

Tanja Klenk  
Frank Nullmeier  
Göttrik Wewer *Hrsg.*

# Handbuch Digitalisierung in Staat und Verwaltung



Springer VS

---

# **Handbuch Digitalisierung in Staat und Verwaltung**

---

Tanja Klenk • Frank Nullmeier •  
Göttrik Wewer  
Hrsg.

# Handbuch Digitalisierung in Staat und Verwaltung

mit 22 Abbildungen und 12 Tabellen



Springer VS

*Hrsg.*

Tanja Klenk  
Universität der Bundeswehr Hamburg  
Hamburg, Deutschland

Frank Nullmeier  
Universität Bremen  
Bremen, Deutschland

Göttrik Wewer  
Lorenz-von-Stein-Institut für  
Verwaltungswissenschaften an der  
Christian Albrechts-Universität zu Kiel  
Kiel, Deutschland

ISBN 978-3-658-23667-0              ISBN 978-3-658-23668-7 (eBook)  
ISBN 978-3-658-31672-3 (print and electronic bundle)  
<https://doi.org/10.1007/978-3-658-23668-7>

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

Springer VS

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jedermann benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des jeweiligen Zeicheninhabers sind zu beachten.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag, noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Lektorat: Jan Treibel

Springer VS ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.

Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

---

## Vorwort

Wir schreiben diese Zeilen im Juni 2020. In Deutschland wird der Corona-Shutdown schrittweise beendet, über Ausmaß, Tempo und Vereinheitlichung der Öffnungsmaßnahmen wird heftig gestritten, Freude über die wiedererlangten Handlungsmöglichkeiten mischt sich mit der Angst vor einer zweiten Welle der Pandemie und den Sorgen über die wirtschaftlichen Folgen. Bei allen Auseinandersetzungen über den richtigen politischen Weg eint eine Aussage alle Positionen: Digitalisierung wird durch die Pandemie einen gewaltigen Schub erfahren. Sie hat die Kommunikations- und Arbeitsnetzwerke aufrechterhalten in einer Zeit, in der persönliche Kontakte verboten waren, sie hat sich bewährt und wird in Zukunft noch weiter ausgebaut und beschleunigt werden. Wo Defizite der Digitalisierung im öffentlichen Sektor sichtbar geworden sind, so beispielsweise in der digitalen Ausstattung und Kompetenz der Schulen, werden neue Programme aufgelegt und bestehende Programme erweitert und mit Vorrang versehen. Digitalisierung erfährt so einen großen Schub infolge der Pandemie: Alle ohnehin vorhandenen Tendenzen in Richtung Digitalisierung werden intensiviert.

Dieses Handbuch liefert die Übersicht zur Digitalisierung in Staat und Verwaltung unmittelbar vor der Corona-Pandemie. Was ist die Ausgangslage für die kommenden Bemühungen, welche Strategien wurden bisher verfolgt und welcher Grad an Digitalisierung ist in welchen Feldern bereits erreicht? Es ist die erste umfassende Bestandsaufnahme dieser Art für den öffentlichen Sektor mit Schwerpunkt auf den Stand in der Bundesrepublik Deutschland. In sechs thematischen Abteilungen und insgesamt 55 Artikeln haben wir versucht, Digitalisierung in den verschiedensten Feldern und Formen aufzugreifen und Ideen, Konzepte und Begrifflichkeiten zu erläutern, die zu Leitformeln des Nachdenkens über Digitalisierung im öffentlichen Raum geworden sind.

Der Plan zu diesem Buch ist anlässlich der Neuauflage des „Handbuchs zur Verwaltungsreform“ entstanden. Dort ließ sich das Megathema „Digitalisierung“ nicht in dem Ausmaß berücksichtigen, das angemessen gewesen wäre. Dieses Manko ließ den Entschluss reifen, der Digitalisierung in Staat und Verwaltung ein eigenes Handbuch zu widmen. Hier liegt der Fokus nicht so sehr darauf, mit welchen Konzepten, Instrumenten und Aktionsplänen Behörden besser werden können, sondern viel offener auf der Frage, wie sich Staat und Verwaltung auf das einzustellen haben, was manche eine „digitale Revolution“ nennen. Dazu einen aktu-

ellen Überblick über den Stand von Wissenschaft und Forschung, aber auch über die laufenden Diskussionen in Verwaltung und staatlichen Einrichtungen zu geben, ist der Sinn und Zweck dieses Handbuchs. Da wir mitten in diesem Prozess der Digitalisierung aller Lebensbereiche stecken und nicht bei allen Themen schon mehr oder weniger gesicherte Erkenntnisse vorliegen, können manche Antworten auf die Leitfrage nur vorläufig sein. In der Summe sollten die Artikel, die dieses Handbuch bietet, jedoch die Orientierung in der nun zu erwartenden Digitalisierungswelle erleichtern.

Ein solches Unternehmen ist nur durch die Zusammenarbeit einer großen Anzahl an Fachleuten aus den verschiedensten Sektoren erfolgreich durchzuführen. Die meisten Entwürfe für die Einzel-Artikel konnten auf einem Autoren-Workshop im Bremer „Haus der Wissenschaft“ diskutiert werden, von dem alle Beteiligten und auch das Gesamtwerk enorm profitiert haben. Wir danken allen Autor\*innen, die sich auf dieses Vorhaben und vor allem auf einen mehrstufigen Prozess der Qualitäts sicherung eingelassen haben, der ihnen einiges abverlangt hat, und hoffen, dass die Artikel durch dieses aufwändige redaktionelle Verfahren eine für Praktiker\*innen aus Verwaltung, Politik und staatlichen Einrichtungen ebenso hilfreiche Fassung erreicht haben wie für Leser\*innen aus dem Umfeld von Wissenschaft und Forschung.

Wir danken der Freien Hansestadt Bremen, der Universität Bremen und dem Bremer Haus der Wissenschaft dafür, dass sie den persönlichen Austausch und die intensiven Diskussionen möglich gemacht haben. Wir danken der Helmut-Schmidt-Universität der Bundeswehr Hamburg, der Universität Bremen und dem Deutschen Institut für Vertrauen und Sicherheit im Internet (DIVSI) für die Unterstützung der Tätigkeit der drei Herausgeber\*innen dieses Buches. Wir danken Frau PD Dr. Tanja Pritzlaff-Scheele für ihre wertvolle Unterstützung bei der Durchsicht der zahlreichen Quellenangaben und der Überprüfung der Literaturverzeichnisse auf Konsistenz. Dem Springer Verlag sei gedankt für die jederzeit gute und problemlose Zusammenarbeit. Dieser Dank gilt besonders Dr. Jan Treibel und Daniel Hawig.

Digitalisierung erfasst aber nicht nur Staat und Verwaltung, sie erfasst auch die Buchproduktion. Dieses Buch fasst den aktuellen Stand der Digitalisierung in Staat und Verwaltung mit Schwerpunkt auf der Bundesrepublik Deutschland zusammen, ist aber nur Teil eines fortlaufenden Prozesses der Dokumentation der Entwicklungen in Staat und Verwaltung.

Interessierte können auf die einzelnen Artikel auf verschiedenen Wegen zugreifen: über die Datenbank des Verlages, über das elektronische Gesamtwerk („eBook“) oder ab Herbst 2020 über das gedruckte Handbuch. In der Datenbank „Springer Reference“ sind nicht nur alle Artikel schon vor der Drucklegung verfügbar („Online first“), sondern auch für Bibliotheken, Forschungsinstitute und Hochschulen digital zugänglich. Für Suchmaschinen sind alle Artikel auch einzeln im Internet auffindbar.

Die digitale Version erlaubt, Artikel schneller zu überarbeiten, wenn es dafür Anlässe gibt, aber auch eine problemlose Ergänzung des Handbuchs um weitere Themen, wenn das sinnvoll erscheint. Anders als eine zweite gedruckte Auflage, über die erst nach einer gewissen Zeit nachzudenken wäre, ist das Werk also ein

„living document“, das ständig aktualisiert werden kann. Wir werden diese Überarbeitungen koordinieren und auch initiieren, wo dies erforderlich scheint. Anregungen der Leserinnen und Leser sind daher sehr erwünscht! Wenn etwa ein Thema zu kurz behandelt worden sein sollte oder wenn neue Entwicklungen Eingang in das Handbuch finden sollen, freuen wir als Herausgeber\*innen uns über entsprechende Hinweise und greifen diese gerne auf.

Hamburg, Bremen und Kiel im Juni 2020  
Die Herausgeber\*innen

---

# Inhaltsverzeichnis

<b>Teil I Einleitung .....</b>	<b>1</b>
<b>Auf dem Weg zum Digitalen Staat? .....</b>	<b>3</b>
Tanja Klenk, Frank Nullmeier und Göttrik Wewer	
<b>Teil II Spielarten der Digitalisierung .....</b>	<b>25</b>
<b>Daten, Metadaten, Interoperabilität .....</b>	<b>27</b>
Herbert Kubicek, Andreas Breiter und Juliane Jarke	
<b>Staatliche Regulierung durch Big Data und Algorithmen .....</b>	<b>41</b>
Sebastian Haunss und Lena Ulbricht	
<b>Künstliche Intelligenz .....</b>	<b>51</b>
Christian Djeffal	
<b>Blockchain in der öffentlichen Verwaltung .....</b>	<b>63</b>
Dieter Rehfeld	
<b>Offene Daten (Open Data) .....</b>	<b>75</b>
Herbert Kubicek und Juliane Jarke	
<b>Data mining für responsive Politikgestaltung .....</b>	<b>91</b>
Lena Ulbricht	
<b>Digitale Geodaten .....</b>	<b>101</b>
Lars Bernard und Stephan Mäs	
<b>Agent-based Modeling und Politikberatung .....</b>	<b>111</b>
Florian Eyert	
<b>Digitale Verhaltenspolitik .....</b>	<b>123</b>
Holger Straßheim	

