkennt man gar den Reifegrad ganzer Volkswirtschaften daran, wie fortgeschritten sie Big Data-Anwendungen einsetzen.[137]

Mit dem anschwellenden Datenstrom und der zunehmenden Steuerungsmacht von Datenanalyse-Werkzeugen verbinden sich aber auch beachtliche Risiken:

- Wer bestimmt über die Entscheidungsmuster, denen selbstlernende Algorithmen folgen?
- Welche Regulierungsaufgabe trifft den Staat, wenn Rechenprogramme gesellschaftlich sensible Bereiche (etwa Gesundheitsdaten) umfassend auswerten können?

---

135 Aus der inzwischen reichhaltigen Literatur zu Big Data siehe etwa *Boehme-Neßler*, DuD 2016, 419 ff.; *Cavanillas/Curry/Wahlster* (Hrsg.), New Horizons for a Data-Driven Economy, 2016; *Ehlen/Brandt*, CR 2016, 570 ff.; *European Data Protection Supervisor*, Meeting the Challenges of Big Data, 2015; *Geiselberger* (Hrsg.), Big Data, 2013; *Martini*, Big Data als Herausforderung für das Datenschutzrecht und den Persönlichkeitsschutz, in: Hill/Martini/Wagner (Hrsg.), Die digitale Lebenswelt gestalten, 2015, S. 97 (109 ff.); *Mayer-Schönberger/Cukier*, Big Data, 2013; *Raabe/Wagner*, DuD 2016, 434 ff.; *Richter*, DuD 2016, 581 ff.; *Roßnagel*, ZD 2013, 562 ff.; *Roßnagel/Nebel*, DuD 2015, 455 ff.; *Sarunski*, DuD 2016, 424 ff.; Fraunhofer Institut für intelligente Analyse- und Informationssysteme, BIG DATA – Vorsprung durch Wissen, 2012; *Werkmeister/Brandt*, CR 2016, 233 ff.

136 Vgl. Fn. 159.

137 Vgl. etwa die These bei *Giesberg*, Big Data wird zum Maßstab für den Fortschritt, FAZ vom 17.8.2015, S. 16.

- Wie fügen sich automatisierte Datensammlung und -archivierung, selbstlernende Algorithmen und künstliche Intelligenz in das grundrechtliche Koordinatensystem der informationellen Selbstbestimmung ein?
- Ist das aktuelle deutsche und unionale Datenschutzrecht für die neuartigen Datenverarbeitungsprozesse überhaupt ausreichend gerüstet?

Das Kernforschungsthema „Datengestützte Erfüllung öffentlicher Aufgaben“ greift diese übergreifenden Fragen aus einer vorwiegend rechtswissenschaftlichen Perspektive auf.[138]

138 Das Kompetenzzentrum Öffentliche IT (ÖFIT) des Fraunhofer-Instituts für offene Kommunikationssysteme (FOKUS) hat die technologischen Entwicklungen und Chancen von Big Data in einer Trendschau unter dem Schlagwort „Verwaltung x.0“ zusammengefasst: Kompetenzzentrum Öffentliche IT, Verwaltung x.0. Öffentliche Informationstechnologie in der digitalisierten Gesellschaft – Trendthema 29, 2015. Die bislang vorgelegten Studien gehen über eine Analyse gesellschaftlicher Trends für die öffentliche IT und der Identifikation sich daraus ergebender Handlungsfelder bewusst nicht hinaus. Die rechtliche und verwaltungswissenschaftliche Durchdringung der Herausforderungen und Chancen, die eine Massendatenanalyse durch die öffentliche Verwaltung mit sich bringt, steht demgegenüber noch aus – ihr widmet sich der Programmbereich „Digitalisierung“.

1. Algorithmenkontrolle als Regulierungsaufgabe

Big-Data-Algorithmenkontrolle als Regulierungsaufgabe (Martini/Kolain/Nink)	
Projekt-inhalt	Das Projekt „Algorithmenkontrolle als Regulierungsaufgabe“ widmet sich der Frage, welche rechtlichen Herausforderungen von selbstlernenden Algorithmen ausgehen, in welchen Bereichen dadurch grundrechtlich relevante Eingriffe zu befürchten sind und wie dem regulatorisch – bspw. durch Qualitätsnormung, Zertifizierung oder Wirkungskontrollen – zu begegnen ist.[139] Zu den Risikosphären algorithmenbasierter Entscheidungsfindung zählen insbesondere: Diskriminierungsrisiken des Einsatzes selbstlernender Algorithmen und dadurch ausgelöste Kontrollbedarfe; Normative Werteprogrammierung selbstlernender Algorithmen und Qualitätssicherungsmechanismen.
For-schungs-ziele	Analyse des grundsätzlichen normativen Regelungsbedarfs, insbesondere mit Blick auf Möglichkeiten der (regulierten) Selbstregulierung und Regelungsansätze in anderen Rechtsbereichen (GenDG, Hochfrequenzhandel, Atomenergie); Bewertung der Ausgestaltung, Leistungsfähigkeit und des Fortentwicklungsbedarfs der Datenschutz-Folgeabschätzung i. S. d. Art. 35 DSGVO.

Komplexe Datenverarbeitungsprozesse, die für den Betrieb eines „Internets der Dinge“[140], für Steuerungsvorgänge in der Infrastrukturregulierung und in der digitalen Produktion essenziell sind, beruhen auf Programmcode, den Algorithmen strukturieren und steuern.

---

139 Mit Blick auf die verbraucherschützenden Aspekte ist das Projekt teilweise drittmittelfinanziert: Der Programmbereich hat sich im Rahmen des Ausschreibungsverfahrens für das Förderprogramm „Innovationsförderung im Verbraucherschutz in Recht und Wirtschaft – Verbraucherbezogene Forschung über das ‚Internet der Dinge‘“ des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) mit seinem Antrag zur Algorithmenkontrolle als verbraucherpolitischem Schutzmechanismus durchgesetzt. Das Forschungsvorhaben analysiert regulatorische Ansatzpunkte für eine Kontrolle der Schaltstellen im „Internet der Dinge“ und erarbeitet praktisch nutzbare Lösungsvorschläge für eine wirksame und effektive Umsetzung einer Algorithmenkontrolle.

Algorithmen sind nicht wertungsfrei.[141] Sie gehen stets auf ethische Prämissen und Steuerungsziele ihrer Programmierer zurück, die den von ihnen Betroffenen in der Regel verschlossen bleiben. Je mehr Aufgaben die Gesellschaft teilweise oder ganz auf (vollständig oder teilweise) automatisierte Systeme auslagert und je (persönlichkeits-)sensibler die Sphären sind, in die selbstlernende Systeme eindringen und deren Informationen sie in die Datenverarbeitung einspeisen,[142] umso virulenter wird die Frage nach den (verfassungs-)rechtlichen Grenzen ihres Einsatzes, nach geeigneten Kontrollmethoden sowie nach staatlichen Organisationsstrukturen, um die technischen Möglichkeiten im Rahmen des für das Gemeinwohl Dienlichen und Akzeptablen zu halten.

Big-Data-Technologie weist vor diesem Hintergrund in mancher Hinsicht strukturelle Ähnlichkeit mit risikotechnologischen Innovationen,

---

Der Programmbereich hat einen zweiten Drittmittelantrag gestellt, der sich mit der Beobachtung und Diskussion von Kontrolldefiziten und Lösungsstrategien beim Einsatz algorithmisierter Dienstleistungen durch den Staat auseinandersetzt. Unter dem Titel „Kontrolldefizite algorithmisierter staatlicher Dienstleistungen“ soll das Projekt offenen Fragen im Zusammenhang mit der Kontrolle von Algorithmen in der öffentlichen Verwaltung nachgehen und Perspektiven für die Entwicklung von Lösungsstrategien erarbeiten. Ziel des Projekts ist es, die Problematik des Algorithmeneinsatzes zu analysieren sowie neue Kontrollstrategien disziplinübergreifend – zwischen Informationssicherheit, Rechts- und Verwaltungswissenschaften, Soziologie sowie Verwaltungs- und Wirtschaftsinformatik – zu diskutieren.

140 *Bräutigam/Klindt*, NJW 2015, 1137 ff.; *Evans*, Das Internet der Dinge, 2011; *Reichwald/Pfisterer*, CR 2016, 208 ff. Siehe auch bereits oben Fn. 2.

141 Teilweise wird deshalb eine „Algorithmen-Ethik“ vorgeschlagen, vgl. *Noller*, PinG 2013, 20 f.; Bundesjustizminister *Maas* hat eine Internet-Charta mit „digitalen Grundrechten“ in die öffentliche Debatte getragen, s. *Maas*, Unsere digitalen Grundrechte, Die ZEIT vom 10.12.2015. Vgl. dazu auch den zivilgesellschaftlichen Vorschlag einer Charta der Digitalen Grundrechte der Europäischen Union, abrufbar unter http://digitalcharta.eu/ (30.11.2016). Die ethischen und moralischen Aspekte von Algorithmen beleuchten *Steinmann/Shuster/Collmann et al.*, Embedding Privacy and Ethical Values in Big Data Technology, in: Matei et al. (ed.), Transparency in Social Media, 2015, S. 277 ff.

142 Vgl. zu diesem Themenkreis auch die in Fn. 118 zitierte populärwissenschaftliche Literatur.

wie etwa der Gentechnik oder der Nanotechnologie, auf: Ihr Gemeinwohlpotenzial ist enorm, solange die Gesellschaft ihre Wirkmacht unter Kontrolle hat. Geraten Risikotechnologien in die falschen Hände oder werden sie missbräuchlich eingesetzt, können sie allerdings kaum beherrschbaren Schaden anrichten.[143] Die Delegation immer weiter reichender Entscheidungen an immer komplexer konfigurierte, intransparente und autonom agierende Systeme birgt bei ungenügender Risikovorsorge – ähnlich wie bei gentechnischen Innovationen – die Gefahr eines folgenschweren Kontrollverlustes.[144] Sachgerechte Big-Data-Regulierung bedarf daher einer effektiven Algorithmenkontrolle.[145]

Wie eine wirksame Algorithmenkontrolle technisch möglich und rechtlich umsetzbar sein kann, stellt eine Gesellschaft, ihren Umgang mit Technik sowie ihre Rechtsordnung vor zahlreiche Fragen. In der Philosophie und der Informatik finden sich erste Überlegungen zu den Herausforderungen, welche insbesondere Robotik und autonome Systeme für die regulatorische Steuerung von komplexen Systemen auslösen.[146] Was das für die normative Steuerung von gesellschaftlich relevanten Prozessen konkret bedeutet, ist aber bislang noch nicht abschließend diskutiert und erforscht. Überhaupt gilt: Die rechtlichen, ethischen und ökonomischen Herausforderungen, denen sich die Erschließung des gemeinwohldienlichen Leistungsportfolios von Big-Data-Technologien gegenübersieht, harren bislang einer fundierten Antwort. Ohne ein grundlegendes Verständnis der technischen Funktionszusammenhänge kann diese nicht gelingen.

---

143 Dazu bereits etwa *Martini* (Fn. 135), S. 153.

144 Gleichermaßen warnend wie auch mehr Transparenz einfordernd *Pasquale* (Fn. 45), S. 145 ff.

145 Dazu bereits *Martini* (Fn. 114), S. 153.

146 Vgl. dazu beispielsweise die Beiträge bei Beck (Hrsg.), Jenseits von Mensch und Maschine, 2012; *Beck*, JR 2009, 225 ff.; Capurro (Hrsg.), Ethics and robotics, 2009; Hilgendorf/Günther (Hrsg.), Robotik und Gesetzgebung, 2013.

a) Diskriminierungsverbote

Mit der Delegation hoheitlicher Entscheidungen an digitale Assistenzsysteme verbinden sich Big-Data-spezifische Diskriminierungsrisiken, die den grundrechtlichen Gleichbehandlungsgrundsatz[147] und auch sozialstaatliche Teilhaberechte auf das juristische Prüfungstableau rufen. Ihnen gilt es, durch Qualitätsvorgaben für die Programmierung der Software und ihrer Selbstlernmechanismen Rechnung zu tragen.

b) Kontrollmechanismen

Das Leitbild einer transparenten Verwaltung (Open Government) sowie das Nutzungspotenzial effizienter, vollautomatisierter Verwaltungsverfahren[148] stehen zur Intransparenz selbstlernender Big-Data-Analysealgorithmen in einem Spannungsverhältnis: Je weniger die von der Verwaltung für ihre Entscheidungsfindung genutzten Analyse-Tools und Entscheidungsassistenten nachvollziehbare Analyseergebnisse und darauf aufbauende Empfehlungen produzieren, desto größer sind die rechtsstaatlichen Bedenken ihres Einsatzes im Hinblick auf die Prinzipien der Begründbarkeit und Verantwortungsklarheit.

aa) Regulierungsansätze des unionalen Datenschutzrechts

Das Phänomen der algorithmenbasierten Entscheidungsfindung tangiert das Verbot automatisiert generierter Einzelentscheidungen, wie es bisher § 6a BDSG und – als dessen unionsrechtliche „Ablösung“ – nunmehr Art. 22 DSGVO[149] anlegen. Den Vorschriften liegt eine überzeugende Leitidee zugrunde: Kein Mensch darf zum bloßen Objekt eines Algorithmus werden. Sie verstehen sich als Ausprägung des Menschenwürdegedankens, zu dem sich unsere Rechtsordnung als unverfügbarem Eigenwert gesellschaftlicher Ordnung bekennt. Aus diesem Grund stellt die DSGVO automatisiert generierte Entscheidungen – dazu zählt

147 Dazu aus populärwissenschaftlich-soziologischer Sicht der Chefredakteur des Magazins GEO *Kucklick*, Die granulare Gesellschaft, 2014, S. 43 ff.

148 Mit diesem neuen Typus des Verwaltungsverfahrens beschäftigt sich das Projekt „Regelungsbedarf und rechtliche Grenzen elektronischer vollautomatisierter Verwaltungsverfahren“ (C.II.6, S. 57 ff.).

149 Dazu ausführlich *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO, 2016, Art. 22, Rn. 15 ff.

auch das sog. Profiling[150] – vor Zulässigkeitshürden: Sie sind nur rechtmäßig, wenn sie entweder in vertraglichen Beziehungen erforderlich sind, wenn sie aufgrund einer entsprechenden Rechtsvorschrift[151] erfolgen oder wenn der Betroffene eingewilligt hat.

Für die gesellschaftliche Akzeptanz von Big-Data-Technologien und einen wirksamen Persönlichkeitsschutz in der digitalen Welt wird es darauf ankommen, wie die Rechtsordnung auf die grundrechtssensiblen Diskriminierungs- und Wettbewerbsrisiken reagiert, die von dem Einsatz intransparenter Entscheidungsalgorithmen im privaten und staatlichen Bereich[152] ausgehen. Besonderes Regulierungspotenzial kann insoweit der durch Art. 40 ff. DSGVO vorgezeichneten (regulierten) Selbstregulierung[153] sowie Formen der Ko-Regulierung zuwachsen. Auch der Datenschutz-Folgenabschätzung wird hierbei eine wichtige Rolle als Regulierungsinstrument zukommen.[154]

bb) Algorithmenkontrolle im „Internet der Dinge“

Im „Internet der Dinge“ lassen sich Daten- und Verbraucherschutz kaum sauber voneinander abtrennen. Ein verbrauchschutzfreundliches „Internet der Dinge“ ist ohne eine kontrollierte, diskriminierungsfreie und gemeinwohlorientierte Infrastruktur sowie Schnittstellenverwaltung undenkbar.

Dass die Rechtsordnung Algorithmen weithin als Betriebsgeheimnis einstuft[155] und einer staatlichen Kontrolle ab einer kritischen Schöpfungshöhe grundsätzlich entzieht, löst eine regulierungspolitische Konfliktlage zu dem Anspruch Deutschlands und der EU aus, einen Raum

---

150 Dazu *Martini* (Fn. 149), Art. 22, Rn. 21 ff.

151 Die Öffnungsklauseln der DSGVO begutachten umfassend *Kühling/Martini/Heberlein et al.*, Die DSGVO und das nationale Recht – Erste Überlegungen zum nationalen Regelungsbedarf, 2016.

152 Vgl. *Pariser* (Fn. 54); siehe auch *Hofstetter*, APuZ 2015, 33 ff.; *Hofstetter*, Sie wissen alles, 2014.

153 Siehe dazu am Beispiel des Geodatenschutzrechts *Martini*, NVwZ-Extra 3/2016, 1 (10 ff.).

154 *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO, 2016, Art. 35, Rn. 3 ff.

155 Dies gilt im Falle der Scoring-Formel bei der Kreditauskunft der SCHUFA bereits nach dem ausdrücklichen Willen des historischen Gesetzgebers, vgl. BT-Drs. 16/10529, S. 17: „[…] die Score-Formel, an deren Geheimhaltung die Unternehmen ein überwiegendes schutzwürdiges Interesse haben“. Vgl. dazu auch BGHZ 200, 38 ff.; *Martini* (Fn. 114), S. 134 ff. m. w. N.

hoher Datenschutzstandards zu etablieren. Algorithmen entpuppen sich so schnell als „Blackbox“, in der substanzielles Gefährdungspotenzial für die Grundrechte der Verbraucher schlummert. Im „Internet der Dinge“ gilt dieser Befund insofern in besonderer Weise, als sich hier zur fehlenden Transparenz eine für den Einzelnen kaum überschaubare Masse und Komplexität an Datenflüssen hinzugesellt, die ohne technische Hilfsmittel (etwa Visualisierung oder Suchmasken) und staatliche Einflussmöglichkeiten weder versteh-, geschweige denn kontrollierbar sind. Der Verwirklichung des Grundrechts auf informationelle Selbstbestimmung, dem Prinzip der Nachvollziehbarkeit hoheitlicher Entscheidungen und dem Grundsatz der Datensouveränität legt das Steine in den Weg. Umso mehr ist die Forschung aufgerufen, nach geeigneten Regulierungsansätzen Ausschau zu halten, um die im „Internet der Dinge“ lauernden Gefahren im Interesse des Gemeinwohls einzuhegen.

2. Smart Cities‘ Government: staatliche Infrastrukturaufgaben in der digitalen Welt

Smart Cities’ Government: staatliche Infrastrukturaufgaben in der digitalen Welt (Martini/Rehorst)	
Projektinhalt	Das Projekt richtet seinen Blick auf neue Koordinierungs-, Steuerungs- und Ordnungsaufgaben im Zusammenhang mit intelligenten Verkehrssystemen, autonomen Fahrzeugen sowie intelligenten Strom- und anderen Infrastrukturnetzen, Zählern und Verbrauchsgeräten.
Forschungsziele	Identifizierung der gesetzgeberischen und (fach-)behördlichen Regelungsnotwendigkeiten für die hoheitliche Koordination und aufsichtsrechtliche Kontrolle intelligenter Verkehrs- und Energiesysteme; Klärung der Verfügungshoheit über Fahrzeug-, Netz- und Gebäudedaten sowie notwendiger Zugangs- und Interventionsmöglichkeiten in autonom agierende Infrastruktursysteme.

Der Trendbegriff „Smart Cities‘ Government“ wirft ein Schlaglicht auf das gemeinwohlförderliche Potenzial intelligenter Vernetzung im öffentlichen Raum. In einer mit Sensoren gespickten Welt schlummern große Chancen für eine moderne digitale Infrastruktur (insbesondere den ÖPNV und die Energiesysteme) – aber auch Herausforderungen.

Das Automobil der Zukunft trifft eigenständig Entscheidungen und ist mit seiner Umgebung vernetzt: Die einzelnen Bauteile kommunizieren nicht nur mit dem digitalen Autopiloten, sondern auch mit anderen am Verkehr teilnehmenden Fahrzeugen (warnen diese etwa vor Glatteis oder einem unvermittelten Stauende). In die Fahrbahn eingelassene Sensoren zählen Fahrzeuge, messen Geschwindigkeiten und steuern den Fluss des individuellen wie öffentlichen Personenverkehrs.[156] Automatisierung und Vernetzung ebnen damit einer effizienten Ausnutzung der Verkehrsinfrastruktur unter den Bedingungen erhöhter allgemeiner Mobilität den Weg.

Gerade mobile Anwendungen eröffnen bislang ungeahnte Möglichkeiten gemeinwohlorientierter Datenauswertung.[157] Der Verkehrsfluss in der Smart City[158] vermeidet Staus und lange Wartezeiten an Bushaltestellen und Bahnhöfen: Auf der Grundlage von Positions- und Bewegungsdaten der Verkehrsteilnehmer lassen sich Schwerpunkte der Verkehrsauslastung ermitteln, Verkehrsströme lenken, typische Unfallherde erfassen (und vorhersagen) sowie die Potenziale des öffentlichen Nahverkehrs ausreizen. Intelligente Mobilitätssysteme vernetzen den öffentlichen und privaten Verkehr nahtlos zu einem übergreifenden Ökosystem. Auch die Datenanalyse von Smart Grids (intelligente Stromnetze)[159] verheißt ein verbessertes Bedarfs- und Risikomanagement bei der infrastrukturellen Daseinsvorsorge.

---

156 Dazu *Martini* (Fn. 114), S. 13.

157 Dazu auch *Buschauer*, (Very) nervous systems. Big Mobile data, in: Reichert (Hrsg.), Big Data, 2014, S. 405 ff. Mit der Thematik setzt sich auch das Projekt „Organisationsprinzipien des Mobile Government“ (C.V.1, S. 74 f.) auseinander.

158 Vgl. zum Begriff und zum ökonomischen Potenzial etwa VDE, VDE-Trendreport 2014 – Schwerpunkt: Smart Citys, 2014, S. 4 f.; *Etezadzadeh*, Smart City – Future City?, 2016 sowie allgemein zur gesellschaftspolitischen Diskussion *Bullinger/Röthlein*, Morgenstadt, 2012; *Cocchia*, Smart and digital city – A systematic literature review, in: Dameri/Rosenthal-Sabroux (Hrsg.), Smart City, 2014, S. 13 ff.; *Galdon-Clavell*, Science and Public Policy 40 (2013), 717 ff.; *Franz*, Smart or not smart – What makes a city intelligent?, in: Widmann (Hrsg.), Smart city, 2012, S. 28 ff.; *Kaczorowski*, Die smarte Stadt, 2014; *Swarat/Haselbeck*, Smart Country – Digitale Strategien für Regionen, Executive Summary, 2014; *Townsend*, Smart cities, 2013.

159 Bundesnetzagentur, „Smart Grid“ und „Smart Market“, 2011; *International Energy Agency*, Smart Grids, 2011; *Karsten*, Datenschutz im Smart Grid &

In diesen Handlungsfeldern zeichnen sich schon in naher Zukunft digitalisierte bzw. (voll)automatisierte Einsatzszenarien ab – insbesondere im kommunalen Aufgabenbereich (Stadtwerke, Verkehrsbetriebe etc.), aber auch bei der ebenenübergreifenden Koordination.