<b>Teil III Leitbilder und normative Grundfragen .....</b>	<b>135</b>
<b>Agile Verwaltung .....</b>	<b>137</b>
Daniel Rölle	
<b>Digitale Kommunikationsinfrastrukturen .....</b>	<b>147</b>
Jeanette Hofmann	
<b>Digitale Transparenz .....</b>	<b>159</b>
Caroline Fischer und Sascha Kraus	
<b>Informationsfreiheits- und Transparenzgesetze .....</b>	<b>171</b>
Herbert Kubicek	
<b>Datenschutz .....</b>	<b>187</b>
Göttrik Wewer	
<b>Cybersicherheit .....</b>	<b>199</b>
Wolf J. Schünemann	
<b>Die datengesteuerte Verwaltung .....</b>	<b>209</b>
Basanta E. P. Thapa	
<b>Digitale Ungleichheiten und digitale Spaltung .....</b>	<b>219</b>
Norbert Kersting	
<b>Digitale Ethik .....</b>	<b>231</b>
Göttrik Wewer	
<b>Digitale Souveränität .....</b>	<b>241</b>
Julia Pohle	
<b>Dateneigentum .....</b>	<b>255</b>
Frank Nullmeier	
<b>Teil IV Demokratisches Regieren .....</b>	<b>265</b>
<b>E-Democracy .....</b>	<b>267</b>
Marianne Kneuer	
<b>Online-Partizipation von Bürgerinnen und Bürgern .....</b>	<b>279</b>
Stefan Marschall und Katrin Möltgen-Sicking	
<b>Elektronische Wahlen und Abstimmungen (Electronic Voting) .....</b>	<b>291</b>
Frank Bätge und Thomas Weiler	
<b>Liquid Democracy .....</b>	<b>301</b>
Julia Schwahnholz und Lavinia Zinser	
<b>Elektronische Gesetzgebung .....</b>	<b>313</b>
Axel Piesker, Patrick Schweizer und Carolin Steffens	

---

<b>Soziale Medien (Social Media)</b>	325
Mathias König und Wolfgang König	
<b>Civic Tech</b>	337
Stefan Baack, Christian Djeffal, Juliane Jarke und Hendrik Send	
<b>Co-Creation von digitalen öffentlichen Dienstleistungen</b>	347
Juliane Jarke und Herbert Kubicek	
<b>Mobilisierung von Recht durch Legal Technologies</b>	361
Britta Rehder und Katharina van Elten	
<b>Teil V Akteure und Institutionen</b>	371
<b>Digitale Agenda der Europäischen Kommission</b>	373
Göttrik Wewer	
<b>Diskurse der Digitalisierung und organisationaler Wandel in Ministerien</b>	383
Maximilian Hösl, Florian Irgmaier und Ronja Kniep	
<b>Digitalisierung der Ministerialverwaltung</b>	395
Nadin Fromm und Stefanie Vedder	
<b>IT-Planungsrat</b>	405
Hans-Henning Lühr	
<b>Digitalisierung auf Länderebene</b>	417
Alexander Berzel	
<b>Datenschutzaufsicht</b>	427
Magnus Römer und Lena Ulbricht	
<b>Digitalisierung von Verwaltungsleistungen in Bürgerämtern</b>	437
Christian Schwab, Jörg Bogumil, Sabine Kuhlmann und Sascha Gerber	
<b>Watchdog-Organisationen</b>	449
Karsten Mause	
<b>Teil VI Politikfelder und Instrumente</b>	461
<b>Digitalpolitik</b>	463
Samuel Greef	
<b>Die Auswirkung von Digitalisierung auf Bildungs- und Sozialpolitik</b>	475
Marius R. Busemeyer	
<b>Digitalisierung von Schule, Schulverwaltung und Schulaufsicht</b>	485
Sigrid Hartong, Andreas Breiter, Juliane Jarke und Annina Förschler	

<b>Digitalisierung im Gesundheitssektor</b>	495
Moritz E. Behm und Tanja Klenk	
<b>Smart Cities</b>	507
Felix Butzlaff	
<b>Digitale Polizeiarbeit</b>	517
Constantin Houy, Oliver Gutermuth, Sharam Dadashnia und Peter Loos	
<b>Der Staat als Hacker</b>	527
Martin Schallbruch	
<b>Der elektronische Personalausweis</b>	539
Lasse Gerrits, Martin Wirtz und Sebastian Hemesath	
<b>Digitale Betriebsprüfung</b>	553
Peter Fettke	
<b>Digitale Daseinsvorsorge</b>	565
Sönke E. Schulz	
<b>Koordination und Integration im E-Government</b>	575
Thurid Hustedt und Philipp Trein	
<b>Teil VII Personal, Organisation, Prozesse</b>	585
<b>Digitaler Organisationswandel</b>	587
Moritz Heuberger	
<b>E-Leadership</b>	599
Manuel Misgeld	
<b>E-Kompetenzen</b>	611
Nadine Ogonek, Michael Räckers, Steffen Gilge und Sara Hofmann	
<b>Folgen der Digitalisierung auf öffentliche Dienstleistungen</b>	623
Matthias Döring und Stephan Löbel	
<b>Standardisierter Datenaustausch</b>	633
Matthias Döring und Sebastian Noack	
<b>Digitale Archivpolitik</b>	645
Catharina Wasner und Niklaus Stettler	

---

## Autorenverzeichnis

**Stefan Baack** Weizenbaum Institut, Berlin, Deutschland

**Frank Bätge** Fachhochschule für öffentliche Verwaltung Nordrhein-Westfalen, Köln, Deutschland

**Moritz E. Behm** Fakultät für Wirtschafts- und Sozialwissenschaften, Helmut-Schmidt-Universität, Hamburg, Deutschland

**Lars Bernard** Professur für Geoinformationssysteme, TU Dresden, Dresden, Deutschland

**Alexander Berzel** Gesellschaftswissenschaften, Universität Kassel, Kassel, Deutschland

**Jörg Bogumil** Ruhr-Universität Bochum, Bochum, Deutschland

**Andreas Breiter** Universität Bremen und Institut für Informationsmanagement Bremen, Bremen, Deutschland

**Marius R. Busemeyer** Fachbereich Politik- und Verwaltungswissenschaft, Universität Konstanz, Konstanz, Deutschland

**Felix Butzlaff** Institut für Gesellschaftswandel und Nachhaltigkeit (IGN), Vienna University of Economics and Business, Wien, Österreich

**Sharam Dadashnia** Scheer GmbH, Saarbrücken, Deutschland

**Christian Djeffal** Munich Center for Technology in Society, Technische Universität München, München, Deutschland

**Matthias Döring** Department of Political Science and Public Management, University of Southern Denmark, Odense, Dänemark

**Florian Eyert** Weizenbaum-Institut für die vernetzte Gesellschaft/Wissenschaftszentrum Berlin für Sozialforschung, Berlin, Deutschland

**Peter Fettke** Universität des Saarlandes und Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI), Saarbrücken, Deutschland

**Caroline Fischer** Universität Potsdam, Potsdam, Deutschland

**Annina Förshler** Fakultät für Geistes- und Sozialwissenschaften, Helmut Schmidt Universität, Hamburg, Deutschland

**Nadin Fromm** Lehrstuhl für Public Management, Universität Kassel, Kassel, Deutschland

**Sascha Gerber** Fakultät für Sozialwissenschaft, Ruhr-Universität Bochum, Bochum, Deutschland

**Lasse Gerrits** Politikwissenschaft, Otto-Friedrich-Universität Bamberg, Bamberg, Deutschland

**Steffen Gilge** Sächsische Staatskanzlei, Dresden, Deutschland

**Samuel Greef** Gesellschaftswissenschaften, Universität Kassel, Kassel, Deutschland

**Oliver Gutermuth** Institut für Wirtschaftsinformatik (IWi), DFKI GmbH und Universität des Saarlandes, Saarbrücken, Deutschland

**Sigrid Hartong** Fakultät für Geistes- und Sozialwissenschaften, Helmut Schmidt Universität, Hamburg, Deutschland

**Sebastian Haunss** SOCIUM Forschungszentrum Ungleichheit und Sozialpolitik, Universität Bremen, Bremen, Deutschland

**Sebastian Hemesath** Otto-Friedrich-Universität Bamberg, Bamberg, Deutschland

**Moritz Heuberger** Lehrstuhl für Politikwissenschaft, Verwaltung und Organisation, Universität Potsdam, Potsdam, Deutschland

**Jeanette Hofmann** Politik der Digitalisierung, Wissenschaftszentrum Berlin für Sozialforschung, Berlin, Deutschland

**Sara Hofmann** Department of Information Systems, University of Agder, Kristiansand, Norwegen

**Maximilian Hösl** Wissenschaftszentrum Berlin für Sozialforschung, Berlin, Deutschland

**Constantin Houy** Institut für Wirtschaftsinformatik (IWi), DFKI GmbH und Universität des Saarlandes, Saarbrücken, Deutschland

**Thurid Hustedt** Hertie School, Berlin, Deutschland

**Florian Irgmaier** Weizenbaum-Institut für die vernetzte Gesellschaft/Wissenschaftszentrum Berlin für Sozialforschung, Berlin, Deutschland

**Juliane Jarke** ifib: Institut für Informationsmanagement Bremen GmbH, Universität Bremen, Bremen, Deutschland

**Norbert Kersting** Institut für Politikwissenschaft, Universität Münster, Münster, Deutschland

**Tanja Klenk** Fakultät für Wirtschafts- und Sozialwissenschaften, Helmut-Schmidt-Universität, Hamburg, Deutschland

**Marianne Kneuer** Institut für Sozialwissenschaften, Universität Hildesheim, Hildesheim, Deutschland

**Ronja Kniep** Wissenschaftszentrum Berlin für Sozialforschung, Berlin, Deutschland

**Mathias König** Institut für Kommunikationspsychologie und Medienpädagogik & Institut für Sozialwissenschaften, Universität Koblenz-Landau, Landau in der Pfalz, Deutschland

**Wolfgang König** Institut für Kommunikationspsychologie und Medienpädagogik & Institut für Sozialwissenschaften, Universität Koblenz-Landau, Landau in der Pfalz, Deutschland

**Sascha Kraus** Universität Potsdam, Potsdam, Deutschland

**Herbert Kubicek** ifib: Institut für Informationsmanagement Bremen GmbH, Universität Bremen, Bremen, Deutschland

**Sabine Kuhlmann** Universität Potsdam, Potsdam, Deutschland

**Stephan Löbel** SHI Stein-Hardenberg Institut GmbH, Berlin, Dänemark

**Peter Loos** Institut für Wirtschaftsinformatik (IWi), DFKI GmbH und Universität des Saarlandes, Saarbrücken, Deutschland

**Hans-Henning Lühr** Freie Hansestadt Bremen, Finanzressort, Bremen, Deutschland

**Stefan Marschall** Institut für Sozialwissenschaften, Heinrich-Heine-Universität Düsseldorf, Düsseldorf, Deutschland

**Stephan Mäs** TU Dresden, Dresden, Deutschland

**Karsten Mause** Institut für Politikwissenschaft, Universität Münster, Münster, Deutschland

**Manuel Misgeld** Deutsches Forschungsinstitut für öffentliche Verwaltung Speyer, Speyer, Deutschland

**Katrin Möltgen-Sicking** Fachhochschule für öffentliche Verwaltung NRW, Köln, Deutschland

**Sebastian Noack** Jinit[ Aktiengesellschaft für digitale Kommunikation, Berlin, Deutschland

**Frank Nullmeier** SOCIUM Forschungszentrum Ungleichheit und Sozialpolitik, Universität Bremen, Bremen, Deutschland

**Nadine Ogonek** Westfälische Wilhelms-Universität Münster, Münster, Deutschland

**Axel Piesker** Deutsches Forschungsinstitut für öffentliche Verwaltung, Speyer, Deutschland

**Julia Pohle** Politik der Digitalisierung, Wissenschaftszentrum Berlin für Sozialforschung, Berlin, Deutschland

**Michael Räckers** European Research Center for Information Systems, Westfälische Wilhelms-Universität Münster, Münster, Deutschland