An die neuen technischen Möglichkeiten knüpfen sich aber auch grundsätzliche Fragen, welche die Entwicklung der „vernetzten Stadt" auch jenseits des Verkehrsbereichs betreffen:[160]

- In welchem Umfang und unter welchen Bedingungen ist es überhaupt vertretbar, den Datenfluss in der Smart City (auch) staatlichen Stellen zufließen zu lassen bzw. Daten zwischen privaten und öffentlichen Stellen auszutauschen? Wie kann der Staat die Daten vernetzter privater Geräte und eingebetteter Systeme für die öffentliche Aufgabenwahrnehmung bündeln, ohne dadurch unverhältnismäßig in das Eigentum, die Berufsausübung oder den freien Wettbewerb der Gerätehersteller, Datengeneratoren, Big-Data-Hosting- und Cloud-Provider einzugreifen?
- Wie lässt sich ein Rechtsrahmen für sog. Open Private Data sachgerecht zuschneiden, der „Datenabgabe"pflichten Privater, rechtliche Zuordnungen von Rechten an Daten sowie Informationsrechte des Staates normiert und eine entsprechende Indienstnahme anordnet?
- Wie lässt sich die bereitgestellte Informations- und Kommunikationstechnologie sicher[161], vertraulich sowie frei von Diskriminierungspotenzialen konzipieren?

Smart Meter, 2015; *Neumann/Moorfeld/Reulke*, Die Digitalisierung der Energiewende – vom Smart Grid zur intelligenten Energieversorgung, in: Wittpahl (Hrsg.), Digitalisierung, 2017, S. 141; Zentralverband Elektrotechnik- und Elektroindustrie e.V./Bundesverband der Energie- und Wasserwirtschaft, Smart Grids in Deutschland, 2012.

160 Vgl. zu der technologischen Dimension der Thematik etwa *Allwinkle/Cruickshank*, Journal of Urban Technology 18 (2011), 1; *Budde*, Cities for Smart Environmental and Energy Futures – Impacts on Architecture and Technology, in: Rassia/Pardalos (Hrsg.), Cities for smart environmental and energy futures, 2014; *Erbstößer*, Smart City Berlin – Urbane Technologien für Metropolen, Report 2014, 2014; zu den Herausforderungen von Smart Grids für den Persönlichkeitsschutz etwa *Guckelberger*, DÖV 2012, 613 ff.; *Karsten* (Fn. 159), S. 41 ff.

161 Vgl. dazu etwa Ausschuss Bildung, Forschung und Technikfolgenabschätzung, TA-Projekt: Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung, BT-Drs. 17/5672.

3. *Social-Media-Monitoring durch die öffentliche Verwaltung*

Social-Media-Monitoring durch die öffentliche Verwaltung (Martini/Ammerich/Kolain/Wagner)	
Projekt-inhalt	Der Begriff „Social-Media-Monitoring durch die öffentliche Verwaltung“ umreißt ein sensibles Thema, das in der öffentlichen Wahrnehmung viel, in seiner (rechts-)wissenschaftlichen Aufarbeitung bisher aber nahezu keine Resonanz erfahren hat: eine Auswertung der Inhalte sozialer Netzwerke und sonstiger öffentlich zugänglicher Datenreservoirs durch staatliche Stellen (etwa zu Zwecken kontinuierlicher Trend- und Meinungsforschung, zeitgerechter Risikoprävention, der Gefahrenabwehr oder zur Vorfeld- und Erfolgsanalyse bürgerschaftlicher Partizipationsangebote). Das Projekt lotet die Möglichkeiten und rechtlichen Grenzen einer Analyse nutzergenerierter Inhalte auf unterschiedlichen Plattformen (insbesondere sozialer Netzwerke) aus.
Forschungs-ziele	Identifikation des Leistungspotenzials und der rechtlichen Hürden von Social-Media-Monitoring durch die öffentliche Verwaltung.

Soziale Netzwerke sind das Futter immer ausgereifterer Spielarten der Big-Data-Analyse und künstlichen Intelligenz: Ihre Datensätze können mithilfe von Algorithmen rekonstruieren und prognostizieren, wie der *Homo digitalis* sich verhält – und lernen die Kunst, menschliche Entscheidungen gezielt zu beeinflussen. Dass Facebook den Ausgang demokratischer Wahlen beeinflussen kann, ist inzwischen kein Geheimnis mehr. Schon heute nimmt eine ganze Armada von Propaganda-„Bots“ gezielt Einfluss auf die öffentliche Meinungsbildung.

Technologien der Sentimentanalyse und Algorithmen zur Auswertung der Interaktion in sozialen Netzwerken sind bereits weit entwickelt und vielfach im praktischen Einsatz. Dank ihrer Multifunktionalität verheißen die auf dem Markt in großer Zahl vorfindlichen Monitoring-Tools, die Ernte stetig wachsender Datenfelder einzufahren und automatisiert die Spreu vom Weizen zu trennen. Sie machen sich damit das Kommunikationsbedürfnis, aber auch den Hang zur Selbstdarstellung der Menschen zunutze.[162]

Mittels Social-Media-Monitoring lassen sich Präferenzartikulationen der Bevölkerung erfassen und typische Verhaltensmuster erkennen, um

---

162 *Martini* (Fn. 135), S. 121 f.

daraus Potenziale für sehr unterschiedliche Zwecke abzuleiten, die von der Gemeinwohlentwicklung bis hin zur Produktoptimierung reichen.[163]

Private Unternehmen folgen dem Analysepfad des Social-Media-Monitorings bereits seit geraumer Zeit; öffentliche Stellen folgen mit Verzögerung, aber immer nachhaltiger.[164] Die öffentliche Verwaltung nutzt ihre Möglichkeiten nicht nur zur Evaluation behördeneigener Social-Media-Präsenzen, sondern auch zur Trend- und Meinungsforschung, zur politischen Strategieoptimierung und als Stethoskop politischer Krisen-

---

163 Zu den Anwendungsfeldern und Einsatzszenarien ausführlich *Aßmann/Pleil*, Social Media Monitoring: Grundlagen und Zielsetzungen, in: Zerfaß/Piwinger (Hrsg.), Handbuch Unternehmenskommunikation, 2007, S. 585 ff.; *Hoffmann/Schulz/Brackmann*, Web 2.0 in der öffentlichen Verwaltung, in: Schliesky/Schulz (Hrsg.), Transparenz, Partizipation, Kollaboration, 2012, S. 163 ff.; *Gentsch/Zahn*, Potenziale und Anwendungsfelder von Web-Monitoring im Unternehmen, in: Brauckmann (Hrsg.), Web-Monitoring, 2010, S. 97 ff.; *Hofmann*, Methoden des Social Media Monitoring, in: König/Stahl/Wiegand (Hrsg.), Soziale Medien, 2014, S. 161; *Plum*, Methoden und Technologien des Web-Monitorings – ein systematischer Vergleich, in: Brauckmann (Hrsg.), Web-Monitoring, 2010, S. 21; *Werner*, Social Media – Analytics & Monitoring, 2013, S. 116 ff.; *Solmecke/Wahlers*, ZD 2012, 550 ff. Dazu auch mit US-amerikanischem Blickwinkel President's Council of Advisors on Science and Technologie, Report to the President: Big Data and Privacy: A technological Perspective, 2014, S. 28 f.; *Pentland*, Social physics, 2014.

164 Zwar finden sich zum Social-Media-Monitoring nicht-öffentlicher Stellen bereits erste Veröffentlichungen. Siehe etwa *Schreiber*, PinG 2 (2014), 34 ff.; *Sen*, Social Media Monitoring für Unternehmen, 2011; *Venzke-Caprese*, DuD 2013, 775 ff. Mit Blick auf die – einem anderen regulatorischen Regime unterworfenen – öffentlichen Stellen fehlte es im deutschsprachigen Raum zu diesem Thema demgegenüber bislang an rechts- und verwaltungswissenschaftlichen Forschungsarbeiten. Dem hat das Forschungsprojekt abgeholfen: In einer ersten Publikation zum Social-Media-Monitoring öffentlicher Stellen analysiert es die rechtlichen und technischen Grundlagen – im Fokus stehen verfassungs- und datenschutzrechtliche Fragen (unter Berücksichtigung der Neuerungen durch die DSGVO): *Martini*, VerwArch. 107 (2016), 307 ff. Ihre Forschungsergebnisse zu Chancen und Grenzen des Einsatzes von Social-Media-Monitoring haben die Wissenschaftler des Forschungsprojekts zudem im Rahmen des Zukunftskongresses „Staat und Verwaltung“ am 21.6.2016 in Berlin vor- und zur Diskussion gestellt.

intervention. Nicht zuletzt interessieren sich auch und insbesondere Sicherheitsbehörden für die digitalen Datenberge und die darin verborgenen Ermittlungsschätze.[165]

Dass die deutsche öffentliche Verwaltung das Leistungsportfolio des Social-Media-Monitorings im internationalen Vergleich nur zögerlich erschließt, gründet sich auch auf Rechtsunsicherheiten, die das Monitoring mit sich bringen kann. Mit ihm verbindet sich das Risiko einer digitalen Blockwart-Mentalität, welche die individuelle Entfaltungsfreiheit unter eine Glocke der Dauerbeobachtung sperrt.[166] Eine vollständige Erfassung des Informationsstroms sozialer Netzwerke droht die demokratische Selbstentfaltung und unbefangene Entwicklung der digitalisierten Gesellschaft zu ersticken.[167] Die Grenze zu erkennen, ab der der Staat auf den digitalen, in sozialen Netzwerken offen zutage liegenden Datenschatz als Instrument behördlicher Entscheidungsunterstützung zugreifen darf, ohne zu einem Überwachungsstaat zu mutieren, verlangt der legislativen und exekutiven Staatsgewalt daher besonderes Feingespür ab.

---

165 Vgl. etwa *Richards*, Intellectual privacy, 2015, S. 109 ff.

166 Siehe auch den kurzen Essay von *Martini*, Angst vor einem digitalen Blockwart, FAZ vom 27.10.2016, S. 6.

167 Vgl. etwa die allgemeine Wertung des BVerfG in Rn. 153 seines Urteils zu NSA-Selektoren, s. Fn. 47.

4. Mitgliedstaatliche Regelungsspielräume unter der Datenschutz-Grundverordnung

Mitgliedstaatliche Regelungsspielräume unter der Datenschutz-Grundverordnung – Wandel der Datenschutzprinzipien in Zeiten von Big-Data (Martini/Nink/Weinzierl)	
Projektinhalt	Das Forschungsprojekt greift das Zusammenspiel zwischen der DSGVO und dem nationalen Datenschutzrecht auf und gleicht deren bisherige Konzepte mit den Funktionsbedingungen der Digitalisierung ab. Projektschwerpunkte sind: • Regulatorische Neuerungen der DSGVO (insbesondere für die Rechtsanwendung in der deutschen öffentlichen Verwaltung) und die Reichweite des Regelungsspielraums, den sie den Mitgliedstaaten belassen; • Konfliktlagen zwischen den wirtschaftlichen Chancen einer Massendatenauswertung und den Grundwerten des Persönlichkeitsschutzes (insbesondere mit Blick auf die persönlichkeitsrechtlichen Prinzipien der Datenminimierung bzw. -sparsamkeit, Transparenz, Zweckbindung sowie Direkterhebung)
Forschungsziele	Analyse der unionsrechtlichen Vorgaben und verbleibender nationaler Regelungsspielräume bei der Ausgestaltung der Datenschutzprinzipien.

Die Grundstrukturen des Datenschutzrechts stammen noch aus einer Zeit von Lochkarten und Aktenordnern. Während im Jahre 1983 die Ankündigung einer Volkszählung die Bevölkerung in helle Aufregung versetzte und das daran anknüpfende Grundsatzurteil des BVerfG[168] gleichsam zur Geburtsstunde modernen Datenschutzrechts avancierte, gehen Volkszählungen im 21. Jahrhundert (so etwa im Fall des Zensus 2011[169]) vergleichsweise geräuschlos vonstatten. Der gesellschaftliche Umgang mit persönlichen Daten sowie die Wahrnehmung ihrer Sensibilität haben seither einen teilweise grundlegenden Wandel erfahren. Für viele „Digital Natives“ ist es im 21. Jahrhundert selbstverständlicher Teil ihres Alltags, Mahlzeiten, Verabredungen, bisweilen sogar intime Momente mit einem unbestimmten Personenkreis auf Facebook, Instagram und Co. zu teilen.

168 BVerfGE 65, 1.

169 Vgl. zum Zensus 2011 im Hinblick auf das Gebot kommunaler Gleichbehandlung *Martini*, Der Zensus 2011 als Problem interkommunaler Gleichbehandlung, 2011.

Fitness-Armbänder, Smart Homes und soziale Medien bergen – ungeachtet der Erleichterungen des Alltags, die sie dem Einzelnen vermitteln, und ihrer innovativen Wertschöpfungspotenziale – zugleich gänzlich neue Bedrohungsszenarien für die Privatsphäre des Einzelnen. Spätestens seit den Enthüllungen des Whistleblowers *Edward Snowden* ist der Öffentlichkeit ins Bewusstsein gerückt, dass eine anlasslose Massenaufzeichnung des digitalen Datenstroms keine Science-Fiction mehr ist.[170]

Die digitale Vermessung der Welt wirft zahlreiche Grundsatzfragen auf, insbesondere:

- Wie lassen sich in einer Umgebung der digitalen Einhegung und der freiwilligen Preisgabe persönlicher Daten die Datenschutzprinzipien der Transparenz, der Datensparsamkeit, der Direkterhebung sowie der Zweckerforderlichkeit realisieren und durchsetzen, ohne die wirtschaftliche Innovationsfähigkeit digitaler Technologien auszubremsen? Wie müss(t)en Datenverarbeitungsvorgänge gestaltet bzw. modifiziert werden, um in Einklang mit den Vorgaben von Art. 2 Abs. 1 Abs. 1 i. V. m. Art. 1 Abs. 1 S. 1 GG zu stehen?
- Erfordert das digitale Zeitalter gar eine völlige Neujustierung der informationellen Selbstbestimmung und des Verständnisses von Privatsphäre?
- Kann ein Koppelungsverbot eine Lösung bieten – oder eine Verpflichtung der Diensteanbieter, neben kostenlosen datenhungrigen Onlinediensten gleichwertige kostenpflichtige Dienste vorzuhalten?
- In welche Richtungen verändert die DSGVO den materiellen Datenschutz, seine mitgliedstaatliche Implementierung und justizielle Durchsetzung sowie die jeweiligen Aufsichtsstrukturen?

Die 28 Mitgliedstaaten der Europäischen Union haben sich mit Erlass der DSGVO darauf verständigt, auf ihrem gemeinsamen Markt international hohe Standards im Umgang mit personenbezogenen Daten zu etablieren. Es sind weniger die materiell-rechtlichen Neuerungen, mit denen sie Akzente setzt. Vor allem das Marktortprinzip[171] und eine Modifikation der unionalen Datenaufsichtsstruktur läuten eine datenschutzrechtliche „Frischzellenkur“ ein, deren Wirkung weit über die Grenzen der Union hinausstrahlt: Der Unionsgesetzgeber verpflichtet

---

170 Zu den Hintergründen des NSA-Skandals bspw. *Greenwald*, Die globale Überwachung, 2014; *Rosenbach/Stark*, Der NSA-Komplex, 2014.

171 Vgl. dazu S. 39 mit Fn. 133.

die Datenschutzbehörden zu einer unionsweiten Koordinierung. Verantwortliche, die nicht in der Union niedergelassen sind und Auftragsverarbeiter müssen einen Vertreter bestellen (Art. 27 Abs. 1 DSGVO). Die Union will damit einem befürchteten digitalen Imperialismus der Internetgiganten aus dem Silicon Valley die Stirn bieten. Kombiniert mit dem Wechsel zur Handlungsform der Verordnung geht damit eine – im Verhältnis zum bisherigen Richtlinien-Regime – deutlich sichtbare Harmonisierung und Stärkung des Datenschutzrechts einher. In der Sache ist die DSGVO allerdings in Teilen eher eine Richtlinie im Verordnungsgewand und damit ein Hybrid zwischen beiden Handlungsformen:[172] Mit rund vier Dutzend Öffnungsklauseln erlaubt sie den Mitgliedstaaten in substanziellem Umfang, insbesondere im öffentlichen Sektor, eigene Akzente zu setzen.

Die Novellierung des unionalen Datenschutzrechts konfrontiert den nationalen Gesetzgeber mit der Frage, welcher Regelungsspielraum ihm unter den Vorgaben der DSGVO noch verbleibt. Was darf er in einem neuen BDSG aufrechterhalten, was muss er streichen? Aufgrund der kurzen Frist bis zum Inkrafttreten der DSGVO sowie des baldigen Endes der Legislaturperiode des 18. Deutschen Bundestags findet das nationale Gesetzgebungsverfahren unter enormem Zeitdruck statt.[173]

---

172 In diesem Sinne *Kühling/Martini* (Fn. 132), 449; dazu auch umfassend *Kühling/Martini/Heberlein et al.* (Fn. 151), S. 1 ff.

173 Mit der Auslotung des Regelungsspielraums, der den Nationalstaaten unter dem Regime der DSGVO zukommt, hat Programmbereichsleiter Prof. Dr. Mario Martini gemeinsam mit seinem Regensburger Kollegen Prof. Dr. Jürgen Kühling, LL.M. und mit Unterstützung der Forschungsreferenten des Programmbereichs bereits Anfang 2016 begonnen. In enger Kooperation mit dem BMI entstand im inhaltlichen Kontext des Forschungsprojekts ein Gutachten im Umfang von 530 Seiten: *Kühling/Martini/Heberlein et al.* (Fn. 151). Das Werk versteht sich als Handlungsleitfaden und Grundlage für den nationalen Gesetzgebungsprozess. Es wirft einen vertiefenden Blick auf die Öffnungsklauseln der DSGVO, den damit verbundenen Regelungsauftrag an den deutschen Gesetzgeber sowie die Stellung und Kooperationsmöglichkeiten der datenschutzrechtlichen Aufsichtsbehörden. Zu Öffnungsklauseln siehe auch *Benecke/Wagner*, DVBl. 2016, 600 ff.; zum Geltungsbereich nationaler Regeln *Laue*, ZD 2016, 463 ff.

5. *Das Once-only-Principle als datenschutzkonforme Strategie eines ebenenübergreifenden E-Governments?*

Das Once-Only-Principle als datenschutzkonforme Strategie eines ebenenübergreifenden E-Governments? **(Martini/Nink/Weinzierl)**	
Projektinhalt	Das Forschungsprojekt beleuchtet das Once-Only-Principle der unionalen E-Government-Strategie aus datenschutzrechtlicher Sicht.
Forschungsziele	Vorschläge zur datenschutzkonformen Realisierung des Once-Only-Principle im Lichte des Zweckbindungsgrundsatzes der DSGVO.

Besondere Herausforderungen für die Datenverarbeitung des öffentlichen Sektors bergen die Vorgaben der DSGVO im Hinblick auf das Bemühen, Leistungsangebote der öffentlichen Verwaltung mithilfe des Once-only-Principles zu vereinfachen. Das Prinzip ist Teil der E-Government-Strategie der Europäischen Union.[174] Es bezeichnet den Ansatz, Bürger nur *einmal* zur Eingabe bestimmter Daten bzw. zur Übermittlung von Dokumenten oder Zertifikaten aufzufordern – anstatt bei jedem neuen Verfahren dieselben Angaben und Nachweise erneut abzufragen.[175] Sind für einen neuen Verwaltungsvorgang bei einer anderen Behörde innerhalb der EU bereits Stamm- und Registerdaten vorhanden, sollen die Felder der Formulare automatisch vorausgefüllt werden (sog. pre-filling). Damit zielt die Union auf effizientere digitale Angebote und den Abbau bürokratischer Hürden im E-Government, insbesondere in der Interaktion zwischen Behörden. Im Jahr 2017 startet die Kommission zunächst eine Pilotinitiative mit interessierten Mitgliedstaaten, welche auf die Definition einer interoperablen Lösung abzielt, über die sich die Verwaltungen der Mitgliedstaaten in bestimmten KMU-bezogenen

174 Europäische Kommission (Fn. 15), S. 7.

175 Vgl. Europäische Kommission, Workshop on new eGovernment Action Plan: Workshop report, 2015. Das Vorbild für das binnenmarktweite Once-only-Principle lieferte Estland, das bereits Ende der 1990er Jahre ein solches für seine Verwaltung verabschiedete (vgl. OECD, Estonia and Finland: Forstering strategic capacity across governments and digital services across borders, 2015, S. 204).

Service-Bereichen vernetzen und gemeinsame Basis-Register nutzen können.[176]

Dass das Once-only-Principle – sofern (wie typischerweise) personenbezogene Daten betroffen sind – in einem Spannungsverhältnis zu dem datenschutzrechtlichen Zweckbindungsgrundsatz (Art. 5 Abs. 1 lit. b DSGVO) und den Prinzipien der Datensparsamkeit bzw. -minimierung (Art. 5 Abs. 1 lit. c DSGVO) und Transparenz (Art. 5 Abs. 1 lit. a Var. 3 DSGVO) steht und wie dieses Spannungsverhältnis regulatorisch aufzulösen ist, wird bisher nicht erkennbar problematisiert. Diese Analyse macht sich der Programmbereich zur Aufgabe.

6. Regelungsbedarf und rechtliche Grenzen elektronischer vollautomatisierter Verwaltungsverfahren

Regelungsbedarf und rechtliche Grenzen elektronischer vollautomatisierter Verwaltungsverfahren **(Ziekow/Braun Binder)**	
Projektinhalt	Das Forschungsprojekt „vollautomatisierte Verwaltungsverfahren“ untersucht (ausgehend von Modernisierungsvorschlägen des Bundesministeriums der Finanzen [BMF]), ob die Ansätze vollautomatisierter Verwaltungsverfahren in der Steuerverwaltung auf andere Massenverfahren übertragbar sind und ob sie über Massenverfahren hinaus für weitere Verwaltungsverfahren von Nutzen sein können. Besonders im Fokus stehen: • Notwendigkeit, rechtliche Grenzen und Kontrolle von Risikomanagementsystemen, • Zulässigkeit von Abweichungen vom Untersuchungsgrundsatz, • Schutz der Verfahrensrechte Betroffener, • Elektronische Bekanntgabe von Verwaltungsakten über Behördenportale.
Forschungsziele	Analyse des verwaltungsverfahrensrechtlichen Anpassungsbedarfs und der verfassungsrechtlichen Grenzen mit Blick auf die Einführung vollautomatisierter Verwaltungsverfahren.

176 Vgl. Europäische Kommission, Digital Single Market Strategy – Questions and answers, 2015, S. 8. Nach Auskunft der EU soll die Unterzeichnung der entsprechenden Finanzhilfevereinbarung Ende 2016 erfolgen, sodass im Idealfall die inhaltliche Arbeit zu Beginn des Jahres 2017 beginnen kann.

Zum 1. Januar 2017 tritt das Gesetz zur Modernisierung des Besteuerungsverfahrens in seinen wesentlichen Teilen in Kraft. Es verankert u. a. die Möglichkeit, vollautomatisierte Steuerbescheide zu erlassen in der Abgabenordnung (AO). Im Laufe des Gesetzgebungsverfahrens hat das Parlament die parallele Anpassung des Verwaltungsverfahrensgesetzes des Bundes (VwVfG) und des Zehnten Buchs Sozialgesetzbuch (SGB X) beschlossen. Die Änderungen zielen darauf, die Möglichkeit eines vollautomatisierten Erlasses von Verwaltungsakten in alle drei Säulen des Verwaltungsverfahrensrechts zu implementieren und sie damit weitgehend einheitlich fortzuentwickeln. Dazu gehört auch die fortan in allen drei Verfahrensordnungen vorgesehene Möglichkeit der Bekanntgabe elektronischer Verwaltungsakte über Behördenportale.

Inwieweit sich die ursprüngliche Vorlage, die allein als Änderung der AO geplant war, als Blaupause für eine eventuelle Anpassung des VwVfG heranziehen lässt bzw. in welchen Punkten für das Verwaltungsverfahren eigenständige rechtliche Lösungen zu entwickeln sind, harrt einer Klärung.[177] Aus den bei der Analyse dieser Forschungsfrage gewonnenen Erkenntnissen lassen sich Vorschläge für die rechtliche Gestaltung vollautomatisierter Verwaltungsverfahren auf der Grundlage des VwVfG entwickeln; damit verknüpfen sich zahlreiche verwaltungsverfahrensrechtliche Fragestellungen:

1. *Welche Typen von Verwaltungsverfahren* eignen sich zur ausschließlich automationsgestützten Durchführung und unter welchen Voraussetzungen darf die zuständige Behörde sie durchführen?
2. Ist mit Blick auf die Sicherung der gesetzmäßigen und gleichmäßigen Anwendung des materiellen Rechts der Einsatz von *Risikomanagementsystemen* bzw. von anderweitigen *Kontrollsystemen* erforderlich? Welche rechtlichen Grenzen sind dem Einsatz von automatisierten Risikomanagement- und/oder Kontrollsystemen gesetzt?
3. Inwieweit sind Abweichungen vom verwaltungsverfahrensrechtlichen *Untersuchungsgrundsatz* zulässig?
4. Wie steht es um den Schutz der *Verfahrensrechte* Betroffener?

177 Zwischenergebnisse der ersten Projektphase hat der Programmbereich bereits veröffentlicht: *Braun Binder*, NVwZ 2016, 342 ff.; *dies.*, NVwZ 2016, 960; *dies.*, Jusletter IT vom 25.5.2016, 1 ff. Zwischenergebnisse der zweiten Phase sind *Braun Binder*, DÖV 2016, 891 ff.; *dies.*, DStZ 2016, 526 ff.; *dies.*, Jusletter IT vom 22.9.2016, 1 ff.

5. Welche Änderungen sind mit Blick auf die *elektronische Bekanntgabe* von Verwaltungsakten durch Bereitstellung zum Datenabruf notwendig?

III. Digitale Sicherheitsarchitektur

Sicherheitsbehörden bewegen sich im Internet oft in einer rechtlichen Grauzone. Vielfach ist ihr digitaler Handlungsradius nicht hinreichend rechtsklar markiert. Die normativen Vorgaben einerseits und die Bedürfnisse der Praxis anderseits sind dabei, insbesondere auch aus Sicht der Kriminalwissenschaften, häufig nicht deckungsgleich. Daraus erwächst ein Spannungsverhältnis. Dessen Implikationen zu ermitteln und aufzulösen, ist Aufgabe normativer Analyse und rechtspolitischen Ausgleichs.

Sicherheit im Internet heißt nicht nur Rechtssicherheit für Behörden und Bürger. Staatliche Aufgabe ist es auch, funktionsfähige und integre Informations- und Kommunikationsnetze bereitzustellen und eine vertrauliche individuelle Kommunikation zu gewährleisten. Dem Staat als rahmensetzender Ordnungsmacht kommt hierbei eine Infrastrukturverantwortung zu.[178]

178 Zu diesem Topos allgemein und grundlegend *Hermes*, Staatliche Infrastrukturverantwortung, 1998.

1. Ein digitales Ordnungsrecht

Ein digitales Ordnungsrecht (Martini/Kolain/Nink)	
Projekt-inhalt	Die normative Ausgestaltung digitaler Ermittlungs- und Gefahrenabwehrmaßnahmen durch Ordnungsbehörden stellt den Gesetzgeber vor Herausforderungen. Zu ihnen gehören • spezifisch digitale polizeiliche Standardmaßnahmen, • technische Innovationspotenziale in der Ermittlungsarbeit und • digitale Datensteuerung an Verkehrsknotenpunkten.
For-schungs-ziele	Rechtliche Einordnung und Bewertung neuer digitaler Instrumente zur Gefahrenabwehr; konkrete Normierungsvorschläge für digitale Standardmaßnahmen; praxisgerechter, rechtmäßiger Einsatz innovativer Ermittlungsmaßnahmen wie etwa Bodycams, Drohnen, Predictive Policing, Netzwerkforensik, Targeted Profiling; Datensteuerung an Verkehrsknotenpunkten und bei der Grenzkontrolle.

Je stärker die Welle der Digitalisierung die Arbeits- und Alltagswelt flutet, desto weniger bilden auf analoge Vorgänge ausgerichtete Normen einen validen Anker für die Abwehr im Internet lauernder Gefahren für die öffentliche Sicherheit und Ordnung. Das allgemeine und das besondere Ordnungsrecht tun sich bislang schwer damit, digitale Fahndungs- und Ermittlungsmaßnahmen in ihrer Normstruktur zu verorten. Die Rechtspraxis behilft sich bisweilen (notgedrungen) mit Analogien oder Erst-recht-Schlüssen zu Befugnissen, die in der analogen Welt entstanden und auf sie zugeschnitten sind. Der Rechtsprechung kommt dadurch vermehrt eine Deutungshoheit zu, die sie von ihrer originären Aufgabe der Rechtserkenntnis entfremdet und eine Spannungslage zu dem verfassungsrechtlichen Bestimmtheitsgebot aufbaut.

An der Schwelle zum „Internet der Dinge“[179], in Zeiten ubiquitärer Massendatenauswertung und mit Blick auf überbordende Datenmengen in den Händen international agierender Internetkonzernen ist die Arbeit

179 Siehe oben Fn. 2 und 140.

der Ordnungsbehörden auf normenklare, verfassungsrechtlich abgesicherte Grundlagen angewiesen. Innovative Ermittlungsansätze wie das Predictive Policing[180], der Einsatz unbemannter Luftfahrzeuge (engl. unmanned aerial vehicle, UAV) bzw. Drohnen[181] sowie der Netzwerkforensik[182] oder des Targeted Profiling[183] werfen nicht nur Fragen nach ihrer Vereinbarkeit mit den Wertentscheidungen der Verfassung auf, sondern fordern auch Antworten darauf, inwieweit bestehende polizeirechtliche Standardmaßnahmen auf digitale Ermittlungsmethoden anwendbar sind.

Den konkreten Forschungsbedarf illustriert das neue Eigensicherungsinstrument „Bodycam" beispielhaft: Im Wege von Pilotprojekten haben die Miniatur-Kameras auf der Schulter von Polizisten in mehreren Bundesländern[184] sowie bei der Bundespolizei ihren Weg auf deutsche Straßen gefunden. Polizeibeamte tragen sie offen an der Polizeiuniform und aktivieren sie temporär in Gefahrensituationen – mit dem Ziel, Gewalt gegen Einsatzkräfte zu vermeiden und die Beweiserhebung zu vereinfachen.

Bodycams der Polizei lösen ein Spannungsverhältnis zwischen dem Schutz der körperlichen Unversehrtheit der Beamten[185] und dem Persönlichkeitsrecht der Aufgezeichneten aus. Ihr praktischer Einsatz ist

---

180 Dazu bspw. *Legnaro/Kretschmann*, Krim. Journal 2015, 94 ff.; *Meinecke*, Big Data und Data Mining: Automatisierte Strafverfolgung als neue Wunderwaffe der Verbrechensbekämpfung?, in: Taeger (Hrsg.), Big Data & Co, 2014, S. 183 ff.

181 Dazu mit Blick auf Drohnen im Einsatz internationaler Kriegsführung *Städele*, Völkerrechtliche Implikationen des Einsatzes bewaffneter Drohnen, 2014; zum Drohneneinsatz bei Versammlungen i. S. d. Art. 8 GG *Roggan*, NVwZ 2011, 590 ff.

182 Dazu *Frantzen*, Einsatz der Netzwerkforensik für Ermittlungsbehörden, 2013.

183 Vgl. etwa *Turvey*, Criminal profiling, 4. Aufl., 2012.

184 Vorreiter war das Land Hessen, das die Bodycams – gestützt auf § 14 Abs. 6 HSOG – nunmehr dauerhaft im Rahmen von Polizeistreifen einsetzt. Ausführlich zu Bodycams *Kipker/Gärtner*, NJW 2015, 296 ff.; *Martini/Nink/Wenzel*, NVwZ-2016, 1772 f. sowie NVwZ-Extra 24/2016, 1 ff.; *Parma*, DÖV 2016, 809 ff.

185 Der Eigensicherungsaspekt ist nicht zwingend die einzige, aber wichtigste Triebfeder für den Bodycam-Einsatz und entsprechende Gesetzesinitiativen.

durch rechtliche, organisatorische und technische Maßnahmen zu flankieren, die den Aspekten „Datenschutz“, „Transparenz“ und „effektiver Rechtsschutz“ eine zentrale Rolle zumessen. Der gesetzgeberische Konkretisierungsbedarf betrifft dabei nicht nur das „Ob“ des Einsatzes,[186] sondern insbesondere auch das „Wie“: Von der Ausgestaltung der konkreten Voraussetzungen für die Erhebung, Verwendung, Auswertung und Löschung der Video- und ggf. auch Tonaufnahmen hängt es ab, welches Ziel Bodycams effektiv fördern und ob ihr Einsatz dem Grundsatz der Verhältnismäßigkeit entspricht.[187]

Im Gefolge der zunehmenden Digitalisierung der Grenzkontrollen, der Abläufe an Flughäfen und des Bahnverkehrs stellt sich auch für die Bundespolizei die Frage, inwiefern sie ihre Aufgabenerledigung durch eine effektive Datensteuerung und -kontrolle optimieren kann. Der Rechtsrahmen ist bislang unscharf konturiert. Noch nicht erforscht ist insbesondere die Frage, wie die kollidierenden Interessen – auch organisatorisch – mit einem modernen Datenschutz und hohen IT-Sicherheitsstandards in Einklang zu bringen sind.

Vgl. zum Begriff der Eigensicherung auch *Ziems*, Videoüberwachung bei Anhalte- und Kontrollvorgängen zur Eigensicherung der Polizeibeamten, 2006, S. 68 f.

186 Dazu gehört auch die Frage, ob sich der Bodycam-Einsatz in einem Pilotprojekt auf bestehende Ermächtigungsgrundlagen (z. B. die jeweilige landesrechtliche Datenerhebungs-Generalklausel) stützen lässt, oder es aufgrund der möglicherweise erhöhten Grundrechtsrelevanz einer eigenständigen, passgenauen Ermächtigungsgrundlage bedarf. Dazu im Einzelnen *Martini/Nink/Wenzel* (Fn. 184), 7 f.

187 Konkrete Vorschläge für eine verfassungskonforme Nutzung geben auch *Kipker/Gärtner* (Fn. 184), 297 ff.

2. Schutzmechanismen der digitalen Kommunikation

Schutzmechanismen der digitalen Kommunikation (Martini/Sorge/Kolain)	
Projekt-inhalt	Digitales Identitätsmanagement; sicherer und datenschutzkonformer Zugang zu Internetleistungen, insbesondere E-Government-Diensten.
For-schungs-ziele	Entwicklung rechtlicher Standards für ein nutzerzentriertes, ebenen- und ressortübergreifendes digitales Identitätsmanagement für natürliche und juristische Personen (insbesondere im Hinblick auf die eIDAS-VO[188] und ihre Auswirkungen auf das nationale Recht); Handlungsstrategien der öffentlichen Verwaltung für Anreize, digitale Identitäten (z. B. die eID-Funktion des neuen Personalausweises oder De-Mail) flächendeckend zu nutzen, sowie für die Fortentwicklung der regulatorischen Rahmenbedingungen; Analyse der rechtlichen und organisatorischen Rahmenbedingungen eines digitalen Identitätsmanagements für Objekte im „Internet der Dinge“.

Im Behördenalltag ist die Vorlage eines Lichtbildausweises und die eigenhändige Unterschrift von Dokumenten noch der Standardfall sicherer Authentifikation im Verwaltungsverfahren. Soll der *Homo digitalis* auch via Internet Leistungsangebote der öffentlichen Verwaltung in Anspruch nehmen, etwa ein Kfz-Kennzeichen beantragen können,[189] bedarf es neben technischer Infrastruktur insbesondere auch Regelungen, Standards und Umsetzungsstrategien für deren sicheren und effektiven Praxiseinsatz.

188 Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. Nr. L 257, S. 73, ber. ABl. 2015 Nr. L 23, S. 19 und ABl. 2016 Nr. L 155, S. 44.

189 Zu den rechtlichen Grenzen BVerfGE 123, 39 ff.; *Buchmann/Roßnagel*, K&R 2009, 543 ff.; *Henning/Volkamer/Budurushi*, DÖV 2012, 789 ff.; *Luch/Schulz/Tischer*, BayVBl 2015, 253 ff.; *Will*, NVwZ 2009, 700 ff.

a) Vertrauen in die technische Infrastruktur als Schlüsselelement digitaler Entwicklungsperspektiven

Einen digitalen Zugangskanal zur öffentlichen Verwaltung zu legen und den Bürgern zur Nutzung freizugeben, ist nicht nur eine technologische und organisatorische Herausforderung. E-Government funktioniert nicht ohne begründetes Vertrauen in die technische Infrastruktur. Der Staat ist dazu aufgerufen, einen ausreichenden Schutz der individuellen Kommunikation zu gewährleisten. Ziel ist ein hoher Grad an Vertraulichkeit und Integrität.

Rund 70 % der Menschen in Deutschland sehen den Staat in der Pflicht, aktiv für Sicherheit zu sorgen.[190] Gerade die (idealtypische) Gruppe der sog. „effizienzorientierten Performer" – ein leistungsorientierter Teil der Bevölkerung mit einem Altersdurchschnitt von 38 Jahren und einem formal durchschnittlichen Bildungsniveau – misst dem Staat eine hohe Schutzverantwortung zu.[191] Ähnliches gilt für die sog. „verantwortungsbedachten Etablierten", die über ein formal hohes Bildungsniveau verfügen und einen Altersdurchschnitt von 52 Jahren aufweisen.[192]

Das erhoffte Vertrauen kommt der Bevölkerung aber zusehends abhanden: 66 % der Deutschen trauen dem Staat nicht mehr zu, aktiv Sicherheit im Internet herzustellen.[193] Der Cyberangriff auf den Deutschen Bundestag, der dessen elektronische Infrastruktur zeitweise in einen Lähmungszustand versetzte, war für viele Bürger insoweit ein Fanal: Wenn der Staat es nicht schafft, seine eigenen politischen Herzkammern zu schützen, dann – so eine verbreitete Einschätzung – sei es ihm auch nicht mehr zuzutrauen, die digitalen Infrastrukturen der Bürger hinreichend zu verteidigen. Besonders ausgeprägt ist das Misstrauen in die Sicherheitsgewährleistungskompetenz des Staates bei Menschen, welche die technische Komplexität des Internets schnell überfordert, insbesondere bei älteren Personen sowie bei Personen mit formal unterdurchschnittlicher Bildung, die das Internet kaum oder gar

---

190 Deutsches Institut für Vertrauen und Sicherheit im Internet (Fn. 5), S. 86.

191 Deutsches Institut für Vertrauen und Sicherheit im Internet (Fn. 5), S. 47, 85.

192 Deutsches Institut für Vertrauen und Sicherheit im Internet (Fn. 5), S. 59, 85.

193 Deutsches Institut für Vertrauen und Sicherheit im Internet (Fn. 5), S. 86 f.

nicht nutzen (sog. „vorsichtige Skeptiker“ und „internetferne Verunsicherte“).[194]

b) Digitales Identitätsmanagement

Ein nutzerzentriertes, ebenen- und ressortübergreifendes digitales Identitätsmanagement ist insbesondere auf vertrauenswürdige Identitäten angewiesen.[195] Die eID-Funktion des neuen Personalausweises (nPA) hat den ersten Schritt zu einer rechtssicheren digitalen Identität bereits vollzogen.[196] Die eIDAS-VO der Europäischen Union hat seit dem 1.7.2016 einen einheitlichen Rechtsrahmen für elektronische Sicherheitsdienste geschaffen.[197] Die Vorschriften der Verordnung gelten un-

---

194 Deutsches Institut für Vertrauen und Sicherheit im Internet (Fn. 5), S. 65, 71, 85.

195 Vgl. hierzu aus Sicht der Trendforschung *Fromm/Welzel/Hoepner et al.*, Vertrauenswürdige digitale Identität: Baustein für öffentliche IT, 2013.

196 Vgl. das zum November 2010 in Kraft getretene Gesetz über Personalausweise und den elektronischen Identitätsnachweise sowie zur Änderung weiterer Vorschriften vom 18. Juni 2009 (BGBl. I S. 1346).

197 In ihrem Art. 6 fordert die eIDAS-VO eine gegenseitige Anerkennung elektronischer Identifizierungssysteme der Mitgliedstaaten. Neben digitalen Identifizierungsdiensten regelt sie Vertrauensdienste. Die Verordnung novelliert bzw. ersetzt insoweit die Signaturrichtlinie von 1999 (Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. 2000 Nr. L 13, S. 12). Ihr Regelungsumfang beinhaltet insbesondere:

- elektronische Signaturen, Siegel, Zeitstempel und Einschreib-Zustellungsdienste (insbesondere auch neue Signatur-Standards – m460, CEN – ETSI),
- Dienste zur Website-Authentifizierung (insb. SSL-Dienste) und
- die Verwahrung von elektronischen Signaturen, Siegeln und Zertifikaten.

Die praktische Umsetzung der vorgeschlagenen Maßnahmen bringt weitreichende Änderungen für die öffentliche Verwaltung mit sich. Bei vollständiger Umsetzung wäre ein digitales Äquivalent zur eigenhändigen Unterschrift von Dokumenten gefunden (vgl. auch Art. 25 II eIDAS VO). Der Rechtsverkehr mit Einschreiben, der Zugang zur Justiz und zahlreiche, persönlichkeitssensible E-Government-Dienste hätten den Schritt in die digitale Welt endgültig vollzogen.

mittelbar, belassen den Mitgliedstaaten aufgrund ihrer inhaltlichen Offenheit und ihrer zahlreichen Implementierungsermächtigungen jedoch viele Interpretations- und Anwendungsspielräume.[198] Die Auswirkungen auf die deutsche Rechtsordnung, insbesondere die verbleibenden nationalen Ausgestaltungsspielräume, und die Gestaltungsoptionen der Europäischen Kommission sind noch nicht umfassend wissenschaftlich ausgeleuchtet.

Das Themenfeld „digitale Identitäten" ist nicht nur für natürliche und juristische Personen von Belang, sondern auch ein zentraler Erfolgsfaktor für das „Internet der Dinge". Jedes der dort vernetzten Objekte besitzt eine eigene Identität und muss zuverlässig sowie möglichst datensparsam ansteuerbar und kommunikationsfähig sein. Eine regulatorische Herausforderung liegt insbesondere in der Definition übergreifender Standards sowie vergleichbarer Vertrauensniveaus und Sicherheitsstufen.[199] Daran mitzuwirken, macht sich das Forschungsprojekt durch interdisziplinäre Grundlagenforschung zur Aufgabe.[200]

IV. Öffentlich-private Kooperationsfelder im digitalen Raum

Digitale Technologien verzahnen staatliche und private Akteure in einer immer größeren Zahl und Vielfalt digitaler Kooperations-, Kollaborations- und Koproduktionsprozesse. Das Zusammenspiel der öffentlichen Verwaltung mit der Wirtschaft unterliegt infolgedessen einem radikalen Wandel, der ebenso neue Chancen wie Herausforderungen mit sich bringt.

Das Handelsregister, das Grundbuch sowie die Signatur als Schriftformersatz nimmt die eIDAS-VO zwar ausdrücklich aus (zudem die rein verwaltungsinterne Verwendung von Vertrauensdiensten). Die einschlägigen nationalen Regelungen (insbesondere das SigG und die SigV) bedürfen jedoch in gleicher Weise einer Anpassung an die Erfordernisse digitalen Rechtsverkehrs. Zu dem Ergebnis eines Normscreenings der Bundesregierung s. Bundesministerium des Innern, Bericht der Bundesregierung zur Verzichtbarkeit der Anordnungen der Schriftform und des persönlichen Erscheinens im Verwaltungsrecht des Bundes, 2016.

198 Vgl. hierzu *Roßnagel*, MMR 2015, 359 ff.; *Jandt*, NJW 2015, 1205 ff.; *Sosna*, CR 2014, 825 ff.

199 *Fromm/Welzel/Hoepner et al.* (Fn. 195), S. 15.

200 Das Projekt weist Schnittmengen mit „Smart Cities' Government: staatliche Infrastrukturaufgaben in der digitalen Welt" (C.II.2, S. 47 ff.) und „Mitgliedstaatliche Regelungsspielräume unter der Datenschutz-Grundverordnung " (C.II.4, S. 53 ff.) auf.

1. *Kooperative eingebettete Systeme: Vernetzung der öffentlichen Verwaltung mit intelligenten Industrie 4.0-Umgebungen*

Kooperative eingebettete Systeme: Vernetzung der öffentlichen Verwaltung mit intelligenten Industrie 4.0-Umgebungen **(Martini/Nink/Wagner/Weinzierl)**	
Projekt-inhalt	Wie ein kooperativer Kontrollansatz für eingebettete Systeme und intelligente Umgebungen aussehen kann, gehört zu den zentralen Herausforderungen von Industrie 4.0-Umgebungen. Ihrer Erforschung widmet sich das Projekt „Kooperative eingebetete Systeme“. Im Fokus steht die Gewährleistungsfunktion der öffentlichen Hand für eine sichere und wirksame Infrastruktur sowie eine staatliche Teilhabe an den Daten im öffentlichen Interesse.
Forschungs-ziele	Das Projekt analysiert die Herausforderungen für die Konfiguration und rechtliche Ausgestaltung von Schnittstellen der Industrie 4.0 mit der öffentlichen Verwaltung (etwa in den Bereichen Arbeitsschutz, Datenschutz, Anlagensicherheit, Störvorsorge) und korrespondierende E-Government-Leistungen für Unternehmen.

Immer dann, wenn ein Akteur Hardware- und Softwarekomponenten in ein umfassenderes Produkt einbindet, um produktspezifische Funktionsmerkmale zu realisieren, handelt es sich um „eingebettete Systeme“[201]. Definierte Schnittstellen und Protokolle ermöglichen ihnen die Interaktion mit der Außenwelt. Ein plastisches Beispiel liefert die Logistik: Nicht nur Fahrer und Unternehmen sind über Navigationssysteme und Smartphones miteinander vernetzt („Internet der Dienste“), sondern zunehmend auch Fahrzeuge und Lieferungen („Internet der Dinge“).[202] Beide Ebenen verschmelzen zu einer intelligenten Logisti-

---

201 Im Englischen spricht man von „Embedded Systems“, dazu bspw. *Bakos*, Embedded systems, 2016; *Berns/Bernd/Trapp*, Eingebettete Systeme, 2010; *Halang/Holleczek*, Eingebettete Systeme, 2011; *Teich/Haubelt*, Digitale Hardware/Software-Systeme, 2. Aufl., 2007.