**Britta Rehder** Fakultät für Sozialwissenschaften, Ruhr-Universität Bochum, Bochum, Deutschland

**Dieter Rehfeld** regio iT gesellschaft für informationstechnologie mbh, Aachen, Deutschland

**Daniel Rölle** Lehrstuhl für Verwaltungswissenschaft, Universität Konstanz, Konstanz, Deutschland

**Magnus Römer** European New School of Digital Studies, Stiftung Europa-Universität Viadrina, Frankfurt (Oder), Deutschland

**Martin Schallbruch** ESMT Berlin, Berlin, Deutschland

**Sönke E. Schulz** Schleswig-Holsteinischer Landkreistag, Kiel, Deutschland

**Wolf J. Schünemann** Institut für Sozialwissenschaften, Universität Hildesheim, Hildesheim, Deutschland

**Christian Schwab** Universität Potsdam, Potsdam, Deutschland

**Julia Schwanholz** Institut für Politikwissenschaft, Georg-August-Universität Göttingen, Göttingen, Deutschland

**Patrick Schweizer** Deutsches Forschungsinstitut für öffentliche Verwaltung, Speyer, Deutschland

**Hendrik Send** Alexander von Humboldt Institut für Internet und Gesellschaft, Berlin, Deutschland

Fachbereich Wirtschaft, Hochschule Anhalt, Bernburg, Deutschland

**Carolin Steffens** Deutsches Forschungsinstitut für öffentliche Verwaltung, Speyer, Deutschland

**Niklaus Stettler** Hochschule für Technik und Wirtschaft HTW Chur, Chur, Schweiz

**Holger Straßheim** Fakultät für Soziologie, Universität Bielefeld, Bielefeld, Deutschland

**Basanta E. P. Thapa** Fraunhofer-Institut für offene Kommunikationssysteme, Kompetenzzentrum Öffentliche IT, Berlin, Deutschland

**Philipp Trein** University of Lausanne, Lausanne, Schweiz

**Lena Ulbricht** Weizenbaum-Institut für die vernetzte Gesellschaft, Wissenschaftszentrum Berlin für Sozialforschung, Berlin, Deutschland

**Katharina van Elten** Fakultät für Sozialwissenschaften, Ruhr-Universität Bochum, Bochum, Deutschland

**Stefanie Vedder** Lehrstuhl für Public Management, Universität Kassel, Kassel, Deutschland

**Catharina Wasner** Hochschule für Technik und Wirtschaft HTW Chur, Chur, Schweiz

**Thomas Weiler** NRW Fortschrittskolleg Online-Partizipation, Fachhochschule für öffentliche Verwaltung NRW, Köln, Deutschland

**Göttrik Wewer** Lorenz-von-Stein-Institut für Verwaltungswissenschaften an der Christian Albrechts-Universität zu Kiel, Kiel, Deutschland

**Martin Wirtz** Stadt Aachen, Aachen, Deutschland

**Lavinia Zinser** Institut für Politikwissenschaft, Georg-August-Universität Göttingen, Göttingen, Deutschland

---

# **Teil I**

## **Einleitung**



---

# Auf dem Weg zum Digitalen Staat?

## Stand und Perspektiven der Digitalisierung in Staat und Verwaltung

Tanja Klenk, Frank Nullmeier und Göttrik Wewer

### Inhalt

1	Digitalisierung – ein vielschichtiges Phänomen .....	4
2	Auf dem Weg in ein digitales Zeitalter .....	5
3	Formen der Digitalisierung .....	7
4	Gute Technik, böse Technik? Zwischen Utopien und Dystopien .....	10
5	Staatlichkeit im digitalen Zeitalter .....	12
6	Umrisse einer digitalen Verwaltung .....	14
7	Konzeption und Gliederung des Handbuchs .....	15
8	Eine erste Zwischenbilanz .....	19
	Literatur .....	22

---

### Zusammenfassung

Digitalisierung ist ein vielschichtiges Phänomen – auch und gerade, was die Digitalisierung in Staat und Verwaltung betrifft. Der Beitrag führt ein in die Diskussion über Staatlichkeit im digitalen Zeitalter, unterscheidet mit basaler und starker Digitalisierung zwei Formen des Veränderungsprozesses und beschreibt die Konturen einer digitalen Verwaltung. In der öffentlichen Diskussion schwankt die Bewertung von Digitalisierung zwischen Utopie und Dystopie.

---

T. Klenk (✉)

Fakultät für Wirtschafts- und Sozialwissenschaften, Helmut-Schmidt-Universität, Hamburg,  
Deutschland

E-Mail: [tanja.klenk@hsu-hh.de](mailto:tanja.klenk@hsu-hh.de)

F. Nullmeier

SOCIUM Forschungszentrum Ungleichheit und Sozialpolitik, Universität Bremen, Bremen,  
Deutschland

E-Mail: [frank.nullmeier@uni-bremen.de](mailto:frank.nullmeier@uni-bremen.de)

G. Wewer

Lorenz-von-Stein-Institut für Verwaltungswissenschaften an der Christian Albrechts-Universität zu  
Kiel, Kiel, Deutschland

E-Mail: [g.wewer@bvdp.de](mailto:g.wewer@bvdp.de)

Der Beitrag zieht vor diesem Hintergrund eine kritische Bilanz des bisherigen Stands der Digitalisierung in Staat und Verwaltung.

### Schlüsselwörter

Digitalisierung (starke und schwache) · Digitaler Staat/Digitale Verwaltung · Datengetriebene Verwaltung · Electronic Government · Öffentliche Verwaltung

## 1 Digitalisierung – ein vielschichtiges Phänomen

Digitalisierung ist in aller Munde. Die Wirtschaft wandelt sich zur Industrie 4.0, immer neue Digitalisierungsprogramme werden von Parteien, Verbänden und *Think Tanks* auf den politischen Markt geworfen und Ängste wie Hoffnungen verbinden sich mit diesem Begriff. Wie bereits beim Begriff Globalisierung werden auch hier sehr viele verschiedene Entwicklungen in einer Vokabel gebündelt. Digitalisierung wird oft zu einem Etikett, das fast alle größeren Veränderungen im Übergangsfeld von Technik und Gesellschaft umschließt. Digitalisierung erfasst alle Bereiche der Gesellschaft, ist keineswegs auf einige Branchen beschränkt, sondern vollzieht sich in allen Teilen der Wirtschaft, aber auch darüber hinaus, sie verändert Politik, Kommunikation und Medien, Kultur, Wissenschaft, Erziehung, und unsere gesamte Lebensweise. Kein Bereich ist heute mehr von Digitalisierung irgendwelcher Art ausgespart.

Dieses Handbuch widmet sich nur einem bestimmten Ausschnitt dieses Entwicklungsprozesses, nämlich der Digitalisierung in Staat und Verwaltung. Es will für diesen Bereich differenziert beschreiben und analysieren, was unter Digitalisierung verstanden wird, welche Veränderungen in der Einführung digitaler Medien bereits erfolgt sind, welche Vorhaben ins Auge gefasst sind und wie dies Staat und Verwaltung selbst umgestalten wird.

Digitalisierung in Staat und Verwaltung bildet nur einen Teilbereich der weit umfassenderen Digitalisierung der Politik. Die Analyse der Digitalisierung aller Bereiche der Politik ist eine lohnende Aufgabe: Parteien, Verbände, zivilgesellschaftliche Organisationen und Initiativen erleben deutliche Veränderungen durch neue Wege der Digitalisierung, gerade im Bereich der sozialen Medien. Organisationszentrierte Politikmodelle werden von Kampagnenpolitik abgelöst, neue Formen der Wahlkampfgestaltung werden sichtbar. Der Kontakt zwischen politisch Engagierten und politischen Eliten wird von digitalen Kommunikationsformen bestimmt, man kann sogar eine parteiartige Organisation auf eine Internetplattform gründen. Diese Prozesse sind in sich aber so vielfältig und umfangreich, dass ihre Untersuchung ein eigenes Handbuch wert wäre. Dieses Handbuch beschränkt sich bewusst auf Staat und Verwaltung.

Zur öffentlichen Verwaltung zählen nicht nur Ämter und Behörden, sondern auch Schulen und Hochschulen, Polizei und Gerichte, Krankenhäuser und Bundeswehr. Dass die digitale Transformation im gesamten Staat im gleichen Maße und mit ähnlichen Veränderungsschritten erfolgt, ist weder zu erwarten noch zwingend

notwendig. Für den Justizvollzug sind sicher andere Konzepte erforderlich als für Klassenräume oder Hörsäle und die Digitalisierung der Parlamente wird andere Wege gehen als die administrative Koordination zwischen den Ländern. Digitalisierung ist also auch in Staat und Verwaltung ein sehr vielschichtiges Geschehen, das es differenziert zu betrachten gilt. Die Breite dieser Entwicklung aufzuzeigen und die Varianz innerhalb dessen, was Digitalisierung genannt wird, näher herauszuarbeiten, ist eines der wesentlichen Anliegen dieses Handbuchs.

---

## 2 Auf dem Weg in ein digitales Zeitalter

Der Beginn des digitalen Zeitalters wird oft auf das Jahr 2002 datiert, in dem es erstmals möglich gewesen sein soll, mehr Informationen digital zu speichern als analog aufzubewahren (Hilbert und López 2011). Seither ist die Datenmenge, die auf dem Globus jährlich erzeugt wird, förmlich explodiert (Burke 2015). Nach einer Faustregel verdoppelt sich das Volumen alle zwei Jahre. Von 2016 bis 2025 soll es sich auf 163 Zettabyte (eine Zahl mit 21 Nullen) verzehnfachen, was ein jährliches Wachstum von rund dreißig Prozent bedeuten würde. Der größte Anteil dieser Daten soll dann nicht mehr von privaten Nutzern des Internets erzeugt werden, sondern von Unternehmen, deren Anteil von dreißig auf sechzig Prozent steigen soll. Die Anfänge der Digitalisierung reichen weit in das 20. Jahrhundert zurück. Frühe Versuche, der Entwicklung einen Namen zu geben, lauteten „Computerzeitalter“, „Informationsgesellschaft“ und „Wissensgesellschaft“, aber auch „Netzwerkgesellschaft“ (Manuel Castells). Das „Internet der Dinge und der Dienste“, in dem praktisch alles mit allem vernetzt ist, Menschen und Maschinen, Produkte und Services, stellt allerdings einen technologischen Quantensprung dar, der es recht fertigen könnte, nun von einem „digitalen Zeitalter“ zu sprechen.

Digitalisierung bedeutet zunächst nicht mehr als die Umwandlung von analogen Werten in digitale Formate. Analog sind Signale, die stufenlos, unterbrechungsfrei, also kontinuierlich und damit beliebig genau sein können. Digitale Signale können nur einen diskreten, d. h. abgegrenzten und gestuften Vorrat an Werten annehmen. Die Werte werden auch nur zu periodischen Zeitpunkten erfasst, also diskontinuierlich. Durch die Begrenzung der Werte wird aber Vergleichbarkeit und Übertragbarkeit in einer Welt der Daten möglich. Man kann Informationen in digitaler Form weit einfacher wieder- und weitergeben, speichern, lesen, komprimieren, weiterverarbeiten, durchsuchen und verteilen. Werden elektronische Medien mit digitaler Codierung eingesetzt, spricht man von der Nutzung digitaler Medien. Die Nutzung von digitaler Informations- und Kommunikationstechnologie hat mittlerweile alle Lebensbereiche durchdrungen, so dass von einer Informations- oder Datengesellschaft gesprochen wird, in der Daten allein deshalb erzeugt werden, um daraus neue Daten zu generieren, oder Daten anfallen, weil anderswo bereits Daten angefallen sind. Die mit erheblichem Tempo laufenden technologischen Innovationen ermöglichen es, mit zunehmender Kapazität Daten zu übertragen, sie zu speichern, mit ihnen zu rechnen und zu steuern. Stand Digitalisierung im ausgehenden 20. Jahrhundert für eine *Automatisierung* von Prozessen, so geht es heute mittlerweile um

eine *Autonomisierung* von Prozessen. Es geht nicht mehr nur darum, dass automatische Einrichtungen selbstständig Aufgaben verrichten, die repetitiv und in bestimmten Routinen durchzuführen sind. Es geht vielmehr um technische Systeme, die selbstständig lernen und selbstständig Lösungen entwickeln. Solche Systeme der künstlichen Intelligenz (KI) werden in der Verwaltung zum Beispiel verwendet, um öffentliche Räume zu überwachen oder um Risiken und Gefahren vorherzusagen. Künstliche Intelligenz (*artificial intelligence*) wird auch genutzt, um zukünftiges Verhalten zu simulieren und damit Entscheidungs- und Handlungsmöglichkeiten zu eruieren (*agent-based modeling*). Die Systeme künstlicher Intelligenz lernen durch die „künstliche“ Generierung von Wissen und Erfahrung. Dieses sogenannte *machine learning* erfolgt durch die systematische Auswertung und Verarbeitung einer beständig wachsenden Datenflut, die sich sowohl aus routinemäßig erhobenen Daten (z. B. von Krankenversicherungen, Mobilfunk- oder Kreditkartenunternehmen) als auch aus unstrukturierten Daten, die zum Beispiel in sozialen Netzwerken entstehen, speist (*big data*).

Will man diese Entwicklungen zu einer Definition zusammenfassen, bietet sich vielleicht folgende Formulierung an:

Digitalisierung bezeichnet den Entwicklungsprozess, in dem gesellschaftliche Vorgänge auf digitale Kommunikation und Informationsvermittlung sowie auf die Nutzung digitalen Medien umgestellt werden und dadurch zunehmend automatisiert und autonomisiert erfolgen.

Der Begriff der Digitalisierung hat sich jedoch längst von dem ursprünglichen Thema der Umstellung von analogen auf digitale Signale gelöst und wird mittlerweile in einem viel breiteren Sinne verwendet. So werden mit Digitalisierung heute insbesondere auch die durch die Nutzung digitaler Medien ausgelösten *Effekte* in Politik und Verwaltung, Wirtschaft und Zivilgesellschaft beschrieben. Da Technologie hier in ihren Anwendungen besteht, ist die Gesamtheit der Neugestaltungen gesellschaftlicher Kommunikation als Digitalisierung zu betrachten. Es geht nicht nur um digitale Informationsspeicherung, sondern um die Sammlung von Daten zur politischen und wirtschaftlichen Steuerung als Teil eines Digitalen Staates und eines „data-centric and data-intensive capitalism“ oder kurz Datenkapitalismus (Morozov 2015).

Zu diesen Effekten gehört beispielsweise ein Strukturwandel der Öffentlichkeit, infolge dessen sich die Vorstellungen von und der Umgang mit Transparenz, Datenschutz, Zugang zu Informationen, Agenda Setting etc. einschneidend verändert haben (Wewer 2014). Die digitale Öffentlichkeit ist im Vergleich zur prädigitalen Öffentlichkeit nicht nur durch neue Kommunikationsmedien (*E-mail, twitter, social media* etc.), sondern auch durch ein grundlegend verändertes Kommunikationsverhalten geprägt. Tradierte Vorstellungen von ‚Öffentlich‘ und ‚Privat‘ sind hinfällig geworden und die Grenzziehung zwischen beiden Bereichen ist neu auszuhandeln.

Zu den Effekten der Digitalisierung gehört aber auch der Wandel der Arbeit. In der Arbeitswelt manifestierte sich die Digitalisierung zunächst vor allem durch Computerisierung, d. h. als Rationalisierung von Arbeitsprozessen durch elektronische Datenverarbeitung. Ein frühes Beispiel aus dem Bereich der öffentlichen Verwaltung ist die EDV-basierte Rationalisierung in deutschen Finanzbehörden. Digitalisierung wird dabei immer unter dem Gesichtspunkt der Wirkung auf die

Anzahl und Qualität der Arbeitsplätze betrachtet: In welchem Umfang gefährdet Digitalisierung Arbeitsplätze durch Automatisierung und in welchem Maße schafft sie Arbeitsplätze über neue Geschäftsmodelle und neue digitale Produkte? Welches der beiden Szenarien – Arbeitsplatzvernichtung oder Digitalisierung als Jobmotor – eintreffen wird, ist in Politik und Wissenschaft höchst umstritten (Frey und Osborne 2013; Dengler und Matthes 2015). Digitalisierung verändert die Arbeitswelt zudem in qualitativer Hinsicht: andere Qualifikationen sind verlangt, räumliche und zeitliche Restriktionen verlieren an Bedeutung, Digitalisierung macht neue Arbeitsformen und neue Varianten von Arbeitsteilung möglich, verändert Betriebsstrukturen und verlangt von Führungskräften ein verändertes Führungsverhalten.

Schließlich hat Digitalisierung auch Auswirkungen auf den privaten Raum und wandelt hier Formen der sozialen Interaktion, der privaten Lebensführung, des Lernens oder des sozialen Engagements recht einschneidend (Peinl 2018). Der Wandel der privaten Lebensführung wiederum hat Rückwirkungen auf Staat und Verwaltung, verändern sich doch zum Beispiel die Erwartungshaltungen der Bürger\*innen, was die Erreichbarkeit, Zugänglichkeit und Transparenz von öffentlichen Einrichtungen betrifft.

---

### 3 Formen der Digitalisierung

Unter „Digitalisierung in Staat und Verwaltung“ sind zunächst alle Formen öffentlichen Handelns zu verstehen, die sich digitaler Technologien bedienen. Das reicht von elektronischen Formularen über automatisierte Bescheide bis zur Unterstützung durch Algorithmen bei Entscheidungen, ob Straftäter vorzeitig entlassen werden sollen. Wer abschätzen möchte, ob sich dadurch staatliches Handeln, Staat und Verwaltung als solche grundsätzlich verändern, braucht allerdings genauere Kriterien, welcher Grad und welche Form digitaler Transformation angestrebt wird, bereits erreicht ist oder sich in Zukunft ergeben wird. Prinzipiell lassen sich zwei Formen oder Stufen der Digitalisierung unterscheiden:

- Eine *basale (oder schwache) Digitalisierung* meint die Bereitstellung von öffentlichen Dienstleistungen und die Durchführung von politischen Prozessen unter Nutzung digitaler Formate und Medien. Hier besteht die Digitalisierung allein in der Umwandlung analoger in digitale Informationen, darin, dass Akten elektro-nisch geführt oder kommunale Dienste auch *online* angeboten werden. Das elektronische Regieren und Verwalten (*Electronic Government*) ist nur eine erste Möglichkeit der digitalen Transformation von Staat und Verwaltung. Bevor sie elektronisch abgebildet werden, sollen die Arbeitsprozesse zwar daraufhin über-prüft werden, ob sie optimiert werden können, aber solange das den Charakter von Staat und Verwaltung und die Art und Weise staatlichen Handelns nicht grundlegend verändert, ist Digitalisierung kein wesentlicher Wandel. So wie man einst Telegraf, Telefon und Telefax genutzt hat, um seine Aufgaben zu erledigen, gilt das heute eben für Personal Computer, das Internet, die „*Social Media*“ und die *Cloud*.

- 
- Von *starker* Digitalisierung lässt sich sprechen, wenn nicht nur bekannte Prozesse in Staat und Verwaltung um digitales Prozessieren ergänzt oder darauf umgestellt werden, sondern wenn sich öffentliches Handeln generell und speziell administrative Prozesse durch den Einsatz digitaler Technologien in ihrer Struktur wesentlich verändern. Wesentlich soll dabei heißen, dass entweder das Produkt öffentlichen Handelns nicht mehr dasselbe ist (*output*), die Voraussetzungen der Leistungserstellung sich grundlegend verändern (*input*) oder der Prozess von anderen Akteuren und Verfahren bestimmt wird (*throughput*). Starke Digitalisierung erzeugt einen Digitalen Staat und eine Digitale Verwaltung. Dieser *Digitale Staat* ist ein daten-gesteuerter, manche sagen: ein daten-getriebener Staat („*data-driven*“); die *Digitale Verwaltung* eine daten-gesteuerte Verwaltung. Die Ausrichtung öffentlichen Handelns an Rechtsnormen würde überlagert durch die Steuerung des öffentlichen Lebens auf der Grundlage von Datenanalysen (*Big Data, Data Analytics*). Nicht *Electronic Government*, sondern *Smart Government*. Dass ein solcher Ansatz, von dem sich manche ein stärker „evidenz-basiertes“, was heißt: datenbasiertes, staatliches Handeln erhoffen, nicht nur mehr Effektivität und Effizienz verspricht, sondern eigene Probleme, Widersprüche und Grenzen aufweist, steht auf einem anderen Blatt. In ihm steckt ein technokratisches Politik-, Staats- und Verwaltungsmodell, über das zu diskutieren wäre.