202 Vgl. hierzu bereits Fn. 2 sowie *Brand/Hülser/Grimm et al.*, Internet der Dinge – Perspektive für die Logistik, 2015; Bundesministerium für Wirtschaft und Energie, Zukunft der Arbeit in der Industrie 4.0, 2014, S. 28 ff.; *Martini* (Fn. 114), S. 15 ff.; *Schöpker*, Fracht und Trailer immer in Echtzeit – volle Transparenz in der Supply Chain, in: Voß (Hrsg.), Logistik – eine Industrie, die (sich) bewegt, 2015, S. 55 ff.; *Stich/Adema/Blum*, Supply Chain 4.0: Logistikdienstleister im Kontext der vierten industriellen Revolution, in:

kumgebung, die Daten zu Positionskoordinaten und Wetterbedingungen, zum Zustand der Waren und des Fahrzeugs bzw. zur Auslastung des Fahrers austauscht und auf dieser Basis das Transportwesen koordiniert sowie optimiert.

Auch smarte Fabriken der Zukunft[203] werden viele Prozesse in Echtzeit über eingebettete vernetzte Systeme steuern und koordinieren. Auf der Grundlage aktuellster Prozessdaten können Unternehmen die miteinander verknüpften Wertschöpfungsketten und Verfahrensebenen aufeinander abstimmen. Der bedarfsgesteuerte Einsatz anwendungsoffen konstruierter Maschinen lässt sich dabei weitestgehend automatisiert organisieren. Werkstücke können künftig mittels eingebetteter Systeme Umgebungsdaten verarbeiten und daraus Steuerungsbefehle ableiten. Neben diese vertikale Integration tritt in der Industrie 4.0 auch die horizontale Vernetzung zwischen mehreren Unternehmen: Sie ist Ausgangspunkt flexibel gestaltbarer gemeinsamer Wertschöpfungsprozesse.[204]

Voß (Hrsg.), Logistik – eine Industrie, die (sich) bewegt, 2015, S. 63 ff.; *Wulf/Burgenmeister*, CR 2015, 404 ff.

203 *Anderl/Anokhin/Arndt*, Effiziente Fabrik 4.0 Darmstadt – Industrie 4.0 Implementierung für die mittelständige Industrie, in: Sendler (Hrsg.), Industrie 4.0 grenzenlos, 2016, S. 121 ff.; *Bauernhansl*, Die Vierte Industrielle Revolution – Der Weg in ein wertschaffendes Produktionsparadigma, in: Bauernhansl/Hompel/Vogel-Heuser (Hrsg.), Industrie 4.0 in Produktion, Automatisierung und Logistik, 2014, S. 5 ff.; *Landherr/Neumann/Volkmann et al.*, Digitale Fabrik, in: Westkämper/Spath/Constantinescu et al. (Hrsg.), Digitale Produktion, 2013, S. 107 ff.; *Lucke*, Smart Factory, in: Westkämper/Spath/Constantinescu et al. (Hrsg.), Digitale Produktion, 2013, S. 251 ff.; *Martini* (Fn. 114), S. 16 ff.; *Schlick/Stephan/Loskyll et al.*, Industrie 4.0 in der praktischen Anwendung, in: Bauernhansl/Hompel/Vogel-Heuser (Hrsg.), Industrie 4.0 in Produktion, Automatisierung und Logistik, 2014, S. 57 ff.; *Stark/Damerau/Lindow*, Industrie 4.0 – Digitale Neugestaltung der Produktentstehung und Produktion am Standort Berlin, in: Sendler (Hrsg.), Industrie 4.0 grenzenlos, 2016, S. 169 ff.

204 *Bauernhansl* (Fn. 203), S. 5 ff.; *Eckert*, DuD 2015, 641 ff.; *Eigner*, Das Industrial Internet, in: Sendler (Hrsg.), Industrie 4.0 grenzenlos, 2016, S. 137 ff.; *Kagermann/Wahlster/Helbig*, Deutschlands Zukunft als Produktionsstandort sichern, 2013; *Koch/Kuge/Geissbauer et al.*, Industrie 4.0, 2014; *Sendler*, Die Grundlagen, in: ders. (Hrsg.), Industrie 4.0 grenzenlos, 2016, S. 17 ff.

In beiden Beispielszenarien verbindet im Idealfall ein sog. „Industrial Data Space“ die einzelnen Interaktionsebenen. Diese Schnittstelle erfüllt einerseits die Aufgabe einer Dolmetscher-Einheit für die reibungsfreie Kommunikation zwischen verschiedenen technischen Instanzen und andererseits die eines Daten-Treuhänders für die sachlich richtige und vertrauenswürdige Zuordnung sensibler Geschäfts- und Personendaten. Die autonom agierenden Systeme stellen dabei gegenläufige Anforderungen an ihr Risikomanagement. Sie sind auf der einen Seite besonders risikoavers, auf der anderen Seite aber auch besonders risikoaffin: Unter ihrem Regime ist weniger die Zuverlässigkeit von Personen entscheidend als vielmehr ihre Zuverlässigkeit als System (Systemstabilität). Sie versprechen maximale Effizienzgewinne, sind aber zugleich nur bedingt kontrollierbar und können sich daher bei internen Steuerungsfehlern/-defiziten auch als ineffizient und gefährlich erweisen. Standards für eine ordnungsgemäße Ausgangsprogrammierung sind die zentrale Weichenstellung zu Beginn des Innovationszyklus.[205]

Für die hoheitliche Aufsicht über und störfallbezogene Intervention in autonome, eingebettete Systeme ist die effektive, sichere und rechtmäßige Vernetzung der öffentlichen Verwaltung mit intelligenten Umgebungen entscheidend. Wie ein kooperativer Kontrollansatz für eingebettete Systeme und intelligente Umgebungen – auch wettbewerbs- und vergaberechtlich[206] – aussehen kann, wirft zahlreiche wissenschaftlich herausfordernde Fragen auf. Da die Ideen und Fragen rund um die Industrie 4.0 im Wesentlichen erst in jüngster Vergangenheit aufgekommen sind, ist der allgemeine Forschungsstand in diesem Themenfeld noch dünn.[207]

---

205 Ist die verwendete Softwareumgebung geistiges Eigentum und damit Betriebsgeheimnis eines IT-Dienstleisters, fehlt nach jetziger Rechtslage die Möglichkeit einer Offenlegung der Algorithmen als Steuerungsinstanzen digitaler Datenströme. Den Fragen staatlicher Algorithmenkontrolle wendet sich das Projekt „Algorithmenkontrolle als Regulierungsaufgabe“ (C.II.1, S. 42 ff.) zu.

206 Vgl. dazu auch die Ansätze bei *Martini/Fritzsche*, VerwArch 104 (2013), 449 ff.

207 Die größten Leistungen hat die Informatik erbracht. Die Rechtswissenschaft beleuchtet bislang vornehmlich die vertrags-, arbeits-, urheber- und datenschutzrechtlichen Aspekte der neuen technischen Möglichkeiten. Siehe beispielsweise *Bräutigam/Klindt* (Fn. 140), S. 1137 ff.; *Günther/Böglmüller*, NZA 2015, 1025 ff.; *Zech*, CR 2015, 137 ff. Aufsichtsrechtliche Fragen sind in vielen Bereiche indes noch nahezu unerforscht.

Angesichts der Schutzbedürftigkeit vernetzter Systeme greift der Gesetzgeber auf dem Feld der Sicherheit kritischer Infrastrukturen in immer kürzeren Regelungsintervallen regulatorisch ein.[208] Auch die DSGVO erweitert in ihren Art. 32–34[209] den Kreis rechtlicher Anforderungen an die Datensicherheit und versucht, dieses wichtige normative Handlungsfeld an die Erfordernisse der digitalen Welt anzupassen. Der Programmbereich stellt sich der Herausforderung, die technische, normative und administrative Entwicklung einer „Industrie 4.0", eines „Internets der Dinge" sowie ihrer Schnittstellen von Beginn an interdisziplinär wissenschaftlich zu begleiten.

2. Datenschutzrechtliche Verantwortungsstrukturen in komplexen Online-Akteursnetzwerken

Datenschutzrechtliche Verantwortungsstrukturen in komplexen Online-Akteursnetzwerken (Martini/Rehorst/Wagner)	
Projekt-inhalt	Haftungs- und Zurechnungsfragen für Rechtsverstöße in bzw. durch Online-Anwendungen, bei denen verschiedene Akteure die Datenverarbeitungsprozesse wahrnehmen, beeinflussen und steuern, werfen komplexe Rechtsfragen auf. Ihnen wendet sich das Forschungsprojekt zu. Es berücksichtigt dabei insbesondere unionsrechtliche Aspekte, etwa • Zurechnungsfragen beim Zusammenspiel von Portalbetreibern und deren Angestellten sowie Dienstleistern, professionellen Portalnutzern, Portalbesuchern und Werbetreibenden, • Regelungen der DSGVO zu „gemeinsam für die Verarbeitung Verantwortlichen" sowie zu Verantwortlichen und Auftragsverarbeitern.

208 Geschehen insbesondere durch das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), vom 17. Juli 2015 (BGBl. I S. 1324), zuletzt geändert durch Art. 5 Abs. 8 G zur Aktualisierung der Strukturreform des Gebührenrechts des Bundes vom 18.7.2016 (BGBl. I S. 1666) – auf europäischer Ebenen durch die NIS-RL, Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. Nr. L 194, S. 1; s. auch *Schallbruch*, CR 2016, 663 ff.; *Voigt/Gehrmann*, ZD 2016, 355 ff.; *Witt/Freudenberg*, CR 2016, 657 ff.

209 Dazu *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO, 2016, Art. 32, 33 und 34, S. 390 ff.

Forschungsziele	Analyse der rechtlichen Anforderungen bei der Einbindung von Drittdiensten (insbesondere in staatliche Online-Angebote via [Social] Plug-ins); Identifikation nationaler Regelungsspielräume für datenschutzrechtliche Verantwortungsstrukturen unter der DSGVO; Vorschläge für die Normierung sachgerechter Verantwortungsstrukturen für das kooperative Zusammenwirken interaktiver Online-Akteursnetzwerke.

Das nationale Datenschutzrecht ordnet das komplexe Zusammenspiel von Diensteanbietern, technischer Infrastrukturebene und Inhalterstellern im Web 2.0 bislang vorwiegend entlang linearer Vertrags-, Nutzungs- und Auftragsbeziehungen. Die Verantwortungssphären sind grundsätzlich voneinander getrennt, hauptverantwortlich ist der Verarbeiter als „Herr der Daten".[210]

Dem arbeitsteiligen Zusammenwirken in sozialen Netzwerken, bei App-Diensten oder auf komplexen Online-Plattformen[211] werden diese datenschutzrechtlichen Verantwortungsstrukturen nur bedingt gerecht. Die Rechtswissenschaft ist aufgerufen, Lösungskonzepte für die Verantwortlichkeit der Akteure in digital vernetzten Räumen[212] zu entwickeln. Klärungsbedürftig ist bspw., ob und ggf. wie rechtliche Konstruktionen wie der Zweckveranlasser, die Verkehrssicherungspflicht oder der Erfüllungsgehilfe auf kooperatives Zusammenwirken im digitalen Raum

210 Dazu ausführlich *Martini/Fritzsche*, NVwZ-Extra 21/2015, 1 (5). Zu „gemeinsam für die Verarbeitung Verantwortlichen" pro futuro *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO, 2016, Art. 26, Rn. 19 ff. Die DSGVO bringt auch und gerade für Auftragsverarbeiter erhebliche Neuerungen mit sich, vgl. etwa *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO, 2016, Art. 28, Rn. 19 ff. und *ders.*, in: Paal/Pauly (Hrsg.), DS-GVO, 2016, Art. 29, Rn. 28 f.; eine neue Verpflichtung etabliert auch Art. 30 Abs. 2 DSGVO, vgl. *ders.*, in: Paal/Pauly (Hrsg.), DS-GVO, 2016, Art. 30, Rn. 20 ff.

211 Vgl. dazu auch jüngst Bundesministerium für Wirtschaft und Energie, Grünbuch Digitale Plattformen, 2016.

212 Interessante Forschungsfragen ergeben sich auch im Hinblick auf die Zurechnung und Haftung in autonomen Systemen, vgl. etwa *Horner/Kaulartz*, CR 2016, 7 ff.; *Reichwald/Pfisterer* (Fn. 140), 208 ff. Zur Blockchain-Technologie und der Beschäftigung des Programmbereichs mit dieser Thematik, s. bereits S. 18 mit Fn. 66.

übertragbar sind.[213] Für die rechtmäßige und sachgerechte Einbindung der Dienste Dritter in das Online-Angebot der öffentlichen Verwaltung erarbeitet das Forschungsprojekt Handlungsempfehlungen.[214] Ziel ist die normativ gesicherte Abgrenzung von (ordnungsrechtlichen) Verantwortungsstrukturen im Internet, insbesondere bei der gemischten Beteiligung von öffentlichen und privaten Stellen sowie bei jeweils unterschiedlichen Mitwirkungsbeiträgen einzelner Akteure. Die Vorgaben und Auslegungsspielräume der DSGVO stellen dafür die Weichen. Im Unterschied zum BDSG kennt sie das Regelungsinstrument einer gesamthänderischen datenschutzrechtlichen Verantwortlichkeit und belässt dem nationalen Gesetzgeber ab Ende Mai 2018 nur noch wenig Regelungsspielraum zur Ausgestaltung der Zurechnungsstrukturen.[215]

V. Digital Public Management

Die digitale Transformation zieht mit den Innovationen, die sie angestoßen hat, nicht nur eine informationstechnische und regulatorische Modernisierung des öffentlichen Sektors nach sich. Sie stellt auch die Organisationsprinzipien und Koordinationsmechanismen der öffentlichen Verwaltung, ja ihr kulturelles Selbstverständnis auf die Probe. Die Entwicklungsdynamik einer digitalen Gesellschaft fordert der Verwaltung insbesondere erhebliche Anpassungsfähigkeit, Flexibilität und Reaktionsgeschwindigkeit ab. Tradierte Informations-, Kommunikations- und

---

213 Für einen Teilbereich von Online-Akteursnetzwerken ist aus dem Programmbereich bereits der Vorschlag einer Auswahlverantwortlichkeit des Betreibers einer sog. Facebook-Fanpage nach § 11 Abs. 2 S. 1 u. 4 BDSG ad maiore ad minus entstanden, die eine Haftung des Diensteanbieters Facebook flankiert (*Martini/Fritzsche* [Fn. 210], 11 ff.). Die Überlegungen haben das BVerwG im sog. Fanpage-Rechtsstreit maßgeblich dazu veranlasst, den Rechtsstreit zur Klärung dem EuGH vorzulegen (BVerwG, EuGH-Vorlage v. 25.2.2016 – 1 C 28/14 –, ZD 2016, 393 [396, Rn. 35]): „Nach dem nationalen Recht kommt insoweit in Betracht, die Auswahl- und Überprüfungspflichten (§ 11 Abs. 2 Satz 1 und 4 BDSG), die der nationale Gesetzgeber in Umsetzung des Art. 17 Abs. 2 RL 95/46/EG bei einer Datenverarbeitung im Auftrag vorgeschrieben hat, entsprechend heranzuziehen (s. *Martini/Fritzsche*, NVwZ-Extra 21/2015, 12)."

214 Siehe hierzu für das Anwendungsfeld der Online-Bürgerbeteiligung *Martini/Fritzsche*, Kompendium Online-Bürgerbeteiligung, 2015, S. 74 ff.

215 Siehe Art. 4 Nr. 7, Art. 26, 27, 28 und 29 DSGVO. S. dazu *Martini*, in: Paal/Pauly (Fn. 209), Art. 26–29.

Entscheidungsroutinen der bürokratisch-legalistischen Verwaltungskultur stoßen an ihre Leistungsgrenzen. Die netzwerkaffine Organisationslogik zahlreicher E-Government-Anwendungen bricht die hierarchisch strukturierte Aufbau- und Ablauforganisation auf und ersetzt sie durch IT-gestützte Kooperations- und Koordinationsansätze sowie ein Denken in Geschäftsprozessen.

Das Anschwellen der Datenflut, die auf die öffentliche Verwaltung einströmt, sowie die Möglichkeiten und Herausforderungen ihrer intelligenten Auswertung und Nutzung lassen immer öfter die Forderung nach einer stärker datenbezogenen, sich von einem Silodenken entfernenden Verwaltungskultur erklingen.[216] Aus ähnlichen Überlegungen speist sich der in den USA zu beobachtende Trend, in den Ministerien die Führungsposition eines Chief Digital Officers (CDO) einzurichten:[217] CDOs obliegt die Erschließung von Datenpotenzialen, die Datenanreicherung durch Zusammenführung fragmentierter Datenbestände oder Hinzufügung externer Informationen (sog. data enrichment), darüber hinaus der Datenschutz, die Sicherung der Datenqualität und – das gilt allerdings vorrangig für den privatwirtschaftlichen Bereich – die Datenmonetarisierung.[218]

Die organisatorische Transformation und der damit verbundene verwaltungskulturelle Wandel einschließlich der veränderten personellen Rollen- und Kompetenzprofile bilden den Ausgangspunkt des vierten Kernthemenbereichs des Programmbereichs: dem „Digital Public Management“.

---

216 Vgl. etwa OECD Public Governance and Territorial Development Directorate (Fn. 95); *Lutes*, Data-driven government: Challenges and a path forward. IBM-Analytics White Paper, 2015, S. 7. Das IBM-Whitepaper versteht unter einer datenbezogenen Verwaltung (*data-driven government*) eine Verwaltung, die für kritische Entscheidungen bei Bedarf jederzeit auf relevante, anwendungstauglich aufbereitete Informationen zugreifen kann (a. a. O., S. 3).

217 Dazu *Moore*, Rise of the Data Chiefs: Meet the Federal Officials Aiming to Usher in Government's 'Golden Age' of Data, http://www.nextgov.com/big-data/2015/03/rise-data-geeks-meet-federal-officials-aiming-usher-governments-golden-age-data/107736/ (20.11.2016).

218 Vgl. IBM Institute for Business Value, The new hero of big data and analytics – The Chief Data Officer, 2014, S. 4.

1. *Organisationsprinzipien des Mobile Government*

Organisationsprinzipien des Mobile Government (Krcmar)	
Projekt-inhalt	Das Forschungsprojekt „Organisationsprinzipien des Mobile Government“ analysiert die Möglichkeiten der öffentlichen Verwaltung, mobile Dienste im Interesse des Gemeinwohls einzusetzen. Das Projekt erbringt Grundlagenarbeit für mobiles E-Government (Dienste auf mobilen Endgeräten) und analysiert, ob sich Strategien aus dem privaten auf den öffentlichen Sektor übertragen lassen. Darüber hinaus identifiziert es Erfolgsfaktoren für die Verwaltung. Gegenstand des Forschungsprojekts sind insbesondere: • die Analyse inländischer und ausländischer Plattformen des Mobile Government (z. B. GovApps.de); • Location-Based-Services; • Mobile-first-Strategien von Unternehmen und ihre Übertragbarkeit auf die öffentliche Verwaltung.
For-schungs-ziele	Das Projekt vermittelt Erkenntnisse, ob und wann bei Verwaltungsdiensten ein valider Bedarf nach mobilen E-Government-Diensten existiert – und wie diese konkret aussehen sollten. Es erarbeitet Handlungsempfehlungen für die nutzergerechte und rechtskonforme Ausgestaltung mobiler E-Government-Dienste und analysiert die rechtlichen Rahmenbedingungen. Dazu gehören insbesondere • die Identifikation von Erfolgsfaktoren mobiler E-Government-Dienste; • praxistaugliche Handlungsempfehlungen für die Verwaltung; • eine rechtskonforme Implementierung.

In den vergangenen Jahren ist das mobile Internet zum wesentlichen Entwicklungsfeld der digitalen Gesellschaft geworden. „Mobile First“ ist die dominierende Strategie in der digitalen Wirtschaft. Es überrascht daher nicht, dass führende E-Government-Länder über ein umfassendes und zugleich ausdifferenziertes Leistungsangebot des Mobile-Government verfügen.[219] Im Vergleich zu den internationalen Vorreitern gibt es

219 Vgl. etwa *Chen/Vogel/Wang*, Decision Support Systems 2016, S. 47 ff.; *Goyal/Purohit*, SIES Journal of Management 2012, 56 ff.; UN Dept. of Economic & Social Affairs, Journal of E-Governance 2012, 61 f.

in Deutschland nur eine geringe Zahl an mobilen E-Government-Angeboten (insbesondere auf kommunaler Ebene).[220] Die Forschung ist dazu aufgerufen, Ideen für eine erfolgreiche Ausgestaltung mobiler E-Government-Dienste zu entwickeln,[221] ohne dabei die rechtlichen Rahmenbedingungen[222] aus dem Blick zu verlieren. Mobile Government ist ein zwar noch vergleichsweise junges und wenig bearbeitetes, dafür aber für den praktischen Erfolg von E-Government-Dienstleistungen besonders wichtiges Forschungsfeld.

---

220 Vgl. dazu *Wirtz*, Perspektiven des kommunalen E-Government, 2015; *World Economic Forum* (Fn. 4), S. 27. Derzeit nutzen die Bürger mobile Angebote primär, um Informationen einzuholen (z. B. Fahrplanauskünfte oder Öffnungszeiten), artikulieren in Befragungen aber allgemein ein Interesse an dem Ausbau mobiler E-Government-Dienste; nur 18 % der Befragten gaben an, auch zukünftig keine mobilen Online-Angebote nutzen zu wollen, Initiative D21 (Fn. 16), S. 26 f.

221 Voraussetzung für ein Mobile Government ist ein mobiler Zugang zu Verwaltungsangeboten. Im Hinblick auf die Möglichkeit einer Handy-Signatur zur Nutzung der eID des neuen Personalausweises bestehen Schnittmengen mit dem Projekt „Schutzmechanismen der digitalen Kommunikation“ (C.III.2, S. 63 ff.).

222 Dazu instruktiv *Hoffmann*, MMR 2013, 631 ff.

2. IT-Inkubator öffentliche Verwaltung

IT-Inkubator öffentliche Verwaltung – Digital-Service-Teams in der öffentlichen Verwaltung (Mergel)	
Projekt-inhalt	Eine erfolgreiche digitale Transformation schließt grundsätzlich auch organisatorische Ansätze zur Schaffung und Förderung von Start-up-Strukturen ein, die innovative IT-Lösungen für die öffentliche Verwaltung hervorbringen. Dazu gehören insbesondere • innovative Kooperationsformen der Exekutive mit IT-Experten, Start-Up-Akteuren und der Open-Source-Community; • Organisationsprinzipien innovationsaffiner und exzellenter, verwaltungsinterner Beratungseinheiten für die digitale Transformation, z. B. einer Digitalagentur.
Forschungs-ziele	Prozesse und Methoden zur digitalen Transformation in der öffentlichen Verwaltung; Organisationsprinzipien von Digital-Service-Teams; Public-Service-Motivation von Mitgliedern der Digital-Service-Teams; Best-Practice-Empfehlungen zur Etablierung inkubativer Strukturen in der Verwaltung i. S. v. „Verwaltungs-Startups“ für neue E-Government-Leistungen und Innovationslabore; Rechtliche Ausgestaltungsmöglichkeiten, insbesondere zu organisationsrechtlichen Experimentierspielräumen.