Mit diesen zwei Stufen soll eine qualitative Einordnung der Digitalisierungsprozesse in Staat und Verwaltung möglich werden. An dem einen Ende einer Skala wäre ein Zustand einzutragen, bei dem zwar die Umstellung auf digitale Formate erfolgt, aber ohne grundlegende Veränderungen der Abläufe und Strukturen. Diesem stände das Bild eines Digitalen Staates gegenüber. Ein *Digitaler Staat* wäre ein Staat, dessen Struktur durch Digitalisierung deutlich anders wäre, sowohl in den Organisationsstrukturen als auch bei den Prozessabläufen, in der Zuschneidung der öffentlichen Aufgaben und Politikfelder, im Verhältnis von öffentlicher und privater Aufgabenwahrnehmung sowie in den Beziehungen zu den Bürger\*innen (als Wähler\*innen, als Betroffene staatlicher Aufgabenwahrnehmung oder als Antragsteller\*innen und Klienten staatlicher Dienstleistungen). Zu einer solchen Neugestaltung würde auch eine Verschiebung des Wertesystems gehören, an dem sich öffentliches Handeln orientiert. Ein Digitaler Staat würde das Gefüge von Freiheit, Gleichheit, Gerechtigkeit und Solidarität, Inklusion und Nachhaltigkeit mindestens deutlich verschieben, wenn nicht neue Wertekategorien einführen und starke Umdeutungen tradierter Werte und Kriterien des Staatshandelns mit sich bringen.

Digitale Staatlichkeit kann den demokratischen Rechts- und Sozialstaat, wie er für die Bundesrepublik gilt, in Frage stellen. Während man bisher mit statistischen Durchschnittsgrößen operieren musste, wenn staatliche Programme konzipiert werden sollten, kann der Einzelne heute mit Echtdaten beschrieben werden. In der „granularen Gesellschaft“, wie Christoph Kucklick die doppelte Auflösung überkommener Gewissheiten genannt hat, kann die Wirklichkeit immer feinkörniger erfasst werden. „Zum einen die digitale Hochauflösung von uns Menschen und all den Phänomenen, die uns umgeben. Zum anderen aber auch die Auflösung jener

Institutionen, die sich in einer grobkörnigen Welt entwickelt haben und die nun nicht mehr mithalten können und hinderlich werden“ (Kucklick 2015, S. 14 f.). Dazu zählt er unter anderem das Rechtssystem, die Demokratie und den Sozialstaat. Das deckt sich mit Positionen, wonach es sich bei der Demokratie um eine „veralte Technologie“ handelt.

Für Politik- und Verwaltungswissenschaft werden soziotechnische Veränderungen dann besonders interessant, wenn Sensoren, Algorithmen, künstliche Intelligenz und anderes zu einem „anderen Staat“ und zu einer „anderen Verwaltung“ führen, also eine starke Form der Digitalisierung erfolgt. Wenn diese gegeben ist, wird die Frage der Bewertung, welches Ausmaß der Digitalisierung das richtige sei, besonders wichtig. Wie das Ausmaß der Digitalisierung in Staat und Verwaltung aber bewertet wird, hängt entscheidend von der Sichtweise ab, die eine Beobachter\*in einnimmt.

Eine erste Sichtweise ist allein an der Wirksamkeit öffentliches Handeln interessiert, sie ist *effektivitätsorientiert*. Sie hebt die Potenziale digitaler Technologien hervor, fragt vor allem danach, welche davon für die (bessere, optimale) Erfüllung von öffentlichen Aufgaben und Verfahren genutzt werden können. Kriterium in der Bewertung des Digitalisierungsniveaus in Staat und Verwaltung ist dann, ob öffentliche Aufgaben oder Verfahren durch Digitalisierung – in Bezug auf tradierte Maßstäbe – besser geworden sind bzw. besser werden können. Man kann aber bereits etwas stärker technologieorientiert fragen, ob die Potenziale der Digitalisierung umfassend ausgeschöpft worden sind oder nur ein Teilbereich der digitalen Technologien für die Verbesserung der staatlichen Aufgabenwahrnehmung eingesetzt wurde. Das kann auch für das Staat-Bürger\*innen-Verhältnis gelten. Im demokratischen Sinne wäre eine Effektivitätssteigerung genau dann gegeben, wenn digitale Medien zur stärkeren Partizipation der Bürger\*innen und zur erhöhten Kontrollierbarkeit staatlichen Handelns führen.

Eine *technologiezentrierte* Sichtweise fragt nach der Einführung jener Digitalisierungsformen, die auch in fortgeschrittenen Wirtschaftssektoren eingesetzt werden. Eine erfolgreiche Digitalisierung von Staat und Verwaltung ist dann jene, die alle in der Wirtschaft verwendeten Instrumentarien auch nutzt – letztlich unabhängig davon, ob damit Verbesserungen in der Erfüllung öffentlicher Aufgaben verbunden sind oder nicht. Wenn Staat und Verwaltung nicht selbst Roboter, Algorithmen und künstliche Intelligenz nutzen, um ihre Arbeit zu optimieren, dann drohen sie weiter hinter Wirtschaft und Gesellschaft zurückzufallen – und es wird ihnen auch an Erfahrung und Urteilskraft mangeln, bestimmte Entwicklungen überhaupt noch kompetent einschätzen und begleiten zu können. Eine stark Zurückbleibende Digitalisierung der öffentlichen Hand lässt die staatliche Steuerungs- und Regulierungsfähigkeit wahrscheinlich weiter sinken. Umgekehrt muss eine Entwicklung, bei der Staat und Verwaltung in der digitalen Transformation nicht zu den Vorreitern, sondern zu den Nachzüglern gehören, kein Nachteil sein: Wer nicht immer gleich auf der neuesten Modewelle mitschwimmt, zahlt vielleicht weniger Lehrgeld. Nicht alles, was technisch möglich ist, ist wirklich sinnvoll.

In der ersten Sichtweise ist eine „selektive“ Nutzung von Digitalisierungstechnologien mitgedacht, in der zweiten nicht. Selektiv heißt, dass in Staat und Verwaltung

---

nur jene Formen der Digitalisierung aufgegriffen werden sollten, die eine Verbesserung der Aufgabenerfüllung darstellen. Andere Digitalisierungsformen können aber auch ungenutzt bleiben, weil nicht erkennbar ist, wie sie zu einer Verbesserung der Aufgabenerledigung führen sollten. Die zweite Perspektive dagegen hält jede Nachahmung und Übernahme anderweitig erfolgter Digitalisierung *per se* für einen Modernisierungsschritt, der es wert ist, implementiert zu werden.

Denkbar wäre aber auch eine dritte Perspektive, die nach gesellschaftlich-politischen Lösungen sucht, die in Staat und Verwaltung unter Nutzung digitaler Medien und Formate gefunden werden. Können Staat und Verwaltung vielleicht Vorreiter gesellschaftlicher Innovationen sein, die auf dem Einsatz digitalisierter Abläufe beruhen und neue Beziehungen zwischen Bürger\*innen und dem politischen Gemeinwesen erzeugen? Das wäre eine *innovationszentrierte* Sicht auf Digitalisierung von Staat und Verwaltung.

In der Analyse sollte man daher nicht von einer technologischen Determination des Geschehens ausgehen, dagegen sprechen auch die großen Unterschiede in der digitalen Ausgestaltung öffentlicher Verwaltungen zwischen einzelnen Nationalstaaten trotz des gleichen technologischen Standes in diesen Ländern. Es bedurfte sozialer Voraussetzungen, damit Internet und digitale Medien ihre zentrale gesellschaftliche Rolle bekommen konnten und es bedarf des Zusammenwirkens von sehr vielen Akteuren, um funktionsfähige soziotechnische Systeme aufzubauen, die je nach Aufgabenbereich oder Verwaltungs- und Staatsstruktur ganz anders ausfallen können.

---

## 4 Gute Technik, böse Technik? Zwischen Utopien und Dystopien

Die öffentliche Debatte über das, was im digitalen Zeitalter auf uns zukommt, schwankt zwischen Utopien und Dystopien hin und her, wie eine Musterung der Literatur schnell zeigt. Während die einen davon schwärmen, die Probleme der Menschheit ließen sich im Prinzip lösen, wenn wir nur genug Daten hätten (Schmidt und Cohen 2013), befürchten andere den Verlust von Privatsphäre, Freiheit und Humanität, wenn permanent erfasst wird, wo wir uns befinden, mit wem wir uns treffen und was wir tun (Morozov 2013; Welzer 2017; Aust und Ammann 2016). Während manche hoffen, dass Sensoren, Roboter und künstliche Intelligenz uns das Leben leichter machen (Eberl 2016), sorgen sich einige, irgendwann könnten Maschinen den Menschen beherrschen (Schirrmacher 2015). Während man sich hier und dort eine Vitalisierung der Demokratie durch digitale Technologien erhofft, träumen Vordenker im *Silicon Valley* von künstlichen Inseln auf den Weltmeeren, auf denen alles einfach ausprobiert werden kann, weil keine Rechtsordnung, kein Gesetzgeber und kein Richterspruch sie daran hindert (Djeffal 2017). Manche sehen uns dagegen auf dem „Weg in die Überwachungsgesellschaft“ (Schaar 2007) und den „surveillance capitalism“ (Zuboff 2015), Gesellschaftsformen, in denen wir nicht nur vom Staat, sondern auch von privaten Unternehmen nahezu lückenlos kontrolliert werden und Demokratie ans Ende gerät (Hofstetter 2016).