Zur Stärkung ihrer Innovationsfähigkeit gründen oder erwerben etablierte Konzerne vermehrt kleine und flexible Einheiten, die sich – herausgelöst aus der bürokratischen Aufbauorganisation der Unternehmen – mit der Entwicklung innovativer Produkte, Dienstleistungen oder auch mit Modernisierungsaufgaben beschäftigen.[223] Sie tragen damit Erkenntnisse der wirtschafts- und sozialwissenschaftlichen Organisations- und Innovationsforschung in die Praxis hinein. Deren Kernbotschaft lautet: Die Emulation von Start-Up-Strukturen innerhalb einer etablierten Organisation bzw. die Kombination der Wissens- und Erfahrungspotenziale großer Unternehmen erzeugt im Zusammenspiel mit der Agilität, Dynamik und den flachen Hierarchien junger Wachstumsunternehmen

223 Ein prominentes deutsches Beispiel ist beispielsweise die Abteilung „Shareground“ der Deutschen Telekom AG.

ein besonderes Klima der Innovation.[224] Ihre Schöpfungskraft setzt Impulse für ein benutzerfreundliches, den gängigen digitalen Lebenswelten angepasstes und damit intuitiv zu bedienendes Design öffentlicher Services. Eine ähnliche Zielrichtung liegt auch dem sog. Open-Innovation-Ansatz[225] zugrunde – er propagiert allerdings weniger eine nach innen gerichtete Integration als eine Öffnung des Innovationsprozesses nach außen.

Bisher adaptiert der öffentliche Sektor in Europa die vorhandenen Ansätze zur Überwindung interner Innovationshemmnisse und zur Stimulierung des organisationseigenen unternehmerischen Denkens nur zögerlich. Eine Vorreiterrolle bei der Überwindung dieses Trägheitsphänomens nehmen die USA ein. Um das Potenzial der fortschreitenden Digitalisierung für die Erfüllung öffentlicher Aufgaben auszuschöpfen und Verwaltungsleistungen mit den Mitteln der Digitalisierung zu optimieren, hat die Obama-Administration ein innovationsorientiertes Stipendienprogramm (das sog. Presidential Innovation Fellows Program)[226] aufgesetzt sowie Organisationseinheiten eingerichtet, die verwaltungsintern Strukturen für ein Corporate Entrepreneurship und Entwicklungen unter Start-Up-Bedingungen schaffen.[227]

Eine Analyse dieser und weiterer Anwendungsbeispiele kann der deutschen öffentlichen Verwaltung Anregungen für vergleichbare Organisationseinheiten an die Hand geben. Für die deutsche Verwaltung verknüpft sich damit vor allem die Frage, inwieweit sich der Nutzwert sol-

---

224 Vgl. für sog. „Internal Corporate Venturing"-Konzepte etwa *Burgelman*, Administrative Science Quaterly 28 (1983), 223; *Heim*, Erfolgsfaktoren für Internal Corporate Venturing in Großunternehmen, 2015; *Klein*, Internal Corporate Venturing, 2002; *Mes*, Internal Corporate Venturing zur Steigerung der Innovationsfähigkeit etablierter Unternehmen, 2011, S. 106 ff.; *Seeliger*, Corporate Venturing in der Praxis, 2004.

225 Dazu grundlegend *Chesbrough*, Open innovation: The New Imperative for Creating and Profiting from Technology, 2003; Zur Übertragbarkeit des Ansatzes in den öffentlichen Sektor *Mergel/Desouza*, Public Administration Review 73 (2013), 882 ff.

226 https://presidentialinnovationfellows.gov/ (30.11.2016).

227 Beispielsweise das Beratungsteam „18F“ innerhalb der U.S. General Service Administration (https://18f.gsa.gov/ [30.11.2016]).

cher Maßnahmen unter den gegebenen verwaltungskulturellen und organisationsrechtlichen Vorgaben[228] der Bundesrepublik Deutschland fruchtbar machen lässt.

228 Für erste Überlegungen hierzu vgl. *Wegener*, Intrapreneurship und Verwaltungskultur – zur Passfähigkeit von Modernisierungsansätzen in der deutschen Verwaltung, in: Heinrichs/Marschall (Hrsg.), Wege zu einer Intrapreneurship-orientierten öffentlichen Verwaltung, 2009, S. 223 ff.

3. *Open-Innovation-Wettbewerbe der öffentlichen Hand – Bürger und Staat als kollaborative Gesellschaftsintrapreneure*

Open-Innovation-Wettbewerbe der öffentlichen Hand – Bürger und Staat als kollaborative Gesellschaftsintrapreneure (Mergel)	
Projekt-inhalt	Das Projekt „Open-Innovation-Wettbewerbe der öffentlichen Hand“ untersucht die Auswirkungen einer Open-Innovation-Strategie auf die Verwaltungskultur aus internationaler Vergleichsperspektive. Dafür trägt es die Ausgestaltungsmöglichkeiten und Potenziale staatlich initiierter, offener gesellschaftlicher Innovationsprozesse zusammen. Zentrale Inhalte sind: • Internationale Übersicht über Open-Innovation- und Crowdsourcing-Plattformen der öffentlichen Verwaltung; • Vergleich der Ausgestaltung von Open-Innovation-Angeboten, etwa als Wettbewerbsverfahren, Ideenbörse, Online-Werkstätten oder Crowdfunding; • Evaluation der Auswirkungen von Open-Innovation-Ansätzen auf die Verwaltungskultur.
Forschungs-ziele	Der Projektzuschnitt zielt zum einen verwaltungswissenschaftlich darauf ab, die Auswirkungen von Open-Innovation-Maßnahmen auf das Selbstverständnis staatlicher Stellen und ihr Verhältnis zum Bürger zu ermitteln. Zum anderen ermittelt das Forschungsvorhaben, inwieweit die tatsächlichen Innovationsergebnisse dazu beitragen, die öffentliche Verwaltung effektiver und effizienter zu gestalten. Dazu gehören insbesondere • die Auswirkungen von Open-Innovation-Maßnahmen auf das Selbstverständnis staatlicher Stellen und ihr Verhältnis zum Bürger; • die Innovationsformen, die sich aufgrund von Open-Innovation-Maßnahmen einstellen und wie diese „externen“ Innovationen in der öffentlichen Verwaltung umsetzbar sind.

Die Möglichkeiten, die sich mit einem Open-Innovation-Ansatz verbinden, sind von erheblicher Dynamik geprägt. Entsprechend sind auch alle wissenschaftlichen Veröffentlichungen sehr jungen Datums. Während in anderen Ländern (vor allem den angelsächsischen) der Gedanke

von Innovation-Labs bereits Schule gemacht hat,[229] steckt er in Deutschland noch in den Kinderschuhen.[230] Sowohl die wissenschaftliche Analyse als auch die praktische Umsetzung steht noch ganz am Anfang.

Die Entwicklung staatlicher Open-Innovation- und Crowdsourcing-Plattformen[231] legt einen internationalen Vergleich zu der Frage nahe, in welcher Form Open-Innovation-Ansätze die Verwaltungskultur bereichern können und insbesondere die zivilgesellschaftliche Einbindung in hoheitlich gesteuerte Entwicklungsprozesse verändern. Dazu gehört neben den verwaltungskulturellen Auswirkungen sinnvollerweise auch die tatsächliche und rechtliche Ausgestaltung der evaluierten Open-Innovation-Angebote als Wettbewerbsverfahren, Ideenbörse oder Online-Werkstatt.

---

229 *Mergel*, Public Management Review – Special Issue: Digital Government and Public Management, 2016; *dies.*, Social Science Computer Review 33 (2015), 599 ff.; *dies.*, Government Information Quarterly 32 (2015), 464 ff.; *dies.*, JMIR mHealth and uHealth 2 (2014), e58, S. 1 ff.; *dies./Bretschneider/Louis et al.*, The Challenges of Challenge.gov: Adopting Private Sector Business Innovations in the Federal Government, in: IEEE Computer Society Washington (Hrsg.), Proceedings of the 2014 47th Hawaii International Conference on System Science, 2014, S. 2073 ff.; *Mergel/Desouza* (Fn. 225); 882 ff.

230 *Hill* (Fn. 121), S. 493 ff.; siehe auch den Bericht zum Symposium „New Paths for Innovation in the Public Sector" an der Universität Speyer von *Harris-Huemmert*, DÖV 2016, 767 ff.

231 Dazu etwa *Aslantas/Huber*, Modernes Städtemanagement. Open Innovation im öffentlichen Sektor, 2015; *Hödl/Rohrer/Zechner*, Open Data und Open Innovation in Gemeinden, 2015; *Kube*, The economics of open innovation, 2015.

4. Digital-transformationale Führung in der Netzwerkverwaltung

Digital-transformationale Führung in der Netzwerkverwaltung (Hill/Ziekow/Misgeld/Wojtczak)	
Projekt-inhalt	Wie Führung im öffentlichen Dienst ausgestaltet sein sollte, um die digitale Transformation einerseits akzeptanzorientiert und verständnisbasiert, andererseits erfolgsorientiert gestalten zu können, gehört zu den zentralen Herausforderungen einer zukunftsfähigen Verwaltung. Wichtige Facetten sind: • Führung im Spannungsfeld zwischen Netzwerk und Hierarchie; • Voraussetzungen und Charakteristik einer digitalen Führung; • Kognitive und motivationale Faktoren einer verstärkten Wandel- und Anpassungsfähigkeit.
For-schungs-ziele	Analyse der Bedingungen eines netzwerkaffinen Führungsstils; Identifikation von Erfolgsfaktoren akzeptanzorientierter und verständnisbasierter Koordinationsmechanismen.

Eine Netzwerkverwaltung zeichnet sich durch interorganisationale Zusammenarbeit und verschränkte Zuständigkeiten aus. Das Aufkommen neuer Informations- und Kommunikationstechnologien und die damit einhergehende gesellschaftsweite digitale Transformation beschleunigt diese Entwicklung.[232] Für eine sich formierende Netzwerkverwaltung ist eine digital-affine Organisationskultur daher unerlässlich. Dazu gehören flexiblere, modularisierte Arbeitsformen und eine organisationsübergreifende, teambezogene Zusammenarbeit. Die Führungsarbeit wird zunehmend komplex. Ein traditioneller, hierarchieorientierter Führungsstil kann entweder obsolet werden oder den Wandel zur Netzwerkverwaltung behindern. Gleichzeitig bleiben bürokratische Prinzipien im Alltagsgeschäft der Verwaltung gültig und erweisen sich mitunter als sinnvoll.[233]

---

232 Vgl. *Steinbicker*, Der Staat der Wissensgesellschaft, in: Collin/Horstmann (Hrsg.), Das Wissen des Staates, 2014, S. 90 ff.

233 Vgl. *Head/Alford*, Administration & Society 2015, 711 ff.; *Misgeld*, Herausforderungen bei der Steuerung von Veränderungsprozessen in der öffentlichen Verwaltung unter besonderer Berücksichtigung des Personal- und Führungsverhaltens, in: Verenkotte/Beutel/Bönder (Hrsg.), Change Management, 2015, S. 55 ff.

Für eine digitale, netzwerkaffine Organisationskultur gilt das Gebot: Eine gute Führung begreift und nutzt die Chancen der digitalen Transformation. Automatisierte und modularisierte Arbeitsprozesse sind insbesondere nur erfolgreich, wenn Mitarbeiter ihren Mehrwert kennen und nachhaltig einzusetzen wissen. Dem ist ein Führungsstil zuträglich, der eine von unten gewachsene Änderungsbereitschaft fördert und überkommene Koordinationsmechanismen hinterfragt.[234]

Entscheidend ist, dass Mitarbeiter an den organisatorischen Schnittstellen fähig und willens sind, Netzwerkdenken zu pflegen und Wissen auszutauschen. Anhaltspunkte zur Ausschöpfung dieses Potenzials bietet die internationale verwaltungswissenschaftliche Literatur zu Governance-Netzwerken. Diese behandelt das Führungsverhalten jedoch nur ausschnittsweise und nicht auf den deutschen Kontext bezogen.[235] Darüber hinaus ist nicht erforscht, wie die Beteiligten dabei unterstützt werden können, ihre kognitive Distanz (d. h. unterschiedliche kulturelle und disziplinbezogene Prägung) im Hinblick auf eine gelingende, wissensintensive Zusammenarbeit zu überbrücken. Das Projekt greift die bestehenden Ansätze verbindend auf und entwickelt einen erfolgversprechenden Führungsstil in der digitalen Transformation der öffentlichen Verwaltung. Leitfragen sind dabei:

- Welcher Führungsstil und welches Führungsverhalten fördert eine digitale, netzwerkaffine Organisationskultur?
- Welche Herausforderungen bestehen für die Implementierung eines solchen Führungsstils unter den besonderen Voraussetzungen der öffentlichen Verwaltung?
- Inwiefern lässt sich das Spannungsfeld zwischen hierarchiebezogener und netzwerkaffiner Führung auflösen?
- Welche kognitiven und motivationalen Faktoren fördern anspruchsvolle, modularisierte Arbeitsformen und eine organisationsübergreifende Zusammenarbeit?

---

234 Vgl. zur Thematik *Brüggemeier/Schulz*, Gestaltung und Steuerung Öffentlicher Leistungsnetzwerke zwischen institutioneller Vielfalt und "neuer Übersichtlichkeit", in: Röber (Hrsg.), Institutionelle Vielfalt und neue Unübersichtlichkeit – Zukunftsperspektiven effizienter Steuerung öffentlicher Aufgaben zwischen Public Management und Public Governance, 2012, S. 95 ff.

235 Vgl. *Borins/Brown*, Digital Leadership: The Human Face of IT, in: Borins/Kernaghan/Brown et al. (Hrsg.), Digital State at the Leading Edge, 2007, S. 277 ff.

- Welche Implikationen sind damit für das Personalmanagement in der öffentlichen Verwaltung verbunden?

Das Projekt zielt darauf, den konzeptionellen Rahmen anhand der Herausforderungen und Möglichkeiten einer netzwerkaffinen Führung[236] in der Praxis empirisch zu validieren.

236 Dazu bereits etwa *Hill* (Fn. 83).

D. Personen

I. Senior Fellows

Prof. Dr. *Mario Martini*, Programmbereichsleiter, Inhaber eines Lehrstuhls für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht an der Deutschen Universität für Verwaltungswissenschaften Speyer.

Prof. Dr. *Hermann Hill*, Inhaber eines Lehrstuhls für Verwaltungswissenschaft und Öffentliches Recht an der Deutschen Universität für Verwaltungswissenschaften Speyer und Leiter der Wissenschaftlichen Dokumentations- und Transferstelle für Verwaltungsmodernisierung in den Ländern (WiDuT).

Prof. Dr. *Helmut Krcmar*, Inhaber eines Lehrstuhls für Wirtschaftsinformatik an der Technischen Universität München und Geschäftsführer von fortiss.

Prof. Dr. *Ines Mergel*, Professorin für Public Administration im Fachbereich Politik und Verwaltungswissenschaften an der Universität Konstanz.

Prof. Dr. *Christoph Sorge*, Inhaber der juris-Stiftungsprofessur für Rechtsinformatik an der Universität des Saarlandes.

Prof. Dr. Dr. h.c. (NUM) *Jan Ziekow*, Inhaber eines Lehrstuhls für Öffentliches Recht, insbesondere allgemeines und besonderes Verwaltungsrecht an der Deutschen Universität für Verwaltungswissenschaften Speyer, Direktor des Forschungsinstituts für öffentliche Verwaltung Speyer und Leiter des Instituts für Gesetzesfolgenabschätzung und Evaluation (InGFA).

II. Forschungsreferenten

- Dr. iur. *Florian Ammerich*
- Dr. iur. *Nadja Braun Binder* MBA (Programmbereichskoordinatorin)
- *Martin Feldhaus*
- *Michael Kolain*
- *Manuel Misgeld*
- *Manfred Müller*
- *David Nink*
- *Tobias Rehorst*
- *David Wagner*
- *Quirin Weinzierl*
- *Markus Wojtczak*

E. Erste Teilergebnisse

I. Im Jahr 2016 veröffentlichte Werke (geordnet nach Erscheinungsdatum)

- *Mario Martini/David Nink/Michael Wenzel*: Bodycams zwischen Bodyguard und Big Brother, Zu den rechtlichen Grenzen filmischer Erfassung von Sicherheitseinsätzen durch Miniaturkameras und Smartphones, NVwZ 2016, 1772 f. (Kurzfassung); NVwZ-Extra 23/2016, S. 1–17 (Langfassung).
- *Nadja Braun Binder*: Vollständig automatisierter Erlass eines Verwaltungsaktes und Bekanntgabe über Behördenportale, DÖV 2016, S. 891–898.
- *Michael Kolain*: Die Blockchain-Technologie in der öffentlichen Verwaltung (Tagungsbericht), Verwaltung und Management 2016, S. 328–333.
- *Mario Martini*: Angst vor einem digitalen Blockwart, FAZ vom 27.10.2016, S. 6.
- *Hill, Hermann*: Führen in digitalisierten Arbeitswelten, Verwaltung und Management 2016, S. 241–249.
- *Mario Martini*: in: Paal/Pauly, DSGVO, München 2016:
  Art. 21 (Widerspruchsrecht), S. 230–249,
  Art. 22 (Automatisierte Entscheidungen im Einzelfall einschließlich Profiling), S. 249–265,
  Art. 24 (Verantwortung des für die Verarbeitung Verantwortlichen), S. 277–290,
  Art. 25 (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen), S. 291–308,
  Art. 26 (Gemeinsam für die Verarbeitung Verantwortliche), S. 308–320,
  Art. 27 (Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern), S. 320–335,
  Art. 28 (Auftragsverarbeiter), S. 335–358,
  Art. 29 (Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters), S. 358–365,
  Art. 30 (Verzeichnis von Verarbeitungstätigkeiten), S. 365–379,
  Art. 31 (Zusammenarbeit mit der Aufsichtsbehörde), S. 380–390,
  Art. 32 (Sicherheit der Verarbeitung), S. 390–409,
  Art. 33 (Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde), S. 410–426,

Art. 34 (Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person), S. 427–443,
Art. 35 (Datenschutz-Folgenabschätzung), S. 443–465,
Art. 79 (Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter), S. 711–722.

- *Nadja Braun Binder*: Weg frei für vollautomatisierte Verwaltungsverfahren in Deutschland, Jusletter IT 22.9.2016, abrufbar unter http://jusletter-it.weblaw.ch (30.11.2016).
- *Michael Kolain*: Lehren aus dem DAO-Hack. Wieso Smart Contracts die Erwartungen enttäuschen müssen, golem.de vom 7.9.2016.
- *Jürgen Kühling/Mario Martini/Johanna Heberlein/Benjamin Kühl/David Nink/Quirin Weinzierl/Michael Wenzel*: Die Datenschutz-Grundverordnung und das nationale Recht – Erste Überlegungen zum innerstaatlichen Regelungsbedarf, Münster 2016, 525 Seiten.
- *Mario Martini*: Wie neugierig darf der Staat im Cyberspace sein? Social Media Monitoring öffentlicher Stellen – Chancen und Grenzen, VerwArch. 3/2016, S. 307–358.
- *Nadja Braun Binder*: Ausschließlich automationsgestützt erlassene Steuerbescheide und Bekanntgabe durch Bereitstellung zum Datenabruf, DStZ 2016, 526–535.
- *Nadja Braun Binder*: Vollautomatisierte Verwaltungsverfahren im allgemeinen Verwaltungsverfahrensrecht?, NVwZ 2016, 960–965.
- *Jürgen, Kühling/Mario, Martini*: Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, 448–454.
- *Hermann Hill*: Innovation Labs – Neue Wege zu Innovation im öffentlichen Sektor, DÖV 2016, 493–501.
- *Nadja Braun Binder*: Auf dem Weg zum vollautomatisierten Besteuerungsverfahren in Deutschland, Jusletter IT 25.5.2016, abrufbar unter http://jusletter-it.weblaw.ch (30.11.2016).
- *Nadja Braun Binder*: Elektronische Bekanntgabe von Verwaltungsakten über Behördenportale, NVwZ 2016, S. 342–347.
- *Hermann Hill*: Öffentliche Angelegenheiten im Wandel: Neue Herausforderungen für Regieren und Verwalten, in: Karl-Peter Sommermann (Hrsg.), Öffentliche Angelegenheiten – interdisziplinär betrachtet, Berlin 2016, S. 49–59.

- *Hermann Hill*: Die Passagiere tanzen auf der Titanic – während der Eisberg naht! Disruptive Einflüsse der Digitalisierung auf Staat und Gesellschaft, Verwaltung und Management 2016, S. 3–13.
- *Mario Martini*: Do it yourself im Datenschutzrecht, NVwZ 2016, 353 f. (Kurzfassung); NVwZ-Extra 6/2016, S. 1–13 (Langfassung).
- *Mario Martini*: „Datenschutzbeauftragte für Behörden sind gefordert", Interview im Jura-Blog „Datenschutzbeauftragter Info", 11.3.2016, abrufbar unter https://www.datenschutzbeauftragter-info.de/datenschutzbeauftragte-fuer-behoerden-sind-gefordert/ (30.11.2016).
- *Ines Mergel*: Agile Innovation Management: A Research Agenda, in: Government Information Quarterly 2016, 33(3), S. 516–523, abrufbar unter http://dx.doi.org/10.1016/j.giq.2016.07.004 (30.11.2016).

II. Zur Veröffentlichung eingereichte, noch nicht erschienene Werke

- *Mario Martini*: Die Zeitung im Sog des digitalen Wandels, Festschrift für Pitschas; erscheint 2017, 53 Seiten Typoskript.
- *Benjamin Kühl*: Staatlich finanzierte Bewertungsportale Privater – Lebensmittelklarheit.de aus lebensmittel- und verfassungsrechtlicher Perspektive (Dissertation); abgeschlossen im November 2016.[237]
- *Matthias Damm*: Der Zugang zu staatlichen Geodaten als Element der Daseinsvorsorge (Dissertation); abgeschlossen im Juli 2016.[238]

237 Hervorgegangen aus dem Vorläuferprojekt „Staatliches Informationshandeln im Web 2.0".

238 Hervorgegangen aus dem Drittmittelprojekt „Nutzungsbedingungen für Geodaten", gefördert durch das BMI.

F. Literaturverzeichnis

Albrecht, *Jan Philipp*, Finger weg von unseren Daten!, Wie wir entmündigt und ausgenommen werden, München 2014.

Allwinkle, *Sam/Cruickshank*, *Peter*, Creating smarter cities – An overview, Journal of Urban Technology 18 (2011), S. 1–16.

Amos, *Heike*, Zur Geschichte des Forschungsinstituts für öffentliche Verwaltung bei der (Deutschen) Hochschule für Verwaltungswissenschaften Speyer 1956/1962–2001, Speyer 2002.

Andelfinger, *Volker P./Hänisch*, *Till*, Internet der Dinge, Technik, Trends und Geschäftsmodelle, Wiesbaden 2015.

Anderheiden, *Michael*, Gemeinwohl in Republik und Union, Tübingen 2006.

Anderl, *Reiner/Anokhin*, *Oleg/Arndt*, *Alexander*, Effiziente Fabrik 4.0 Darmstadt – Industrie 4.0 Implementierung für die mittelständige Industrie, in: Sendler, Ulrich (Hrsg.), Industrie 4.0 grenzenlos, Berlin/Heidelberg 2016, S. 121–136.

Aslantas, *Ömer/Huber, Tim,* Modernes Städtemanagement. Open Innovation im öffentlichen Sektor, München 2015.