Diese gegensätzlichen Einschätzungen prägen auch die Diskussionen um die Digitalisierung von Staat und Verwaltung. Vieles spricht dafür, dass es beides geben wird, sowohl die befürchteten negativen als auch die erhofften positiven Ergebnisse. Das Internet hat viele Vorteile mit sich gebracht, aber es wird natürlich auch von Kriminellen, Extremisten und Terroristen, Diktatoren und anderen für ihre Zwecke genutzt. Die Verschlüsselung der Kommunikation kann helfen, unsere Privatsphäre gegenüber kommerziellen „Datenfressern“ (Kurz und Rieger 2011), aber auch staatlichen Übergriffen zu schützen, sie nützt aber auch jenen, die vom Betrug leben oder Leib und Leben bedrohen (Schallbruch 2018). Algorithmen können menschliche Vorurteile sichtbar machen, aber solche Vorurteile auch verstärken, indem sie menschliches Ermessen ausschalten, aber in ihrer Programmierung Vorurteilsstrukturen enthalten. Industrieroboter können repetitive Aufgaben erledigen und Menschen entlasten, aber auch zur Herstellung von Kriegsdrohnen verwendet und als tödliche Waffe eingesetzt werden. *Wearables* und *tracking devices* können helfen, den Gesundheitszustand von Patienten genau zu beobachten und sind gerade für die Versorgung in ländlichen Räumen wichtig – sie können auch zur gezielten, Persönlichkeitsgrenzen verletzenden Verhaltens- und Meinungsmanipulation eingesetzt werden. Nahezu alles, was das digitale Zeitalter uns gebracht hat, ist *Dual-use*-Technologie: Es kann zum Nutzen des Gemeinwohls, aber auch zu seinem Schaden eingesetzt werden. Diese allgemeine Erkenntnis gilt auch für Staat und Verwaltung: Beide können das Potenzial, das in den digitalen Technologien steckt, dazu nutzen, ihre internen Abläufe zu verbessern, um den Bürger\*innen bessere Leistungen zu bieten, aber sie können die technischen Möglichkeiten auch nutzen, um Freiheit einzuschränken. Das *Social Scoring System*, das die chinesische Regierung vorantriebt, dürfte Polizei und Justiz entlasten, weil ungewolltes Verhalten im öffentlichen Raum, das von Kameras erfasst worden ist, sofort geahndet werden kann, so dass keine langwierigen Verfahren mehr anfallen, aber die ständige Drohung, Punkte zu verlieren, wenn man sich nicht „anständig“ verhält, und dann Nachteile zu erfahren, führt natürlich zu übermäßig angepasstem Verhalten. Ein staatliches Handeln, das auf dem permanenten Sammeln von Daten beruht, ist in funktionierenden Demokratien (hoffentlich) undenkbar. Aber die Debatte darüber, wo die Grenze verlaufen soll zwischen Sicherheit und Freiheit, zwischen Datensammeln und Sammelverzicht, wird auf lange Zeit große Bedeutung besitzen.

Welche Prognosen und Erwartungen, Hoffnungen und Befürchtungen sich bewahrheiten, ist vor allem eines: unsicher. Niemand kann heute mit Gewissheit sagen, wie wir in zwanzig, fünfzig oder achtzig Jahren leben werden, wie sich die Technik und die Gesellschaft bis dahin entwickelt haben und welche der Szenarien, die gegenwärtig durchgespielt werden, tatsächlich eingetroffen sind. In den Artikeln dieses Handbuchs werden deshalb aktuelle Entwicklungen aufgezeigt und Fragen formuliert, die sich daraus ergeben, aber keine abschließenden Antworten geboten. Wir stehen am Beginn der digitalen Transformation von Staat und Verwaltung, ohne immer schon zu wissen, wohin uns diese führen wird.

## 5 Staatlichkeit im digitalen Zeitalter

Dass der Staat vermutlich künftig aktiver als heute Daten sammeln wird, um nach innen und nach außen besser steuern zu können, reicht noch nicht aus, um von einem „anderen“ Staat reden zu können. Solange wir auch im digitalen Zeitalter Rechtsstaat, Demokratie und Sozialstaat bleiben, hat ein Regimewechsel nicht stattgefunden. Mit dem Aufkommen der ökologischen Frage schien der „Umweltstaat“ oder „Ökostaat“ eine neue Stufe staatlicher Entwicklung darzustellen (Guggenberger 1994), diese Sicht konnte sich aber nicht durchsetzen. Die enorme gesellschaftliche Bedeutung des Umweltthemas hat bis heute keine neue Form von Staatlichkeit erzeugt. Führt die Digitalisierung zu einem Digitalen Staat als einer neuen Stufe in der historischen Entwicklung des modernen Staates?

Wenn ein Staat nach der Drei-Elemente-Lehre von Georg Jellinek aus Staatsgebiet, Staatsvolk und Staatsgewalt besteht, dann wirft das zunächst die Frage auf, ob und wie diese Komponenten durch die digitale Transformation verändert werden. Nationale Grenzen, also klar abgegrenzte Gebiete unter staatlicher Kontrolle, spielen in der virtuellen Welt oft keine Rolle mehr, auch wenn manche Staaten sich gegenüber dem Internet abzuschotten und andere das, was sich darin abspielt, zu regulieren und zu censieren versuchen. Wie sich diese Welt entwickelt, entscheiden nicht nationale Gesetzgeber, sondern große Konzerne mit ihren Angeboten („Code is law“).

Mehrere Pässe, die europäische Freizügigkeit und die weltweite Migration haben ein homogenes Staatsvolk schon längst zur Illusion werden lassen. Dennoch haben die Bürger\*innen eines Landes nicht nur Rechte, sondern auch Pflichten. Estland ist das weltweit erste Land, bei dem man ab 2015 eine virtuelle Staatsbürgerschaft (*E-Residency*) beantragen konnte. Diese berechtigt zwar nicht dazu, an Wahlen teilzunehmen, und führt auch nicht zwingend dazu, dass man einen estnischen Reisepass oder die Genehmigung bekommt, sich physisch in dem Land aufzuhalten, aber man kann über das Netz einfacher staatliche Dienstleistungen in Anspruch nehmen, zum Beispiel relativ unkompliziert eine Firma in Estland gründen. Die Plastikkarte, mit der man sich im Behördennetz legitimiert, kann auch in anderen europäischen Ländern zu diesem Zweck genutzt werden.

Dass nationale Grenzen im digitalen Zeitalter an Bedeutung verlieren, ist so lange unschädlich, wie auf dem eigenen Territorium noch die Staatsgewalt ausgeübt werden kann. Auch dieses Staatselement ist durchaus nicht mehr gesichert. Kriminelle, die von anderen Ländern aus operieren, sind für die deutsche Polizei und Justiz nur schwer zu ermitteln. Der Staat hat Mühe, seine kritischen Infrastrukturen gegen Angriffe von außen zu schützen, und es gelingt ihm nicht, auch noch seine Bürger\*innen davor zu bewahren. Das staatliche Gewaltmonopol gilt im *Cyberspace* nicht; die Staatsgewalt ist dort schwach ausgeprägt (Schallbruch 2018). Der Staat müsse sich so organisieren wie die erfolgreichen Plattformen im *Internet*, meint Tim O'Reilly (2010), also zwischen Nachfrage und Angebot vermitteln, ohne die Leistung unbedingt selbst erbringen zu müssen. Nach seiner Idee sind es nicht mehr Parteien, die Programme aufstellen, mit den sie Wahlen und eine Mehrheit gewinnen wollen, um ihre politischen Vorstellungen umsetzen zu können, sondern was die

Menschen wollen, lasse sich täglich in Echtzeit ermitteln. Der Staat müsse dann nur noch dafür sorgen, dass sie das möglichst auch bekämen. Parlamente, in denen mühsam um Kompromisse gerungen werde, brauche man nicht mehr, wenn die entsprechenden Daten vorlägen. Eine Firma von Bill Gates hat in der Nähe von Phoenix (Arizona) für 80 Millionen Dollar rund 100 km<sup>2</sup> Wüste aufgekauft, um dort eine „intelligente Stadt“ zu errichten, in der alles über Daten gesteuert wird. Hochgeschwindigkeitsnetze, Rechenzentren und autonome Fahrzeuge sollen im Projekt „Belmont“ selbstverständlich sein. Stadtgründung nicht als demokratische Entscheidung, sondern als privates Investment. Eine ähnliche *Smart City* („Neom“) in Saudi-Arabien soll insgesamt sogar 500 Milliarden Dollar kosten.

Eine Staatsgewalt, die auf demokratischer Entscheidungsfindung beruht, ist also durchaus angegriffen – unternehmerische Akteure verstehen sich als Alternative zum Staat. *Google* bzw. *Alphabet* plant an der Wasserseite von Toronto auf zwölf Hektar einen ganz neuen Stadtteil („Quayside“), wo alles miteinander vernetzt sein soll. Amerikanischen Kommunen bietet der Konzern an, ihnen beizubringen, was heute intelligente Steuerung des öffentlichen Lebens heißt. Verdrängt private Initiative im digitalen Zeitalter die öffentliche Daseinsvorsorge oder sammelt der Staat künftig ähnlich viele Daten, um mit den kommerziellen Plattformen mithalten zu können (Brown et al. 2017)? *Facebook* hat der amerikanischen Regierung angeboten, eine Art Melderegister zu führen: Niemand habe mehr Daten über mehr Amerikaner als man selbst. Inzwischen gibt es rund hundert virtuelle Währungen, die nicht von Notenbanken emittiert, sondern im *Internet* „geschöpft“ worden sind (Casey und Vigna 2017). Die *Blockchain*-Technologie hat theoretisch das Potential, nicht nur Notare und Anwälte arbeitslos, sondern auch staatliche Register überflüssig zu machen.

Auch die finanzielle Basis des Staates ist keineswegs gesichert. Wenn in der digitalen Ökonomie, die von transnationalen Plattformen geprägt ist, einerseits die „Clickworker“ keine Steuern und Sozialabgaben zahlen (Nullmeier 2017), und andererseits die Giganten des Internets auch nichts, weil sie ihre Gewinne in Steueroasen lotsen (Mayer-Schönberger und Ramge 2017), ist die Finanzierung des Wohlfahrtsstaates gefährdet. Dass selbst Konzernlenker inzwischen für ein bedingungsloses Grundeinkommen plädieren (siehe z. B. „Wirtschaft für Grundeinkommen“ 2018; Douma 2018), deutet darauf hin, dass sie von einer verringerten Beschäftigung, höherer Arbeitslosigkeit und einer durchschnittlich geringeren Bezahlung der meisten in einer digitalisierten Produktion und Plattform-Ökonomie ausgehen. Wenn der Staat allen ein Grundeinkommen garantieren soll, müssen aber diese Mittel irgendwie aufgebracht werden. Ein Steuermodell für die digitale Welt, mit oder ohne Digitalsteuer, ist sicherlich erforderlich.

Die Beispiele zeigen, dass viele Elemente dessen, was Staatlichkeit ausmacht, durch Digitalisierung in Bewegung geraten. Eine positive Vision des Digitalen Staates hat sich dabei noch nicht herausgeschält, außer dass er transparent, offen und gut vernetzt sein soll. Allein das verstärkte Sammeln von Daten ergibt noch kein Leitbild für die Zukunft. Hier sind noch sehr viele Fragen offen. In den Artikeln dieses Handbuchs, die helfen können sichtbar zu machen, wie facettenreich das Thema ist, werden Hinweise gegeben, worüber aktuell diskutiert wird und worüber weiter nachgedacht werden muss.

## 6 Umrisse einer digitalen Verwaltung

Die öffentliche Verwaltung in Deutschland ist seit gut drei Dekaden vielfältigen Veränderungsimpulsen ausgesetzt: Das Neue Steuerungsmodell, die deutsche Fassung des angelsächsischen Leitbilds von *New Public Management*, mit dem in Deutschland zu Beginn der 1990er-Jahre eine umfassende Verwaltungsreformbewegung angestoßen wurde, stellte den Beginn einer Folge von Reformversuchen dar. Heute gibt es gleich eine ganze Reihe von Leitbildern, die das *New Public Management* ablösen wollen: *Post-NPM*, *New Public Governance*, *whole-of-government*, *joint-up-government*, *Public Value Management* (Reiter und Klenk 2019; O'Flynn 2007).

Die Reformaktivitäten der vergangenen Jahre haben die klassische Weberianische Verwaltung mit ihrem ausgeprägten Hierarchieprinzip, den stark arbeitsteilig organisierten Abläufen, der bürokratisch-regelgebundenen Steuerung, dem Schriftlichkeitsprinzip und dem Unpersönlichkeitsprinzip nicht zum Verschwinden gebracht, sie aber um neue – zum Teil auch sich widersprechende – Organisationsideen ergänzt. Das Leitbild ‚der‘ öffentlichen Verwaltung gibt es heute nicht mehr. Sie gleicht vielmehr einer Bricolage unterschiedlicher Organisationsideen, wobei sich das Gewichtungsverhältnis der verschiedenen Leitbilder und -kulturen je nach Verwaltungssektor und politischer Ebene unterscheidet.

Wie sich die Digitalisierung in die Reformentwicklung einordnet, ist noch offen. Digitalisierung der öffentlichen Verwaltung im Sinne basaler, *schwacher* Digitalisierung würde bedeuten, die gegenwärtige Verwaltungsorganisation einfach noch um ein weiteres Prinzip zu ergänzen, indem bestehende Strukturen und Prozesse zusätzlich oder ausschließlich mit digitalen Medien abgebildet werden: Akten würden (auch) elektronisch geführt, Formulare und Terminvereinbarung (auch) *online* angeboten, Verwaltungspartizipation würde auch über digitale *tools* möglich.

Eine *starke* Digitalisierung würde weitergehende Wirkungen entfalten, sie dürfte zu einer agilen, vernetzten, flexibleren und offeneren Verwaltung führen, die in einer stärkeren Distanz zum klassischen Bild der öffentlichen Verwaltung steht. Eine Administration, die beispielsweise dem auf Digitalisierung basierenden Leitbild der *agilen* Verwaltung (OECD 2015) folgt, hat, konsequent umgesetzt, nicht mehr viel mit Max Webers Idealtypus der Bürokratie zu tun. Langfristige Planungen werden durch iterative Vorgehensweisen ersetzt, feste Laufbahnen weichen flachen und durchlässigen Hierarchien, Autorität ist in der agilen Verwaltung nicht mehr an eine bestimmte Position in der Hierarchie gebunden, Teams oder Projekte können ohne Vorgesetztenfunktion geleitet werden. Eine *vernetzte* Verwaltung wiederum bricht mit dem für die deutsche Verwaltung bislang so wichtigen Ressortprinzip, da Kommunikations- und Arbeitsprozesse bewusst politikfeld- und politikebenenübergreifend organisiert werden. Eine *flexible* Verwaltung schließlich flexibilisiert auch den Personaleinsatz und lässt die Beschäftigte auf Abruf anfallende Arbeiten aus der *Cloud* heraus verrichten. Diese Spielart der Digitalisierung stellt das Alimentationsprinzip in Frage, das zu den hergebrachten Grundsätzen des Berufsbeamtentums gehört. Eine *offene* Verwaltung schlussendlich lässt Verwaltungsprodukte und -dienstleistungen von Kund\*innen und Bürger\*inneninteressen (mit-)bestimmen bzw. beteiligt diese auch an der Her- und Bereitstellung (*co-creation*).

Die *datengetriebene* Verwaltung stellt schließlich die stärkste denkbare Variante der Digitalisierung dar, werden in ihr doch nicht nur Arbeitsprozesse, sondern auch Entscheidungsprozesse automatisiert oder gar autonomisiert (Mohabbat Kar et al. 2018). Auch hier sind sehr unterschiedliche Spielarten der Digitalisierung denkbar: *Big Data Analytics*, die gezielte Zusammenführung und algorithmische Auswertung großer Datenmengen, erlauben vorausschauende – *prädiktive* – *Analysen*, die in der Polizeiarbeit, im Katastrophenmanagement oder in der Gesundheitspolitik verwendet werden können. Auch Stimmungsbeobachtung in Echtzeit und permanentes Monitoring der Bürgerzufriedenheit werden durch *Big Data Analytics* möglich, wodurch Verwaltungsdienstleistungen viel besser personalisiert werden können. *Embedded Sensors* als eine weitere Spielart der digitalen Verwaltung können automatisch Meldung machen, wenn die Parkbank kaputt oder der Müllheimer voll ist, weshalb man einen „Maerker“, einen elektronischen Bürgerservice der „basalen“ Form, der Bürger erlaubt, Ordnungsbehörden auf einem neuen Kommunikationsweg auf Probleme aufmerksam zu machen, dann im Grunde nicht mehr brauchen würde. Systeme künstlicher Intelligenz als dritte Spielart der digitalen Verwaltung wiederum können in der Steuer- oder Sozialverwaltung eingesetzt werden, wo sie autonom Entscheidungen über Leistungen und Anträge treffen. Solche Automatisierungs- und Autonomisierungsprozesse würden das Neutralitätsprinzip der öffentlichen Verwaltung auf eine gänzliche andere Grundlage stellen.

Kurzum: Verwaltungsmodernisierung im Sinne der starken Digitalisierung würde in einem viel umfassenderen Sinne mit den Prinzipien der Weberianischen Verwaltung brechen, als es *New Public Management*, *Post-NPM* oder *New Public Governance* je gelungen ist – ob dies vorstellbar und ob dies überhaupt wünschbar ist, sind Fragen, die in den Artikeln des Handbuchs erörtert werden. Die Digitalisierung der Verwaltung schreitet zudem in sehr unterschiedlichem Maße voran, stößt auf große Unterstützung wie erhebliche Gegenwehr, scheitert an sachlichen Umsetzungsproblemen, produziert euphorische Reaktionen und Enttäuschungen. Zu fragen ist, ob die Entwicklung in eine Richtung weist, die über längere Zeit die Kultur der Verwaltung verändert und so etwas erzeugt wie eine Verwaltungs-, „Kultur der Digitalität“ (vgl. Stalder 2016). Werden hierarchisch-weisungsbezogene Organisationskulturen, die eher dem Bild einer Weberschen Bürokratie entsprechen, durch eine stärker kooperativ-horizontale Administration ergänzt oder ersetzt, wie sie in der *Open-Source-Software*-Zusammenarbeit vorhanden ist, oder kommt es zu Hybridisierungen, Mischungen zwischen alt und neu?

---

## 7 Konzeption und Gliederung des Handbuchs

Ziel des Handbuchs ist eine umfassende Bestandsaufnahme der Formen der Digitalisierung in Staat und Verwaltung. Diskutiert werden dabei der Stand der Digitalisierung sowohl in Bezug auf die institutionelle (*polity*), die inhaltliche (*policy*) als auch die prozessurale (*politics*) Dimension von Politik und Verwaltung. Es werden Institutionen und Organisationen ebenso in den Blick genommen wie politische Programme, Ergebnisse in Politikfeldern, politische Verfahren und politi-

sche Dynamiken, z. B. im Rahmen von *online*-Wahlen oder von digitaler Partizipation bei Entscheidungsprozessen. Ein besonderes Augenmerk des Handbuchs liegt auf den ausführenden Organen von Politik, namentlich den Ministerien und Behörden der öffentlichen Verwaltung. Im Kern geht es dabei um Staat und Verwaltung in *Deutschland*, in etlichen Beiträgen werden jedoch auch internationale Erfahrungen integriert. Auch die europäische Ebene wird in den Blick genommen, erfolgen doch von dort wesentliche Impulse zur Digitalisierung der nationalen Institutionen und Verfahren.

Die Autorinnen und Autoren des Handbuchs kommen aus den verschiedensten Fächern, der Soziologie, der Politikwissenschaft, der Rechtswissenschaft, der Informatik, der Geografie, der Wirtschaftswissenschaft und der Organisationswissenschaften. Was sie miteinander verbindet, ist das Selbstverständnis einer interdisziplinär ausgerichteten Verwaltungs- und Staatswissenschaft und *Policy-Analyse*, die Verwaltung als einen wesentlichen Akteur des politisch-administrativen Systems begreift, der entscheidend zum Gelingen oder Scheitern von Politik beitragen kann (Bauer und Grande 2018).

Das Handbuch richtet sich an alle, die den Stand der Digitalisierung in Staat und Verwaltung aus einer wissenschaftlichen Perspektive reflektieren wollen. Alle Beiträge greifen auf Theorien und Analyserahmen der interdisziplinären Staats-, Verwaltungs- und *Policy*-Forschung zurück, um die bisherige Entwicklung und die Perspektiven der Digitalisierung in Staat und Verwaltung zu dokumentieren und zu diskutieren. Die Beiträge benennen zudem Herausforderungen bei der Umsetzung von Digitalisierung und verweisen auf positive und negative Auswirkungen von Digitalisierungsmaßnahmen. Das Handbuch kann und will aber keine Handlungsanleitung bieten, wie in öffentlichen Institutionen und Verwaltungseinheiten Digitalisierung konkret zu betreiben wäre, auch wenn Defizite bisheriger Digitalisierungspolitik klar benannt und Empfehlungen für eine zukünftige Strategie gegeben werden.

Die Artikel sind in sechs Kapiteln angeordnet. Auf die Einleitung in Teil I folgen.

## I. Spielarten der Digitalisierung

In einem ersten Kapitel werden die Spielarten der Digitalisierung vorgestellt. Unter Digitalisierungsformen oder Spielarten der Digitalisierung wollen wir grundlegende soziotechnische Formen der Verbindung von öffentlichem Handeln und Einsatz digitaler Prozesse und elektronischer Technologien verstehen. Künstliche Intelligenz, *Big Data*-Auswertungen etc. sind gesellschaftliche Entwicklungsformen von wissenschaftlich-technischen Neuerungen. Diese sollen hier vorgestellt und in ihren Bezügen zu öffentlichem Handeln in Staat und Verwaltung vorgestellt und auf ihre Potenziale und Begrenzungen hin befragt werden.