Aßmann, *Stephanie/Pleil, Thomas*, Social Media Monitoring: Grundlagen und Zielsetzungen, in: Zerfaß, Ansgar/Piwinger, Manfred (Hrsg.), Handbuch Unternehmenskommunikation, Wiesbaden 2007, S. 585–604.

Auer-Reinsdorff, *Astrid/Conrad, Isabell (*Hrsg.), Handbuch IT- und Datenschutzrecht, 2. Aufl., München 2016.

Auer-Reinsdorff, *Astrid/Kast, Christian R.,* in: Auer-Reinsdorff, Astrid/Conrad, Isabell (Hrsg.), Handbuch IT- und Datenschutzrecht, 2. Aufl., München 2016.

Aust, *Stefan/Ammann, Thomas,* Digitale Diktatur, Totalüberwachung, Datenmissbrauch, Cyberkrieg, Berlin 2016.

Bächle, Thomas Christian, Mythos Algorithmus, Die Fabrikation des computerisierbaren Menschen, Wiesbaden 2015.

Bakos, Jason D., Embedded systems, ARM programming and optimization, Amsterdam 2016.

Bauernhansl, Thomas, Die Vierte Industrielle Revolution – Der Weg in ein wertschaffendes Produktionsparadigma, in: Bauernhansl, Thomas/Hompel, Michael ten/Vogel-Heuser, Birgit (Hrsg.), Industrie 4.0 in Produktion, Automatisierung und Logistik, Anwendung, Technologien und Migration, Wiesbaden 2014, S. 5–36.

Bauernhansl, *Thomas/Hompel, Michael ten/Vogel-Heuser, Birgit* (Hrsg.), Industrie 4.0 in Produktion, Automatisierung und Logistik, Anwendung, Technologien und Migration, Wiesbaden 2014.

Beck, Susanne, Grundlegende Fragen zum rechtlichen Umgang mit der Robotik, JR 2009, S. 225–230.

Beck, Susanne (Hrsg.), Jenseits von Mensch und Maschine, Ethische und rechtliche Fragen zum Umgang mit Robotern, Künstlicher Intelligenz und Cyborgs, Baden-Baden 2012.

Benecke, Alexander/Wagner, Julian, Öffnungsklauseln in der Datenschutz-Grundverordnung und das deutsche BDSG, Grenzen und Gestaltungsspielräume für ein nationales Datenschutzrecht, DVBl. 2016, S. 600–608.

Benz, Arthur, Eine Gestalt, die alt geworden ist? Thesen zum Wandel des Staates, Leviathan 40 (2012), S. 223–247.

Berns, *Karsten/Bernd, Schürmann/Trapp, Mario,* Eingebettete Systeme, Systemgrundlagen und Entwicklung eingebetteter Software, Wiesbaden 2010.

BITKOM, Datenschutz in der digitalen Welt, 2015, https://www.bitkom.org/Presse/Anhaenge-an-PIs/2015/09-September/Bitkom-Charts-PK-Datenschutz-22092015-final.pdf (26.10.2016).

– Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter, Berlin 2015.

– Jedes zweite Automobilunternehmen erwartet Durchbruch für autonomes Fahren bis 2030, Marktteilnehmerumfrage, Pressemitteilung v. 8.9.2015, https://www.bitkom.org/Presse/Presseinformation/Jedes-zweite-Automobilunternehmen-erwartet-Durchbruch-fuer-autonomes-Fahren-bis-2030.html (6.10.2016).

– Internetnutzer gehen pragmatisch mit Datenschutz um, Benutzerfreundlichkeit darf nicht unter überzogenen Datenschutzregeln leiden, Pressemittelung v. 22.9.2015 Berlin, http://www.bitkom-research.de/epages/63742557.sf/de_DE/?ObjectPath=/Shops/63742557/Categories/Presse/Pressearchiv_2015/Internetnutzer_gehen_pragmatisch_mit_Datenschutz_um (6.10.2015).

Blocher, *Walter,* The next big thing: Blockchain – Bitcoin – Smart Contracts, Wie das disruptive Potential der Distributed Ledger Technology (nicht nur) das Recht fordern wird, AnwBl 2016, S. 612–618.

Boehme-Neßler, Volker, Das Ende der Anonymität, Wie Big Data das Datenschutzrecht verändert, DuD 2016, S. 419–423.

Borges, Georg, Der neue Personalausweis und der elektronische Identitätsnachweis, NJW 2010, S. 3334–3339.

Borins, *Sandford/Brown, David,* Digital Leadership: The Human Face of IT, in: Borins, Sandford/Kernaghan, Kenneth/Brown, David et al. (Hrsg.), Digital State at the Leading Edge, Toronto et. al. 2007, S. 277–301.

Borins, *Sandford/Kernaghan, Kenneth/Brown, David/Bontis, Nick* et al. (Hrsg.), Digital State at the Leading Edge, Toronto et. al. 2007.

Brand, *Leif/Hülser, Tim/Grimm, Vera/Zweck, Axel*, Internet der Dinge – Perspektive für die Logistik, Übersichtsstudie, 2015, https://www.vdi.de/fileadmin/vdi_de/redakteur/dps_bilder/TZ/2009/Band%2080_IdD_komplett.pdf (8.11.2016).

Brauckmann, Patrick (Hrsg.), Web-Monitoring, Gewinnung und Analyse von Daten über das Kommunikationsverhalten im Internet, Konstanz 2010.

Braun Binder, Nadja, Auf dem Weg zum vollautomatisierten Besteuerungsverfahren in Deutschland, Jusletter IT vom 25.5.2016, S. 1–10.

– Weg frei für vollautomatisierte Verwaltungsverfahren in Deutschland, Jusletter IT vom 22.9.2016, S. 1–12.

– Ausschließlich automationsgestützt erlassene Steuerbescheide und Bekanntgabe durch Bereitstellung zum Datenabruf, DStZ 2016, S. 526–535.

– Elektronische Bekanntgabe von Verwaltungsakten über Behördenportale, NVwZ 2016, S. 342–347.

– Vollautomatisierte Verwaltungsverfahren im allgemeinen Verwaltungsverfahrensrecht?, Der Gesetzesentwurf zur Modernisierung des Besteuerungsverfahrens als Vorbild für vollautomatisierte Verwaltungsverfahren nach dem VwVfG, NVwZ 2016, S. 960–965.

– Vollständig automatisierter Erlass eines Verwaltungsaktes und Bekanntgabe über Behördenportale, DÖV 2016, S. 891–898.

Bräutigam, *Peter/Klindt, Thomas,* Industrie 4.0, das Internet der Dinge und das Recht, NJW 2015, S. 1137–1142.

Brüggemeier, *Martin/Schulz, Sirko,* Gestaltung und Steuerung Öffentlicher Leistungsnetzwerke zwischen institutioneller Vielfalt und "neuer Übersichtlichkeit", in: Röber, Manfred (Hrsg.), Institutionelle Vielfalt und neue Unübersichtlichkeit – Zukunftsperspektiven effizienter Steuerung öffentlicher Aufgaben zwischen Public Management und Public Governance, Berlin 2012, S. 95–127.

BSI, Neuer Fall von großflächigem Identitätsdiebstahl: BSI informiert Betroffene, Pressemitteilung v. 7.4.2014, https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Neuer_Fall_von_Identitaetsdiebstahl_07042014.html (6.10.2016).

– Die Lage der IT-Sicherheit in Deutschland 2015, Bonn 2015.

– BSI veröffentlicht Bericht zur Lage der IT-Sicherheit in Deutschland 2016, Pressemitteilung v. 9.11.2016, https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2016/Lage_IT-Sicherheit_in_Deutschland_09112016.html (30.11.2016).

Buchmann, Johannes/Roßnagel, Alexander, Das Bundesverfassungsgericht und Telemedienwahlen – Zu den Auswirkungen des Urteils des BVerfG zu elektronischen Wahlgeräten für die Durchführung von "Internetwahlen" in nicht-politischen Bereichen, K&R 2009, S. 543–548.

Budde, Paul, Cities for Smart Environmental and Energy Futures – Impacts on Architecture and Technology, in: Rassia, Stamatina Th/Pardalos, Panos M. (Hrsg.), Cities for smart environmental and energy futures, Impacts on architecture and technology, Heidelberg 2014.

Bullinger, Hans-Jörg/Röthlein, Brigitte, Morgenstadt, Wie wir morgen leben: Lösungen für das urbane Leben der Zukunft, München 2012.

Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2016, Berlin 2016.

Bundesministerium des Innern, Bericht der Bundesregierung zur Verzichtbarkeit der Anordnungen der Schriftform und des persönlichen Erscheinens im Verwaltungsrecht des Bundes, Berlin 2016.

– Umsetzung der Digitalisierung: Bundeskabinett beschließt E-Rechnungs-Gesetz, Pressemitteilung v. 13.7.2016, https://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2016/07/bundeskabinett-beschliesst-e-rechnungs-gesetz.html (23.11.2016).

Bundesministerium für Wirtschaft und Energie, Zukunft der Arbeit in der Industrie 4.0, Berlin 2014.

– Grünbuch Digitale Plattformen, 2016.

Bundesnetzagentur, „Smart Grid“ und „Smart Market“, Eckpunktepapier der Bundesnetzagentur zu den Aspekten des sich verändernden Energieversorgungssystems, Bonn 2011.

Bundesregierung, Digitale Agenda 2014-2017, Berlin 2014.

– Digitale Verwaltung 2020. Regierungsprogramm 18. Legislaturperiode, Berlin 2014.

Burgelman, Robert A., A Process Model of International Corporate Venturing in the Diversified Major Firm, Administrative Science Quaterly 28 (1983), S. 223–244.

Buschauer, *Regine,* (Very) nervous systems. Big Mobile data, in: Reichert, Ramón (Hrsg.), Big Data, Die Gesellschaft als digitale Maschine, Bielefeld 2014, S. 405–436.

Capurro, Rafael (Hrsg.), Ethics and robotics, Heidelberg 2009.

Cavanillas, José María/Curry, Edward/Wahlster, Wolfgang (Hrsg.), New Horizons for a Data-Driven Economy, A Roadmap for Usage and Exploitation of Big Data in Europe, Cham 2016.

Centre for Internet and Human Rights, Ethics of Algorithms: from radical content to self-driving cars, Final Draft Background Paper, 2015, https://www.gccs2015.com/sites/default/files/documents/Ethics_Algorithms-final%20doc.pdf (6.1.2016).

Chen, *Zhen-Jiao/Vogel, Douglas/Wang, Zhao-Hua,* How to satisfy citizens? Using mobile government to reengineer fair government processes, Decision Support Systems 2016, S. 47–57.

Chesbrough, Henry, Open innovation: The New Imperative for Creating and Profiting from Technology, Boston 2003.

Cisco, Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020, San José 2016.

Cocchia, *Annalisa,* Smart and digital city – A systematic literature review, in: Dameri, Renata Paola/Rosenthal-Sabroux, Camille (Hrsg.), Smart City, Cham 2014, S. 13–43.

Codagnone, Cristiano/Wimmer, Maria A. (Hrsg.), Roadmapping eGovernment Research, Visions and Measures towards Innovative Governments in 2020, Clusone 2007.

Collin, Peter/Horstmann, Thomas (Hrsg.), Das Wissen des Staates, Geschichte, Theorie und Praxis, Baden-Baden 2014.

Corporate Trust, Industriespionage 2014 – Cybergeddon der deutschen Wirtschaft durch NSA & Co.?, 2015, https://www.corporate-trust.de/pdf/CT-Studie-2014_DE.pdf (3.3.2016).

Dameri, Renata Paola/Rosenthal-Sabroux, Camille (Hrsg.), Smart City, Cham 2014.

Deloitte NASACT, Digital Government Transformation Survey, 2015, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-state-nasact-survey.pdf (23.11.2016).

Demmel, Annette/Herten-Koch, Rut, Vergaberechtliche Probleme bei der Beschaffung von Open-Source-Software, NZBau 2004, S. 187–189.

Deutsches Institut für Vertrauen und Sicherheit im Internet, DIVSI Internet-Milieus 2016: Die digitalisierte Gesellschaft in Bewegung, Hamburg 2016.

– Meinungsführer-Studie: Wer gestaltet das Internet?, Hamburg 2012.

– Entscheider-Studie zu Vertrauen und Sicherheit im Internet, Hamburg 2013.

Directorate-General for Communications Networks, Content and Technology, A vision for public services, Draft Version, 13.6.2013, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=3179 (6.1.2017).

Drösser, Christoph, Total berechenbar?, Wenn Algorithmen für uns entscheiden, München 2016.

Eckert, Claudia, Industrie 4.0? Mit Sicherheit!, DuD 2015, S. 641.

Ehlen, Theresa/Brandt, Elena, Die Schutzfähigkeit von Daten – Herausforderungen und Chancen für Big Data Anwender, CR 2016, S. 570–575.

Eigner, Martin, Das Industrial Internet, Engineering Prozesse und IT-Lösungen, in: Sendler, Ulrich (Hrsg.), Industrie 4.0 grenzenlos, Berlin/Heidelberg 2016, S. 137–168.

EMC, The Digital Universe of Opportunities, Infobrief, April 2014, https://www.emc.com/collateral/analyst-reports/idc-digital-universe-2014.pdf (24.11.2016).

Erbstößer, Anne-Caroline, Smart City Berlin – Urbane Technologien für Metropolen, Report 2014, 2014, http://www.technologiestiftung-berlin.de/fileadmin/daten/ (11.3.2016).

Etezadzadeh, Chirine, Smart City – Future City?, Wiesbaden 2016.

Europäische Kommission, Study on eGovernment and the Reduction of Administrative Burden, Final Report, Brüssel 2014.

– Autonomous Systems Report, Special Eurobarometer 427, Brüssel 2015.

– Implementation of the EU regulatory framework for electronic communication – 2015, Commission staff working document, Brüssel 2015.

– A Digital Single Market Strategy for Europe – Analysis and Evidence, SWD(2015) 100 final, Brüssel 2015.
– Digital Single Market Strategy – Questions and answers, Fact Sheet, Brüssel 2015.
– Digital Economy and Society Index – Country Profile Germany, Brüssel 2016.
– Workshop on new eGovernment Action Plan: Workshop report, Brüssel 2015.
– EU-eGovernment-Aktionsplan 2016-2020, COM(2016) 179 final, Beschleunigung der Digitalisierung der öffentlichen Verwaltung, Brüssel 2016.
– eGovernment Benchmark 2016 – Country Factsheet Germany, Brüssel 2016.

Europäisches Parlament, eGovernment – Using technology to improve public services and democratic participation, Straßburg September 2015.

European Data Protection Supervisor, Meeting the Challenges of Big Data, A call for transparency, user control, data protection by design and accountability, Opinion 7/2015, Brüssel 2015.

Evans, Dave, Das Internet der Dinge, So verändert die nächste Dimension des Internet die Welt, 2011, http://www.cisco.com/web/DE/assets/executives/pdf/Internet_of_Things_IoT_IBSG_0411FINAL.pdf (30.11.2016).

Fadavian, Benjamin (Hrsg.), Transparente Staatstätigkeit, Hamburg 2016.

Forbes, Liste der wertvollsten Unternehmensmarken, http://www.forbes.com/pictures/mli45fflfg/1-apple/#25713ad97d28 (5.10.2016).

Frantzen, Andreas, Einsatz der Netzwerkforensik für Ermittlungsbehörden, Vortrag vom 19.12.2013, 2013, https://pound.netzpolitik.org/wp-upload/2013-12-19_CAST-Frantzen-Netzwerkforensik.pdf (24.11.2016).

Franz, Yvonne, Smart or not smart – What makes a city intelligent?, in: Widmann, Helmut (Hrsg.), Smart city, Viennese expertise based on science and research, Wien 2012, S. 28–34.

Fraunhofer Institut für intelligente Analyse- und Informationssysteme, BIG DATA – Vorsprung durch Wissen, Innovationspotenzialanalyse, Sankt Augustin 2012.

Fromm, Jens/Weber, Mike, ÖFIT-Trendschau: Öffentliche Informationstechnologie in der digitalisierten Gesellschaft, Berlin Juli 2014.

Fromm, Jens/Welze, Christian/Hoepner, Petra/Pattberg, Jonas, Vertrauenswürdige digitale Identität: Baustein für öffentliche IT, Berlin 2013.

Galdon-Clavell, G., (Not so) smart cities?, The drivers, impact and risks of surveillance-enabled smart environments, Science and Public Policy 40 (2013), S. 717–723.

Gartner, Inc., Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015, In 2020, 25 Billion Connected "Things" Will Be in Use, Pressemitteilung v. 11.11.2014, http://www.gartner.com/newsroom/id/2905717 (6.10.2016).

Gascó, Mila, New Technologies and Institutional Change in Public Administration, Social Science Computer Review 21 (2003), S. 6–14.

Geiselberger, Heinrich (Hrsg.), Big Data, Das neue Versprechen der Allwissenheit, Berlin 2013.

Gentsch, Peter/Zahn, Anna-Maria, Potenziale und Anwendungsfelder von Web-Monitoring im Unternehmen, in: Brauckmann, Patrick (Hrsg.), Web-Monitoring, Gewinnung und Analyse von Daten über das Kommunikationsverhalten im Internet, Konstanz 2010, S. 97–131.

Giesberg, Georg, Big Data wird zum Maßstab für den Fortschritt, FAZ vom 17.8.2015, S. 16.

Goldstein, Brett/Dyson, Lauren (Hrsg.), Beyond Transparency, Open Data and the Future of Civic Innovation, San Francisco 2013.

Goyal, Ela/Purohit, Seema, Emergence of m-Government – The way forward, SIES Journal of Management 2012, S. 56–65.

Greenwald, Glen, Die globale Überwachung, Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen, München 2014.

Guckelberger, Annette, Smard Grids/Smart Meter zwischen umweltverträglichen Energieversorgung und Datenschutz, DÖV 2012, S. 613–622.

Günther, Jens/Böglmüller, Matthias, Arbeitsrecht 4.0 – Arbeitsrechtlichliche Herausforderungen in der vierten industriellen Revolution, NZA 2015, S. 1025–1031.

Halang, Wolfgang A./Holleczek, Peter, Eingebettete Systeme, Berlin/Heidelberg 2011.

Harris-Huemmert, Susan, New Paths for Innovation in the Public Sector – Ein Symposium an der Universität Speyer, 25.–26. Februar 2016 –, DÖV 2016, S. 767–771.

Head, Brian W./Alford, John, Wicked Problems, Implications for Public Policy and Management, Administration & Society 2015, S. 711–739.

Heim, Frank-Benjamin, Erfolgsfaktoren für Internal Corporate Venturing in Großunternehmen, Eine empirische Analyse, Lohmar 2015.

Heinrichs, Michael/Marschall, Katja (Hrsg.), Wege zu einer Intrapreneurship-orientierten öffentlichen Verwaltung, Dokumentation der Tagung Think Ahead – Move Forward vom 23.–24. April 2008 in Güstrow, Bremen 2009.

Henning, Maria/Volkamer, Melanie/Budurushi, Jurlind, Transparentes eVoting, DÖV 2012, S. 789–796.

Hermes, Georg, Staatliche Infrastrukturverantwortung, Rechtliche Grundstrukturen netzgebundener Transport- und Übertragungssysteme zwischen Daseinsvorsorge und Wettbewerbsregulierung am Beispiel der leitungsgebundenen Energieversorgung in Europa, Tübingen 1998.

Hessische Landesregierung, Strategie Digitales Hessen, Intelligent. Vernetzt. Für Alle, Wiesbaden 2016.

Heuser, Lutz/Wahlster, Wolfgang (Hrsg.), Internet der Dienste, Berlin/Heidelberg 2011.

Hewlett Packard Enterprise, Internet of things research study, Palo Alto 2015.

Hilgendorf, Eric/Günther, Jan-Philipp (Hrsg.), Robotik und Gesetzgebung, Beiträge der Tagung vom 7. bis 9. Mai 2012 in Bielefeld, Baden-Baden 2013.

Hill, Hermann, Wandel von Verwaltungskultur und Kompetenzen im digitalen Zeitalter, in: Hill, Hermann/Martini, Mario/Wagner, Edgar (Hrsg.), Transparenz, Partizipation, Kollaboration, Die digitale Verwaltung neu denken, Baden-Baden 2014, S. 125–148.

– Die Passagiere tanzen auf der Titanic – während der Eisberg naht!, Disruptive Einflüsse der Digitalisierung auf Staat und Gesellschaft, Verwaltung und Management 2016, S. 1–13.

– Führung in digitalisierten Arbeitswelten, Verwaltung und Management 2016, S. 241–249.

– Innovation Labs, Neue Wege zu Innovation im öffentlichen Sektor, DÖV 2016, S. 493–501.

Hill, Hermann/Martini, Mario/Wagner, Edgar (Hrsg.), Transparenz, Partizipation, Kollaboration, Die digitale Verwaltung neu denken, Baden-Baden 2014.

Hill, Hermann/Martini, Mario/Wagner, Edgar (Hrsg.), Die digitale Lebenswelt gestalten, Baden-Baden 2015.

Hödl, *Elisabeth/Rohrer, Tanja/Zechner, Martin,* Open Data und Open Innovation in Gemeinden, Wien 2015.

Hoffmann, Christian, Apps der öffentlichen Verwaltung, Rechtsfragen des Mobile Government, MMR 2013, S. 631–636.

Hoffmann, Christian/Schulz, Sönke E./Brackmann, Franziska, Web 2.0 in der öffentlichen Verwaltung, Twitter, Facebook und Blogs aus rechtlicher Perspektive, in: Schliesky, Utz/Schulz, Sönke E. (Hrsg.), Transparenz, Partizipation, Kollaboration, Web 2.0 für die öffentliche Verwaltung, Kiel 2012, S. 163–208.

Hoffmann-Riem, Wolfgang, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, JZ 2014, S. 53–63.

Hoffmann-Riem, Wolfgang/Schmidt-Assmann, Eberhard/Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. I, Methoden, Maßstäbe, Aufgaben, Organisation, 2. Aufl., München 2012.

Hofmann, Olaf, Methoden des Social Media Monitoring, in: König, Christian/Stahl, Matthias/Wiegand, Erich (Hrsg.), Soziale Medien, Gegenstand und Instrument der Forschung, Wiesbaden 2014, S. 161–170.

Hofmann, Thomas/Schölkopf, Bernhard, Vom Monopol auf Daten ist abzuraten, FAZ vom 29.1.2015, S. 14.

Hofstetter, Yvonne, Sie wissen alles, Wie intelligente Maschinen in unser Leben eindringen und warum wir für unsere Freiheit kämpfen müssen, München 2014.

– Verkannte Revolution: Big Data und die Macht des Marktes, APuZ 2015, S. 33–38.

Horner, Susanne/Kaulartz, Markus, Haftung 4.0, CR 2016, S. 7–14.

IBM Corporation, Towards 2025: Delivering public sector digital transformation in Australia, White Paper, November 2013, http://www-935.ibm.com/services/multimedia/en_final_gov_pub_admin_whitepaper.pdf (24.11.2016).

IBM Institute for Business Value, The new hero of big data and analytics – The Chief Data Officer, Executive Report, Juni 2014, http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&appname=GBSE_GB_TI_USEN&htmlfid=GBE03607USEN&attachment=GBE03607USEN.PDF (24.11.2016).

IEEE Computer Society Washington (Hrsg.), Proceedings of the 2014 47th Hawaii International Conference on System Science, Washington 2014.

Initiative D21, eGovernment Monitor 2015, Berlin 2015.

– D21-Digital-Index 2016, Jährliches Lagebild zur Digitalen Gesellschaft, Berlin 2016.

– eGovernment Monitor 2016, Berlin 2016.

Institute for Prospective Technological Studies (IPTS), Envisioning Digital Europe 2030, Scenarios for ICT in Future Governance and Policy Modelling, 2010, http://ftp.jrc.es/EURdoc/JRC61593.pdf (24.11.2016).

International Energy Agency, Smart Grids, Technology Roadmap, 2011, https://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf (27.10.2016).

Internet & Gesellschaft Collaboratory, Smart Country – Digitale Strategien für Regionen. Interaktiver Hintergrundbericht, https://smartcountry.collaboratory.de/ecm-politik/colab/de/home/beteiligen/draftbill/44586/13 (24.9.2015).

Isensee, Josef, § 71 Gemeinwohl im Verfassungsstaat, in: Isensee, Josef/Kirchhof, Ferdinand (Hrsg.), HdbStR IV, 3. Aufl., Heidelberg 2006, S. 3–80.

Isensee, Josef/Kirchhof, Ferdinand (Hrsg.), HdbStR IV, 3. Aufl., Heidelberg 2006.

IT-Planungsrat, Entscheidungsniederschrift zur 18. Sitzung des IT-Planungsrats am 1. Oktober 2015 in Berlin, 2015, https://joinup.ec.europa.eu/sites/default/files/18._sitzung_entscheidungsniederschrift_mit_anlagen.pdf (24.11.2016).

– Projektsteckbrief Portalverbund, Berlin 2016.

Jandt, Silke, Beweissicherheit im elektronischen Rechtsverkehr, Folgen der europäischen Harmonisierung, NJW 2015, S. 1205–1211.

Kaczorowski, Willi, Die smarte Stadt, Den digitalen Wandel intelligent gestalten; Handlungsfelder, Herausforderungen, Strategien, Stuttgart 2014.

Kagermann, Henning/Wahlster, Wolfgang/Helbig, Johannes, Deutschlands Zukunft als Produktionsstandort sichern, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, Frankfurt am Main 2013.

Karsten, Till, Datenschutz im Smart Grid & Smart Meter, Eine Einführung in die Regelungen zu Smart Grid und Smart Metern aus datenschutzrechtlicher Sicht, Saarbrücken 2015.

Kaulartz, Markus, Die Blockchain-Technologie, CR 2016, S. 474–480.

Kipker, Dennis-Kenji/Gärtner, Hauke, Verfassungsrechtliche Anforderungen an den Einsatz polizeilicher „Body-Cams", NJW 2015, S. 296–301.

Kirchhof, Paul, Das Wettbewerbsrecht als Teil einer folgerichtigen und widerspruchsfreien Gesamtrechtsordnung, in: Kirchhof, Paul (Hrsg.), Gemeinwohl und Wettbewerb, Heidelberg 2005, S. 1–18.

Kirchhof, Paul (Hrsg.), Gemeinwohl und Wettbewerb, Heidelberg 2005.

Klein, Holger, Internal Corporate Venturing, Die Überwindung von Innovationsbarrieren in DAX 100-Unternehmen, Wiesbaden 2002.

Koch, Volkmar/Kuge, Simon/Geissbauer, Reinhard/Schrauf, Stefan, Industrie 4.0, Chancen und Herausforderungen der vierten industriellen Revolution, 2014, http://www.strategyand.pwc.com/media/file/Industrie-4-0.pdf (8.11.2016).

Koch, Wolfgang/Frees, Beate, Dynamische Entwicklung bei mobiler Internetnutzung sowie Audios und Videos, Media Perspektiven 2016, S. 418–437.

Kolain, Michael, Die Blockchain-Technologie in der öffentlichen Verwaltung (Tagungsbericht), Verwaltung und Management 2016, S. 328–333.

Kolain, Michael/Wirth, Christian, Speed Dating on Smart Contracts, in: Parycek, Peter/Edelmann, Noella (Hrsg.), CeDEM16, Conference for E-Democracy and Open Government, Krems 2016, S. 201–204.

Kompetenzzentrum Öffentliche IT, Verwaltung x.0. Öffentliche Informationstechnologie in der digitalisierten Gesellschaft – Trendthema 29, Berlin 2015.

König, Christian/Stahl, Matthias/Wiegand, Erich (Hrsg.), Soziale Medien, Gegenstand und Instrument der Forschung, Wiesbaden 2014.

Koordinierungsstelle für IT-Standards (KoSIT), Standardisierungsagenda, 2.9.2015, http://www.xoev.de/de/detail.php?gsid=bremen83.c.2316.de#Agenda (9.1.2017).

Kube, Mathias, The economics of open innovation, Essays on private and public actors in systems of innovation, Hamburg 2015.

Kucklick, Christoph, Die granulare Gesellschaft, Wie das Digitale unsere Wirklichkeit auflöst, Berlin 2014.

Kühling, Jürgen, Rückkehr des Rechts: Verpflichtung von „Google & Co." zu Datenschutz, EuZW 2014, S. 527–532.

Kühling, Jürgen/Martini, Mario, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, S. 448–454.

Kühling, Jürgen/Martini, Mario/Heberlein, Johanna/Kühl, Benjamin et al., Die DSGVO und das nationale Recht – Erste Überlegungen zum nationalen Regelungsbedarf, Münster 2016.

Landherr, Martin/Neumann, Michael/Volkmann, Johannes/Constantinescu, Carmen, Digitale Fabrik, in: Westkämper, Engelbert/Spath, Dieter/Constantinescu, Carmen et al. (Hrsg.), Digitale Produktion, Berlin, Heidelberg 2013, S. 107–132.

Laue, Philip, Öffnungsklauseln in der DS-GVO – Öffnung wohin?, Geltungsbereich einzelstaatlicher (Sonder-)Regelungen, ZD 2016, S. 463–467.

Legnaro, Aldo/Kretschmann, Andrea, Das Polizieren der Zukunft, The future of policing – policing the future, Krim. Journal 2015, S. 94–111.

Leiner, Peter, Big Data in der Onkologie, Im Fokus Onkologie 2016, S. 12–17.

Luch, Anika D./Schulz, Sönke E./Tischer, Jakob, Online-Wahlen und -Abstimmungen in Deutschland, BayVBl 2015, S. 253–257.

Lucke, Dominik, Smart Factory, in: Westkämper, Engelbert/Spath, Dieter/Constantinescu, Carmen et al. (Hrsg.), Digitale Produktion, Berlin/Heidelberg 2013, S. 251–270.

Lutes, Terence (Terry), Data-driven government: Challenges and a path forward. IBM-Analytics White Paper, April 2015, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GQW03008USEN (24.11.2016).

Maas, Heiko, Unsere digitalen Grundrechte, Die ZEIT vom 10.12.2015, http://www.zeit.de/2015/50/internet-charta-grundrechte-datensicherheit (9.3.2016).

Markl, Volker/Hoeren, Thomas/Krcmar, Helmut, Innovationspotenzialanalyse für die neuen Technologien für das Verwalten und Analysieren von großen Datenmengen (Big Data Management), Finale Studienergebnisse, Version 1.0, Berlin November 2013.

Martens, Kay-Uwe, Rechtsprobleme der Open Source Software in der Verwaltung, KommJur 2007, S. 94–101.

Marthews, Alex/Tucker, Catherine, Government Surveillance and Internet Search Behavior, 29.4.2015,

https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2600645_code512675.pdf?abstractid=2412564&mirid=1 (26.11.2016).

Martini, Mario, Der Markt als Instrument hoheitlicher Verteilungslenkung, Möglichkeiten und Grenzen einer marktgesteuerten staatlichen Verwaltung des Mangels, Tübingen 2008.

– Der Zensus 2011 als Problem interkommunaler Gleichbehandlung, Berlin 2011.

– Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht, DVBl. 2014, S. 1481–1489.

– Big Data als Herausforderung für das Datenschutzrecht und den Persönlichkeitsschutz, in: Hill, Hermann/Martini, Mario/Wagner, Edgar (Hrsg.), Die digitale Lebenswelt gestalten, Baden-Baden 2015, S. 97–162.

– Wie werden und wollen wir morgen leben?, Ein Blick in die Glaskugel der digitalen Zukunft, in: Hill, Hermann/Martini, Mario/Wagner, Edgar (Hrsg.), Die digitale Lebenswelt gestalten, Baden-Baden 2015, S. 9–56.

– Wie neugierig darf der Staat im Cyberspace sein?, Social Media Monitoring öffentlicher Stellen – Chancen und Grenzen, VerwArch. 2016, S. 307–358.

– Do it yourself im Datenschutzrecht, Der „Geo Business Code of Conduct" als Erprobungsfeld regulierter Selbstregulierung, NVwZ-Extra 3/2016, S. 1–13.

– Angst vor einem digitalen Blockwart, FAZ vom 27.10.2016, S. 6.

Martini, Mario/Fritzsche, Saskia, Zwischen Öffentlichkeitsauftrag und Gesetzesbindung: Zum Dilemma deutscher Behörden bei der Einbindung privater Social-Media-Werkzeuge und Geodatendienste in ihre Internetangebote, VerwArch 104 (2013), S. 449–485.

– Kompendium Online-Bürgerbeteiligung, Rechtliche Rahmenbedingungen kommunaler Beteiligungsangebote im Internet, München 2015.

– Mitverantwortung in sozialen Netzwerken, Fanpage-Betreiber in der datenschutzrechtlichen Grauzone, NVwZ-Extra 21/2015, S. 1–16.

Martini, Mario/Nink, David/Wenzel, Michael, Bodycams zwischen Bodyguard und Big brother, Zu den rechtlichen Grenzen filmischer Erfassung von Sicherheitseinsätzen durch Miniaturkameras und Smartphones, NVwZ-Extra 24/2016, 1–18.

Mayer-Schönberger, Viktor/Cukier, Kenneth, Big Data, Die Revolution, die unser Leben verändern wird, München 2013.

McKinsey Global Institute, Internet matters: The Net`s sweeping impact on growth, jobs, and prosperity, Mai 2011, http://www.mckinsey.com/industries/high-tech/our-insights/internet-matters (16.11.2016).

– The Internet of Things: Five critical questions, Interview with leading industry experts, 2015, http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-ofthings-five-critical-questions (6.1.2017).

– Digital Globalization: The new era of global flows, 2016.

McKinsey, E-Government in Deutschland, Eine Bürgerperspektive, März 2015, https://www.mckinsey.de/files/e-government_in_deutschland_eine_buergerperspektive.pdf (7.11.2016).

Meinecke, Dirk, Big Data und Data Mining: Automatisierte Strafverfolgung als neue Wunderwaffe der Verbrechensbekämpfung?, in: Taeger, Jürgen (Hrsg.), Big Data & Co, Neue Herausforderungen für das Informationsrecht, Edewecht 2014, S. 183–202.

Mergel, Ines, Drivers and Barriers for Open Innovation in the Public Sector, Public Management Review – Special Issue: Digital Government and Public Management, 2016.

– The Long Way From Government Open Data to Mobile Health Apps: Overcoming Institutional Barriers in the US Federal Government, JMIR mHealth and uHealth 2014, e58, S. 1–13.

– Open Collaboration in the Public Sector: The Case of Social Coding on Github, Government Information Quarterly 2015, S. 464–472.

– Opening Government: Designing Open Innovation Processes to Collaborate with External Problem Solvers, Social Science Computer Review 2015, S. 599–612.

Mergel, Ines/Bretschneider, Stuart I./Louis, Claudia/Smith, Jason, The Challenges of Challenge.gov: Adopting Private Sector Business Innovations in the Federal Government, in: IEEE Computer Society Washington (Hrsg.), Proceedings of the 2014 47th Hawaii International Conference on System Science, Washington 2014, S. 2073–2082.

Mergel, Ines/Desouza, Kevin, Implementing Open Innovation in the Public Sector: The Case of Challenge.gov, Public Administration Review 73 (2013), S. 882–890.

Mes, Florian, Internal Corporate Venturing zur Steigerung der Innovationsfähigkeit etablierter Unternehmen, Wiesbaden 2011.

Misgeld, Manuel, Herausforderungen bei der Steuerung von Veränderungsprozessen in der öffentlichen Verwaltung unter besonderer Berücksichtigung des Personal- und Führungsverhaltens, in: Verenkotte, Christoph/Beutel, Rainer Christian/Bönder, Thomas (Hrsg.), Change Management, Baden-Baden 2015, S. 55–70.

Moore, Jack, Rise of the Data Chiefs: Meet the Federal Officials Aiming to Usher in Government's 'Golden Age' of Data, 2015, http://www.nextgov.com/big-data/2015/03/rise-data-geeks-meet-federal-officials-aiming-usher-governments-golden-age-data/107736/ (30.6.2016).

Morgenroth, Markus, Sie kennen dich! Sie haben dich! Sie steuern dich!, Die wahre Macht der Datensammler, München 2016.

Nationale Plattform Zukunftsstadt, Die Zukunftsstadt – CO2-neutral, energie-/ressourceneffizient, klimaangepasst und sozial, Langfassung der Strategischen Forschungs- und Innovationsagenda, Februar 2015, http://www.nationale-plattform-zukunftsstadt.de/NPZ_Langfassung_FINA.pdf (24.11.2016).

Nationaler Normenkontrollrat, E-Government in Deutschland: Wie der Aufstieg gelingen kann – ein Arbeitsprogramm (Kurzfassung), Berlin 2016.

– E-Government in Deutschland: Wie der Aufstieg gelingen kann – ein Arbeitsprogramm (Langfassung), Berlin 2016.

Neumann, Kirsten/Moorfeld, Rainer/Reulke, Kerstin, Die Digitalisierung der Energiewende – vom Smart Grid zur intelligenten Energieversorgung, in: Wittpahl, Volker (Hrsg.), Digitalisierung, Bildung/Technik/Innovation, Berlin/Heidelberg 2017, S. 141–150.

Noller, Stephan, Das Netz bedarf einer Algorithmen-Ethik, PinG 2013, S. 20.

O`Reilly, Tim, Open Data and Algorithmic Regulation, in: Goldstein, Brett/Dyson, Lauren (Hrsg.), Beyond Transparency, Open Data and the Future of Civic Innovation, San Francisco 2013, S. 289–301.

OECD, Estonia and Finland: Forstering strategic capacity across governments and digital services across borders, OECD Public Governance Review, Paris 2015.

OECD Public Governance and Territorial Development Directorate, Recommendation of the Council on Digital Government Strategies, Paris 2014.

Paal, Boris P./Pauly, Daniel (Hrsg.), Datenschutz-Grundverordnung, Kommentar, München 2016.

Pariser, Eli, The Filter Bubble, What the Internet is hiding from you, New York 2011.

Parma, David, Rechtsgrundlagen für den Einsatz von "Body-Cams", Eine kritische Bestandsaufnahme nach Einführung mehrerer Pilotversuche, DÖV 2016, S. 809–819.

Parycek, Peter/Edelmann, Noella (Hrsg.), CeDEM16, Conference for E-Democracy and Open Government, Krems 2016.

Pasquale, Frank, The black box society, The secret algorithms that control money and information, Cambridge 2015.

Penney, Jonathon W., Chilling Effects: Online Surveillance and Wikipedia Use, Berkeley Technology Law Journal 31 (2016), S. 117–182.

Pentland, Alex, Social physics, How good ideas spread – the lessons from a new science, London 2014.

Plum, Alexander, Methoden und Technologien des Web-Monitorings – ein systematischer Vergleich, in: Brauckmann, Patrick (Hrsg.), Web-Monitoring, Gewinnung und Analyse von Daten über das Kommunikationsverhalten im Internet, Konstanz 2010, S. 21–47.

President's Council of Advisors on Science and Technologie, Report to the President: Big Data and Privacy: A technological Perspective, Washington Mai 2014.

Raabe, Oliver/Wacker, Richard/Oberle, Daniel/Baumann, Christian/Funk, Christian, Recht ex machina: Formalisierung des Rechts im Internet der Dienste, Berlin/Heidelberg 2012.

Raabe, Oliver/Wagner, Manuela, Verantwortlicher Einsatz von Big Data, Ein Zwischenfazit zur Entwicklung von Leitplanken für die digitale Gesellschaft, DuD 2016, S. 434–439.

Rassia, Stamatina Th./Pardalos, Panos M. (Hrsg.), Cities for smart environmental and energy futures, Impacts on architecture and technology, Heidelberg 2014.

Rauner, Max/Schröder, Thorsten, Die Cogs kommen, Zeit Wissen 2015, S. 64–68.

Rehfeld, Dieter, Die Blockchain, Hat sie das Potenzial Gesellschaft und Wirtschaft neu zu gestalten?, in: Fadavian, Benjamin (Hrsg.), Transparente Staatstätigkeit, Hamburg 2016, S. 25–42.

Reichert, Ramón (Hrsg.), Big Data, Die Gesellschaft als digitale Maschine, Bielefeld 2014.

Reichwald, Julian/Pfisterer, Dennis, Autonomie und Intelligenz im Internet der Dinge, CR 2016, S. 208–212.

Richards, Neil, Intellectual privacy, Rethinking civil liberties in the digital age, Oxford/New York 2015.

Richter, Philipp, Big Data, Statistik und die Datenschutz-Grundverordnung, DuD 2016, S. 581–586.

Röber, Manfred (Hrsg.), Institutionelle Vielfalt und neue Unübersichtlichkeit – Zukunftsperspektiven effizienter Steuerung öffentlicher Aufgaben zwischen Public Management und Public Governance, Berlin 2012.

Roggan, Frederik, Der Einsatz von Video-Drohnen bei Versammlungen, Verdeckte und andere nicht erkennbare Datenerhebungen im Gewährleistungsbereich von Art. 8 I GG, NVwZ 2011, S. 590–595.

Rosenbach, Marcel/Stark, Holger, Der NSA-Komplex, Edward Snowden und der Weg in die totale Überwachung, München 2014.

Roßnagel, Alexander, Big Data – Small Privacy?, ZD 2013, S. 562–567.

– Anwendungsvorrang der eIDAS-Verordnung, Welche Regelungen des deutschen Rechts sind weiterhin für elektronische Signaturen anwendbar?, MMR 2015, S. 359–364.

Roßnagel, Alexander/Nebel, Maxi, (Verlorene) Selbstbestimmung im Datenmeer, Privatheit im Zeitalter von Big Data, DuD 2015, S. 455–460.

Sarunski, Maik, Big Data – Ende der Anonymität?, Fragen aus der Sicht der Datenschutzaufsichtsbehörde Mecklenburg-Vorpommern, DuD 2016, S. 424–427.

Schaar, Peter, Überwachung total, Wie wir in Zukunft unsere Daten schützen, Berlin 2014.

Schallbruch, Martin, Die EU-Richtlinie über Netz- und Informationssicherheit: Anforderungen an digitale Dienste, Wie groß ist der Umsetzungsbedarf der NIS-Richtlinie in deutsches Recht im Bereich digitaler Dienste?, CR 2016, 663–670.

Schlick, Jochen/Stephan, Peter/Loskyll, Matthias/Lappe, Dennis, Industrie 4.0 in der praktischen Anwendung, in: Bauernhansl, Thomas/Hompel, Michael ten/Vogel-Heuser, Birgit (Hrsg.), Industrie 4.0 in Produktion, Automatisierung und Logistik, Anwendung, Technologien und Migration, Wiesbaden 2014, S. 57–84.

Schliesky, Utz/Schulz, Sönke E. (Hrsg.), Transparenz, Partizipation, Kollaboration, Web 2.0 für die öffentliche Verwaltung, Kiel 2012.

Schlieter, *Kai,* Die Herrschaftsformel, Wie Künstliche Intelligenz und berechnet, steuert und unser Leben verändert, Frankfurt am Main 2015.

Schöpker, Ulrich, Fracht und Trailer immer in Echtzeit – volle Transparenz in der Supply Chain, in: Voß, Peter H. (Hrsg.), Logistik – eine Industrie, die (sich) bewegt, Strategien und Lösungen entlang der Supply Chain 4.0, Wiesbaden 2015, S. 55–62.

Schreiber, Marlene, Social Media Monitoring, PinG 2 (2014), S. 34–36.

Seeliger, Carsten W., Corporate Venturing in der Praxis, Rolle im Rahmen des Innovationsmanagements und Ansätze für ein Konzept zur Beurteilung und Steuerung seiner Erfolgsbeiträge, Wiesbaden 2004.

Sen, Evrim, Social Media Monitoring für Unternehmen, Anforderungen an das Web-Monitoring verstehen & die richtigen Fragen stellen, Köln 2011.

Sendler, Ulrich, Die Grundlagen, in: Sendler, Ulrich (Hrsg.), Industrie 4.0 grenzenlos, Berlin/Heidelberg 2016, S. 17–40.

Sendler, Ulrich (Hrsg.), Industrie 4.0 grenzenlos, Berlin/Heidelberg 2016.

Silver, David/Huang, Aja/Maddison, Chris J./Guez, Arthur/Sifre, Laurent et al., Mastering the game of GO with deep neural networks and tree search, Nature 2016, S. 484–489.

Singer, Natasha, White House Proposes Broad Consumer Data Privacy Bill, New York Times online vom 27.2.2015, http://www.nytimes.com/2015/02/28/business/white-house-proposes-broad-consumer-data-privacy-bill.html?_r=0 (20.3.2015).

Solmecke, Christian/Wahlers, Jakob, Rechtliche Situation von Social Media Monitoring-Diensten, ZD 2012, S. 550–555.

Sosna, Sabine, EU-weite elektronische Identifizierung und Nutzung von Vertrauensdiensten – eIDAS-Verordnung, Ein Überblick über die wichtigsten Inhalte und deren Konsequenzen für Unternehmen, CR 2014, S. 825–832.

Sprenger, Florian/Engemann, Christoph (Hrsg.), Internet der Dinge, Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt, Bielefeld 2015.

Städele, Julius Philipp, Völkerrechtliche Implikationen des Einsatzes bewaffneter Drohnen, Berlin 2014.

Stark, Rainer/Damerau, Thomas/Lindow, Kai, Industrie 4.0 – Digitale Neugestaltung der Produktentstehung und Produktion am Standort Berlin, Herausforderungen und Lösungsansätze für die digitale Transformation und Innovation, in: Sendler, Ulrich (Hrsg.), Industrie 4.0 grenzenlos, Berlin/Heidelberg 2016, S. 169–186.

Statistisches Bundesamt, Zufriedenheit der Bürgerinnen und Bürger in Deutschland mit behördlichen Dienstleistungen, Wiesbaden August 2015.

Steinbicker, *Jochen*, Der Staat der Wissensgesellschaft, Zur Konzeption des Staates in den Theorien der Wissensgesellschaft, in: Collin, Peter/Horstmann, Thomas (Hrsg.), Das Wissen des Staates, Geschichte, Theorie und Praxis, Baden-Baden 2014, S. 90–123.

Steinmann, Michael/Shuster, Julia/Collmann, Jeff/Matei, Sorin Adam et al., Embedding Privacy and Ethical Values in Big Data Technology, in: Matei et al. (ed.), Transparency in Social Media, Cham 2015, S. 277–301.

Stich, Volker/Adema, Jens/Blum, Matthias, Supply Chain 4.0: Logistikdienstleister im Kontext der vierten industriellen Revolution, in: Voß, Peter H. (Hrsg.), Logistik – eine Industrie, die (sich) bewegt, Strategien und Lösungen entlang der Supply Chain 4.0, Wiesbaden 2015, S. 63–76.

Swarat, Gerald/Haselbeck, Sebastian, Smart Country – Digitale Strategien für Regionen, Executive Summary, 2014, http://www.collaboratory.de/index.php?action=ajax&title=-&rs=SecureFileStore::getFile&f=/f/f4/SmartCountry_ExecutiveSummary.pdf (11.3.2016).

Symantec, 2016 Internet Security Threat Report, 2016, https://resource.elq.symantec.com/LP=2899?inid=symc_threat-report_istr_to_leadgen_form_LP-2899_ISTR21-report-main (24.11.2016).

Taeger, Jürgen (Hrsg.), Big Data & Co, Neue Herausforderungen für das Informationsrecht, Edewecht 2014.

Teich, Jürgen/Haubelt, Christian, Digitale Hardware/Software-Systeme, Synthese und Optimierung, 2. Aufl., Berlin/Heidelberg 2007.

Tesauro, Gerald/Gondek, David C./Lencher, Jonathan/Fan, James/Prager, John M., Analysis of Watson's Strategies for Playing Jeopardy!, JAIR 2013, S. 205–251.

The Boston Consulting Group, Earning Consumer Trust in Big Data: A European Perspective, 2015, https://www.bcgperspectives.com/content/articles/technology_strategy_digital_economy_earning_consumer_trust_big_data/ (23.11.2016).

The White House, Big Data: Seizing Opportunities, Preserving Values, Washington 2014.

Townsend, Anthony M., Smart cities, Big data, civic hackers, and the quest for a new utopia, New York 2013.

Tufekci, Zeynep, Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency, Colorado Technology Law Journal 2015, S. 203–218.

Tumin, Zachary/Fung, Archon, From Government 2.0 to Society 2.0, Pathways to Engagement, Collaboration and Transformation, Harvard 2011.

Turvey, Brent E., Criminal profiling, An introduction to behavioral evidence analysis, 4. Aufl., Amsterdam 2012.

U.S. Federal CIO Council, Government Use of Technology – Barriers, Opportunities, and Gap Analysis, Dezember 2012, https://cio.gov/wp-content/uploads/downloads/2012/12/Government_Mobile_Technology_Barriers_Opportunities_and_Gaps.pdf (24.11.2016).

UN Dept. of Economic & Social Affairs, Mobile Technologies for Responsible Government and Connected Services, Journal of E-Governance 2012, S. 61–62.

United Nations, UN E-Government Survey 2016, New York 2016.

VDE, VDE-Trendreport 2014 – Schwerpunkt: Smart Citys, Frankfurt am Main 2014.

Venzke-Caprese, Sven, Social Media Monitoring, Analyse und Profiling ohne klare Grenzen?, DuD 2013, S. 775–779.

Verenkotte, Christoph/Beutel, Rainer Christian/Bönder, Thomas (Hrsg.), Change Management, Baden-Baden 2015.

Voigt, Paul/Gehrmann, Mareike, Die europäische NIS-Richtlinie, Neue Vorgaben zur Netz- und IT-Sicherheit, ZD 2016, S. 355–358.

Voß, Peter H. (Hrsg.), Logistik – eine Industrie, die (sich) bewegt, Strategien und Lösungen entlang der Supply Chain 4.0, Wiesbaden 2015.

Voßkuhle, Andreas, § 1 – Neue Verwaltungsrechtswissenschaft, in: Hoffmann-Riem, Wolfgang/Schmidt-Assmann, Eberhard/Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. I, Methoden, Maßstäbe, Aufgaben, Organisation, 2. Aufl., München 2012, S. 1–63.

Walport, Mark, Distributed Ledger Technology, Beyond blockchain, London 2016.

Waseda University/International Academy of CIO, The 12th Waseda – IAC International e-Government Rankings Survey 2016 Report, Tokio 2016.

Wegener, Alexander, Intrapreneurship und Verwaltungskultur – zur Passfähigkeit von Modernisierungsansätzen in der deutschen Verwaltung, in: Heinrichs, Michael/Marschall, Katja (Hrsg.), Wege zu einer Intrapreneurship-orientierten öffentlichen Verwaltung, Dokumentation der Tagung Think Ahead – Move Forward vom 23. – 24. April 2008 in Güstrow, Bremen 2009, S. 223–228.

Welzer, Harald, Die smarte Diktatur, Der Angriff auf unsere Freiheit, Frankfurt am Main 2016.

Werkmeister, Christoph/Brandt, Elena, Datenschutzrechtliche Herausforderungen für Big Data, CR 2016, S. 233–238.

Werner, Andreas, Social Media – Analytics & Monitoring, Verfahren und Werkzeuge zur Optimierung des ROI, Heidelberg 2013.

Westkämper, Engelbert/Spath, Dieter/Constantinescu, Carmen/Lentes, Joachim (Hrsg.), Digitale Produktion, Berlin/Heidelberg 2013.

Widmann, Helmut (Hrsg.), Smart city, Viennese expertise based on science and research, Wien 2012.

Will, Martin, Wahlcomputer und der verfassungsrechtliche Grundsatz der Öffentlichkeit der Wahl, NVwZ 2009, S. 700–702.

Wirtz, Bernd W., Perspektiven des kommunalen E-Government, Studie für das Ministerium des Innern, für Sport und Infrastruktur des Landes Rheinland-Pfalz, Mainz 2015.

Witt, Thorsten/Freudenberg, Philipp, NIS-Richtlinie, Die Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit (NIS) in der Union, CR 2016, S. 657–663.

Wittpahl, Volker (Hrsg.), Digitalisierung, Bildung/Technik/Innovation, Berlin, Heidelberg 2017.

World Economic Forum, Global Risks 2014, Ninth Edition, Cologny 2014.

– The Global Information Technology Report 2016, Cologny 2016.

Wulf, Hans Markus/Burgenmeister, Clemens, Industrie 4.0 in der Logistik – Rechtliche Hürden beim Einsatz neuer Vernetzungs-Technologien, Anwendungsbeispiele und Lösungswege zu sechs zentralen Bereichen der Logistik, CR 2015, S. 404–412.

Zastrow, Volker, Wie Trump gewann, FAS vom 11.12.2016, S. 2 f.

Zech, Herbert, Daten als Wirtschaftsgut – Überlegungen zu einem „Recht des Datenerzeugers", CR 2015, S. 137–146.

Zentralverband Elektrotechnik- und Elektroindustrie e.V./Bundesverband der Energie- und Wasserwirtschaft, Smart Grids in Deutschland, Handlungsfelder für Verteilnetzbetreiber auf dem Weg zu intelligenten Netzen, Berlin 2012.

Zerfaß, Ansgar/Piwinger, Manfred (Hrsg.), Handbuch Unternehmenskommunikation, Wiesbaden 2007.

Ziems, Christian, Videoüberwachung bei Anhalte- und Kontrollvorgängen zur Eigensicherung der Polizeibeamten, Eine Analyse der Rechtslage in Brandenburg, Bremen, Hamburg, Hessen, Niedersachsen, Nordrhein-Westfalen und Rheinland-Pfalz, Berlin 2006.

Zweck, Axel/Holtmannspötter, Dirk/Braun, Matthias/Cuhls, Kerstin et al., Forschungs- und Technologieperspektiven 2030, Ergebnisband 2 zur Suchphase von BMBF-Foresight Zyklus II, Düsseldorf 2015.

Zweck, Axel/Holtmannspötter, Dirk/Braun, Matthias/Hirt, Michael et al., Gesellschaftliche Veränderungen 2030, Ergebnisband 1 zur Suchphase von BMBF-Foresight Zyklus II, Düsseldorf 2015.

FÖV DISCUSSION PAPERS

(institutseigene Reihe, über das Institut zu beziehen)

Nr. 1 *Gisela Färber*, Efficiency Problems of Administrative Federalism, März 2002.

Nr. 2 *Eberhard Bohne/Sabine Frenzel*, Formale und informale Ordnung des Zugangs zum Strommarkt, März 2003.

Nr. 3 *Dorothea Jansen*, Supporting Newly Founded Firms - Personal and Professional Networks, Juli 2003.

Nr. 4 *Hans Herbert von Arnim/Martin Schurig*, The Statute for Members of the European Parliament, September 2003; 2., unveränderte Auflage Oktober 2003.

Nr. 5 *Stefan Koch/Dieter Beck,* Verwaltungspsychologie: Begriffsbestimmung und Forschungsgebiete, September 2003.

Nr. 6 *Hans Herbert von Arnim,* Political finance: Checks and Abuses Current problems and new developments, Dezember 2003.

Nr. 7 *Hans Herbert von Arnim,* A salary of 9,053 Euros for Members of the European Parliament?, Januar 2004.

Nr. 8 *Dorothea Jansen,* Networks, social capital and knowledge production, Februar 2004.

Nr. 9 *Kira Baranova,* Föderative Steuersysteme und Wirtschaftsintegration zwischen Russland und Europa, Mai 2004.

Nr. 10 *Nils Otter,* Föderalismus und Staatsaufgaben – Ein Analyserahmen zum Vergleich alternativer Möglichkeiten der Aufgabenerteilung im föderativen Staat, September 2004.

Nr. 11 *Dorothea Jansen*, Governance of research networks, Oktober 2004.

Nr. 12 *Rainer Pitschas*, Looking Behind New Public Management. “New” Values of Public Administration and the Dimensions of Personnel Management in the Beginning of the 21st Century, Oktober 2004.

Nr. 13 *Helmut Klages,* Wie marode sind die Deutschen? Ein empirischer Beitrag zur Mentalitätsdebatte, Oktober 2004.

Nr. 14 *Arne Franz*, Der Kommunikationsprozess zwischen Verwaltung und Bürgern. Typisierungen, Charakteristika, Auswirkungen auf die Modellierung von Kommunikationsangeboten, November 2004.

Nr. 15 *Helmut Klages/Carmen Daramus/Kai Masser*, Vertrauensverlust in der Demokratie – Lösen Beteiligungsstrategien das Problem?, November 2004; 2., unveränderte Auflage März 2005.

Nr. 16 *Carl Böhret,* „Die Zukunft sieht alt aus" – Signale für die (Kommunal-)Politik aus der Übergangsgesellschaft, Dezember 2004.

Nr. 17 *Hans Herbert von Arnim/Martin Schurig,* Die Besoldung und Versorgung von Angehörigen des Öffentlichen Dienstes und die Ausgestaltung der Politikfinanzierung in der Europäischen Union. Ein Bericht über Verlauf und Ertrag eines Forschungsprojekts, Februar 2005.

Nr. 18 *Hans Herbert von Arnim/Martin Schurig,* Remuneration and Financial Provision for Members of the Civil Service and the Forms of Political Finance in the European Union. An Account of the Origin and Impact of a Research Project, März 2005.

Nr. 19 *Wilfried Rudloff,* Does science matter? Zur Bedeutung wissenschaftlichen Wissens im politischen Prozess. Am Beispiel der bundesdeutschen Bildungspolitik in den Jahren des „Bildungsbooms", April 2005.

Nr. 20 *Andreas Wald*, Zur Messung von Input und Output wissenschaftlicher Produktion. Daten und Ergebnisse einer Untersuchung auf der Ebene von Forschungsgruppen, Mai 2005.

Nr. 21 *Hans-Willy Hohn*, Forschungspolitische Reformen im kooperativen Staat. Der Fall der Informationstechnik, Speyer, Juli 2005.

Nr. 22 *Eberhard Bohne,* Kriterien und institutionelle Voraussetzungen des Bürokratieabbaus, Oktober 2005.

Nr. 23 *Eberhard Bohne,* EU and US Security Strategies from the Perspective of National and European Identities, Januar 2006.

Nr. 24 *Gisela Färber,* Haushaltsnotlagen in der deutschen Finanzverfassung – Ursachen, Abhilfe, Vermeidung –, Januar 2006.

Nr. 25 *Thomas König/Dirk Junge,* Die räumliche Modellierung von EU-Entscheidungssituationen. Akteure, Dimensionen, Interessen, Stimmengewichte und die Natur des Politikraums, Januar 2006.

Nr. 26 *Harald Dalezios,* Die regionale Inzidenz des deutschen Steuersystems. Theoretische Überlegungen zu Identifikation regionaler Unterschiede im Steueraufkommen und ihrer ökonomischen Determinanten, Februar 2006.

Nr. 27 *Jason Dedrick/Kenneth L. Kraemer,* Is Production Pulling Knowledge Work to China? A Study of the Global Computer Industry – Mit einer Einführung von Heinrich Reinermann, Februar 2006.

Nr. 28 *Sonja Bugdahn,* Reforming the World Trade Organization – a Choice between Effectiveness and Equity?, März 2006.

Nr. 29 *Andreas Knorr,* The Rail Liberalisation Index 2004 – A Critical Appraisal, März 2006.

Nr. 30 *Hermann Hill,* Nachhaltige Verwaltungsmodernisierung, Mai 2006.

Nr. 31 *Sebastian Wolf,* Maßnahmen internationaler Organisationen zur Korruptionsbekämpfung auf nationaler Ebene. Ein Überblick, Mai 2006.

Nr. 32 *Andreas Knorr*, Will 'Blacklists' Enhance Airline Safety?, Juni 2006.

Nr. 33 *Hans Herbert von Arnim/Regina Heiny/Stefan Ittner*, Korruption. Begriff, Bekämpfungs- und Forschungslücken, Mai 2006; 2., durchgesehene Aufl. November 2006; 3., unveränderte Aufl. März 2007.

Nr. 34 *Bernd Wirtz/Sebastian Lütje/Gerhardt Schierz,* Elektronische Beschaffung in der Öffentlichen Verwaltung – Eine Analyse der Implementierungsbarrieren von e-Procurement in Kommunen –, Juli 2006.

Nr. 35 *Hans Herbert von Arnim/Regina Heiny/Stefan Ittner,* Politik zwischen Norm und Wirklichkeit. Systemmängel im deutschen Parteienstaat aus demokratietheoretischer Perspektive, Oktober 2006; 2., durchgesehene Aufl. Dezember 2006; 3., unveränderte Aufl. März 2007.

Nr. 36 *Sven Barnekow/Dorothea Jansen,* Local utilities coping with the transformation of the energy market and their role for the diffusion of climate friendly technologies, November 2006.

Nr. 37 *Rudolf Fisch/Dieter Beck,* Organisationsgestaltung und Veränderungsmanagement. Die Organisationskultur als kritischer Erfolgsfaktor, November 2006.

Nr. 38 *Karoline Jahn,* Instrumente, Probleme und Erfolgsaussichten der Regulierung von Entgelten für den Netzzugang nach dem Energiewirtschaftsgesetz, Dezember 2006.

Nr. 39 *Dorothea Jansen,* Theoriekonzepte in der Analyse sozialer Netzwerke. Entstehung und Wirkungen, Funktionen und Gestaltung sozialer Einbettung, August 2007.

Nr. 40 *Gisela Färber/Harald Dalezios,* Aufkommenswirkungen und finanzielle Risiken des Optionsmodells – Eine kritische Analyse des Vorschlags des Saarlandes –, September 2007.

Nr. 41 *Dorothea Jansen/Sven Barnekow/Ulrike Stoll,* Innovationsstrategien von Stadtwerken – lokale Stromversorger zwischen Liberalisierungsdruck und Nachhaltigkeitszielen, September 2007.

Nr. 42 *Eberhard Bohne,* The politics of the ex ante evaluation of legislation, März 2008.

Nr. 43 *Olaf Bartz,* Regulierung des Privatschulwesens aus historischer Sicht und "Public Ecclesiastical Partnership", Mai 2008.

Nr. 44 *Bernd Wirtz/Sebastian Ullrich/Linda Mory,* e-Health – Akzeptanz der elektronischen Gesundheitskarte, Juni 2008.

Nr. 45 *Andreas Knorr/Alexander Eisenkopf,* Road Infrastructure PPPs in Germany: Why Did the *F-Modell* Fail? Two Case Studies, September 2008.

Nr. 46 *Alexander Eisenkopf/Andreas Knorr,* Transportation Infrastructure Planning in Europe – Pitfalls and Opportunities, Oktober 2008.

Nr. 47 *Jörg Bellmann/Andreas Eichinger/Alexander Eisenkopf/Andreas Knorr*, Urban Congestion Charging with an Environmental Component – The Central London Congestion Charge, Februar 2009.

Nr. 48 *Georg Krücken/Albrecht Blümel/Katharina Kloke,* Towards Organizational Actorhood of Universities: Occupational and Organizational Change within German University Administrations, Februar 2009.

Nr. 49 *Richard Heidler*, Erhebung, Visualisierung und mathematische Analyse sozialer Netzwerke – eine methodenorientierte Einführung in die sozialwissenschaftliche Netzwerkanalyse, Februar 2009.

Nr. 50 *Stefan Preller*, Die Zusatzversorgung im öffentlichen Dienst, Systemwechsel, Finanzierung und Ausgabenentwicklung, März 2009.

Nr. 51 *Andreas Glöckner*, “Modernising“ commercial accounting law in Germany – effects on public sector accrual accounting?, Juli 2009.

Nr. 52 *Andreas Knorr/André Heinemann*, Regional airport subsidies in the EU – the case for a more economic approach in the application of the EU’s state aid rules, August 2009.

Nr. 53 *Andreas Knorr/André Heinemann/Alexander Eisenkopf*, Germany’s Autobahn Toll for Heavy Goods Verhicles after four Years: Experiences and Perspectives, Dezember 2009.

Nr. 54 *Rahel Schomaker,* Bereitstellung netzgebundener Infrastruktur – Regulierung vs. Public Private Partnerships, Dezember 2009.

Nr. 55 *Holger Mühlenkamp*, Ökonomische Analyse von Public Private Partnerships (PPP) – PPP als Instrument zur Steigerung der Effizienz der Wahrnehmung öffentlicher Aufgaben oder als Weg zur Umgehung von Budgetbeschränkungen? –, Januar 2010.

Nr. 56 *Christian Bauer*, „Collaborative Governance“ – ein neues Konzept für die Regulierung der europäischen Strom- und Gasmärkte?, Januar 2010.

Nr. 57 *Andrei Király*, Whistleblower in der öffentlichen Verwaltung – Ihre Rechtsstellung bei der Korruptionsbekämpfung, März 2010.

Nr. 58 *Kathrin Przybilla,* The „WTOisation“ of the customs administration: Uniformity of the administration of law according to Article X:3 (a) GATT 1994 and ist implications for EU customs law, März 2010.

Nr. 59 *Eberhard Bohne*, Clash of Regulatory Cultures in the EU: The Liberalization of Energy Markets, Juni 2010.

Nr. 60 *Andreas Knorr/Jörg Bellmann/Rahel Schomaker*, International Trade Rules and Aircraft Manufacturing: Will the World Trade Organization Resolve the Airbus-Boeing Dispute?, August 2010.

Nr. 61 *Albrecht Blümel/Katharina Kloke/Georg Krücken*, Hochschulkanzler in Deutschland: Ergebnisse einer hochschulübergreifenden Befragung, September 2010.

Nr. 62 *Jonas Buche,* Die Europäisierung von Parteien und Parteisystemen – Eine Analyse am Beispiel Schwedens vom Beitritt zur EU 1995 bis zur Reichstagswahl 2006, September 2010.

Nr. 63 *Andreas Knorr/Andreas Lueg-Arndt/Barbara Lueg,* Airport Noise Abatement as an International Coordination Problem – The Case of Zurich Airport –, Januar 2011.

Nr. 64 *Gisela Färber*, Steuerhoheit von Gebietskörperschaften, März 2011.

Nr. 65 *Bernd W. Wirtz/Linda Mory/Robert Piehler*, Kommunales E-Government: Erfolgsfaktoren der Interaktion zwischen Stadtportalen und Anspruchsgruppen, März 2011.

Nr. 66 *Aron Buzogány/Andrej Stuchlik*, Paved with good intentions Ambiguities of empowering parliaments after Lisbon, Mai 2011.

Nr. 67 *Dennis Kutting*, Staatliche Verwaltungsarchitektur der 1950er Jahre in der Bundesrepublik. Forschungsstand, Problemstellung und Perspektiven, Juli 2011.

Nr. 68 *Ulrich Stelkens*, Art. 291 AEUV, das Unionsverwaltungsrecht und die Verwaltungsautonomie der Mitgliedstaaten, August 2011.

Nr. 69 *Gisela Färber*, Impacts of the Global Financial Crisis in a Federation: Evidence from Germany, Januar 2012.

Nr. 70 *Ulrich Stelkens/Hanna Schröder*, EU Public Contracts – Contracts passed by EU Institutions in Administrative Matters, März 2012.

Nr. 71 *Hans Herbert von Arnim*, Der Bundespräsident – Kritik des Wahlverfahrens und des finanziellen Status, März 2012.

Nr. 72 *Andreas Knorr*, Emissionshandel und Luftverkehr – Eine kritische Analyse am Beispiel des Europäischen Emissionshandelssystems (EU ETS), August 2012.

Nr. 73 *Gisela Färber/Julia Einsiedler*, Bürokratiekostenabbau im Steuerrecht: Ein Ansatz zur Vereinfachung des Steuerrechts?, August 2012.

Nr. 74 *Tim Jäkel*, Wer vergleicht seine Leistung, wenn er hohe Schulden hat? Empirische Evidenz aus den deutschen kreisfreien Städten, Mai 2013.

Nr. 75 *Holger Mühlenkamp*, From State to Market Revisited: More Empirical Evidence on the Efficiency of Public (and Privately-owned) Enterprises, Juli 2013.

Nr. 76 *Dirk Zeitz,* Bewertung der Einfacher-zu-Projekte unter dem Blickwinkel eines Vollzugsbenchmarking, September 2013.

Nr. 77 *Stefan Domonkos,* Making Increased Retirement Age Acceptable: The Impact of Institutional Environment on Public Preferences for Pension Reforms, Juni 2014.

Nr. 78 *Daniela Caterina,* Construing and managing the crisis: A cultural political economy perspective on the Italian Labour Market Reform 2012, Juni 2014.

Nr. 79 *Marco Salm,* Property Taxes in BRICS: Comparison and a First Draft for Performance Measurement, Oktober 2014.

Nr. 80 *Dirk Zeitz,* Der Antrag auf Wohngeld als Beispiel der Konsequenzen des Exekutivföderalismus auf den Erfüllungsaufwand, April 2015.

Nr. 81 *Marco Salm/Christian Schwab:* HRM and Change Management: Comparative Results from Three European Cities of Excellence, September 2015.

Nr. 82 *Marius Herr,* Das E-Government-Gesetz des Bundes – Ein verwaltungswissenschaftlicher Literaturbericht –, Oktober 2015.

Nr. 83 *Rahel M. Schomaker/Michael W. Bauer*, Experiments in Public Administration – some research, but no agenda, Juli 2016.

Nr. 84 *Dirk Zeitz*, Erprobung des Vollzugsbenchmarkings am Beispiel des Wohngeldes: Auswertung der Erhebungen, September 2016.

Nr. 85 *Mario Martini* unter Mitarbeit von *Saskia Fritzsche* und *Michael Kolain,* Digitalisierung als Herausforderung und Chance für Staat und Verwaltung. Forschungskonzept des Programmbereichs „Transformation des Staates in Zeiten der Digitalisierung“, Dezember 2016.

ISSN 1868-971X (Print)
ISSN 1868-9728 (Internet)