## II. Leitbilder und normative Grundfragen

Welche Bedeutung Digitalisierung für Staat und Verwaltung gewinnen kann und welche Richtung eine verstärkte Digitalisierung nehmen sollte, wird oft in normativen Entwürfen, Reformkonzepten und Programmatiken beantwortet, die hier unter der zusammenfassenden Vokabel „Leitbilder“ verhandelt werden.

Normative Grundfragen der Digitalisierung werden aber nicht nur in programmatisch auftretenden Leitbildern wie „digitaler Staat“, „agile Verwaltung“ oder „Informationsfreiheit“ verhandelt. Mit Transparenz und digitaler Souveränität haben sich in den letzten Jahren Wertbegriffe entwickelt, die zum Ankerpunkt der kritischen Diskussionen über die Folgen der Digitalisierung geworden sind. Systematisch werden Grundsatzfragen in der digitalen Ethik behandelt und auch im Rechtssystem stellen sich Fragen nach dem Souverän: Wem gehören die Daten? Die Digitalisierung erzeugt einen eigenen Reflexionsraum, in dem teils alte normative Grundfragen neu diskutiert, zum Teil aber auch ganz neue Schwerpunktsetzungen auftreten, die das Gefüge unserer bisherigen Wertbegrifflichkeiten durcheinanderbringen.

### III. Demokratisches Regieren

Wie gestaltet sich demokratisches Regieren unter dem Einfluss von Digitalisierungsprozessen? Entwickelt sich eine neue Form der Demokratie und Rechtsstaatlichkeit? Ist *E-Democracy* eine neue Qualität von Demokratie, verändern sich die Beziehungen zwischen Staat und Bürgern grundlegender, wenn neue Möglichkeiten der *Online*-Partizipation hinzutreten und die *Social Media* zu wesentlichen Kanälen politischer Öffentlichkeit werden mit Folgen für Willensbildung, Gesetzgebung und Verwaltung? Das sind zentrale Fragestellungen des dritten Kapitels „Demokratisches Regieren“.

Demokratische Staatlichkeit zeichnet sich durch die Prägung staatlichen Handelns durch die Bürger\*innenschaft aus. Das geschieht in parlamentarischen Systemen vorrangig über die Wahlen zu den Parlamenten und die Bildung der Regierung aus dem Parlament heraus. Je nach Verfasstheit treten Formen direkter Demokratie hinzu. Eingebettet ist dieser Kern repräsentativer Demokratie in eine Vielfalt von institutionell eröffneten Partizipationsformen, von Petitionen bis zu Formen deliberativer Demokratie, dazu der breite Bereich der öffentlichen politischen Auseinandersetzung bis hin Protest und sozialen Bewegungen. Hier soll interessieren, wie sich die staatlich verfassten Teile dieses demokratischen Geschehens durch Digitalisierung verändern. Die Parlamentsorganisation mag sich ebenso ändern wie das Wählen selbst, was zu *E-Voting* oder *Online*-Wahlen führen kann.

### IV. Akteure und Institutionen

Wer betreibt und gestaltet in Staat und Verwaltung Digitalisierungsprozesse? Von der EU über die Bundesebene bis zu Ländern und Gemeinden erstreckt sich der Kreis der politischen und administrativen Akteure. Hinzu kommen gemeinsame Organe wie der IT-Planungsrat oder spezialisierte Aufgabenträger wie die Datenschutzbeauftragten. Das Kapitel bietet einen Überblick zu den wichtigsten öffentlichen Handlungsträgern mit deutlichem Schwergewicht auf die Bundesrepublik Deutschland.

Digitalisierung hat sich, obwohl zunehmend alle Felder staatlichen Handelns betroffen sind, eine eigene institutionelle Infrastruktur und ein eigenes Akteurennetzwerk geschaffen. Ob unter den Titeln IT-Politik, Netzpolitik oder Datenpolitik, Digitalisierung ist meist verbunden mit der Ausbildung spezieller Abteilungen in Ministerien, eigenen Formen föderaler Koordinierung und spe-

zialisierten Agenturen oder Instituten. Diese vorzustellen und ihre jeweilige Position zu bestimmen, ist Aufgabe dieses Kapitels.

#### V. Politikfelder und Instrumente

Digitalisierung lässt sich aber nicht in einem speziellen Politikfeld einfangen, auf dieses begrenzen. Digitalisierung ist eine Gesamtbewegung, die keinen politischen Bereich unberührt lässt. Für ausgewählte Politikfelder und Instrumente werden daher Digitalisierungsprozesse in Staat und Verwaltung detaillierter dargestellt: Wie wirkt sich Digitalisierung in der Bildungs-, Sozial-Gesundheits-, Verkehrs- und Innenpolitik aus? Wie verändern sich Stadt- und Raumpolitiken? Auch die Politikfelder, die sich mit Sicherheitsfragen beschäftigen, werden durch die neuen Möglichkeiten der Datensammlung und -analyse in ihrer Vorgehensweise gravierend verändert, zugleich sind alle Sicherheitsapparate durch *Hacking* und Cyberattacken einer neuen Gefahr ausgesetzt, weshalb viele bereits einen *Cyber-War* ausgerufen haben.

Als Gesamtbewegung, die keinen politischen Bereich unberührt lässt, verläuft Digitalisierung häufig quer zu tradierten Grenzen von Politikfeldern. Fragen der Integration von Politikfeldern bzw. der politikfeldübergreifenden Koordination werden dadurch besonders virulent. In diesem Kontext wird vielfach diskutiert, ob Digitalisierung als ein eigenständiges Politikfeld begriffen werden sollte, dessen Problem- und Gegenstandsbereich von einem Digitalisierungsministerium bearbeitet wird. Stand und Perspektiven dieser Diskussion werden hier näher vorgestellt und reflektiert.

#### VI. Personal, Organisation und Prozesse

Verwaltungen sind Organisationen, die durch ihre Rechtsbindung auf geordnete Abläufe in besonderem Maße angewiesen sind. Sie werden getragen von den Mitarbeiter\*innen, die in eine bestimmte Organisationskultur, in einen bestimmten organisatorischen Aufbau und vorgegebene oder auch erst zu findende Ablaufprozesse eingebunden sind. Was bedeutet Digitalisierung für diese Ordnungsstrukturen in Verwaltungen? Und was bedeutet sie für die Bediensteten der öffentlichen Verwaltung? Erleichtert sich ihre Arbeit durch schlankere und schnellere IT-gestützte Abläufe? Oder erleben sie Digitalisierung aufgrund fehlender Interoperabilität der verwendeten Systeme und/oder nicht hinreichender Qualifizierung als zusätzliche Last?

Digitalisierung ist zunächst ein Veränderungsprozess. Sie ist nicht einfach als Implementation eines neuen Mediums oder einer neuen Vorgehensweise zu interpretieren. Da Digitalisierung die kulturelle Dimension der Verwaltung betrifft, muss sie in strukturierten Wandlungsprozessen in einer Verwaltung oder anderen staatlichen Einrichtungen unter Beteiligung vieler Akteure entwickelt und eingeführt werden. Erfahrungen mit *Software-Einführungen* existieren seit Jahrzehnten, ohne eine Mitwirkung des Personals ist kein Erfolg zu erwarten. Entsprechend muss auch digitaler Wandel über Verfahren, die heute oft als *Change Management* bezeichnet werden, ermöglicht werden. Wie kann unter diesen Bedingungen organisationaler Wandel organisiert werden? Die meisten Verwaltungen sind erfahren in den verschiedensten Organisationsentwicklungsmaßnahmen der jeweiligen Wellen des *New Public Management*. Ist Digitali-

---

sierung nur eine Fortsetzung dieser seit langem von IT-Fragen zentral bestimmten *Change-Management*-Versuche?

Zum Themenkomplex Personal, Organisation und Prozesse gehören auch die Fragen, wie Führung in einer Verwaltung 4.0 aussehen kann, welche Kompetenzprofile für Verwaltungsmitarbeiter\*innen erforderlich sind, wie Kommunikation und Datenaustausch zwischen Organisationen gestaltet wird. Da Digitalisierung dauerhaften Wandel impliziert, ist schlussendlich auch zu diskutieren, wie in öffentlichen Verwaltungen eine Innovationskultur etabliert werden kann, um die Anpassungs- und Handlungsfähigkeit des öffentlichen Sektors zu verbessern.

Sicher, jeder systematische Blick wird Lücken entdecken, internationale Akteure, andere Länder, besondere Politikfelder und einzelne Spezialinstrumente mögen in diesem Handbuch fehlen. Allen Beteiligten ist bewusst, dass ein solcher Gesamtüberblick mit dem Anspruch auf Lückenlosigkeit noch nicht gelingen kann. Die Möglichkeiten der digitalen Publikation erweisen sich hier als Glücksfall, da sie eine beständige Aktualisierung der Beiträge und eine Erweiterung des Handbuchs ermöglichen.

---

## 8 Eine erste Zwischenbilanz

- (1) Verwaltungsdigitalisierung: Die Beiträge zeigen in ihrer übergroßen Mehrheit, dass in Deutschland die Digitalisierung der Verwaltung selbst im Sinne einer ersten Stufe basaler Digitalisierung, der Umstellung von analogen Verwaltungsprozessen auf die Bereitstellung zusätzlicher oder ausschließlich digitaler Zugangsmöglichkeiten noch nicht vollzogen ist. Wo *Online*-Portale vorhanden sind, scheitert eine durchgehend digitale Bearbeitung daran, dass doch wieder die Papierform oder der persönliche Gang zum Amt erforderlich sind. Medienbrüche und nicht digital umgesetzte Sicherheitsanforderungen lassen eine Insellandschaft an Digitallösungen im Verkehr zwischen Verwaltung und Bürger\*innen entstehen, nicht anders als Jahre vorher bereits bei den verwaltungsinternen Softwarelösungen.
- (2) Bei internationalen Vergleichen landet die Bundesrepublik Deutschland regelmäßig bestenfalls im Mittelfeld, jedenfalls nicht in der Spitzengruppe der Länder, die auf diesem Feld am weitesten sind. So verschiedene Länder wie Singapur und Estland werden eher genannt, wenn von „digitalen Staaten“ die Rede ist. Im *Digital Economy and Society Index* (DESI), mit dem die Europäische Kommission die *Digital Readiness* ihrer Mitglieder erfassen möchte, landete Deutschland 2018 wie schon im Vorjahr unter 28 EU-Mitgliedern auf Platz 14, knapp über dem EU-Durchschnitt. Das kann nicht der Anspruch eines Landes sein, das zu den sieben wichtigsten Industrienationen gehört. Allerdings liefern solche Vergleiche selten Erklärungen, warum bestimmte Länder langsamer vorankommen als die führenden Nationen, und sie benennen meist auch die Stellschrauben nicht, an denen gedreht werden müsste, um möglichst rasch eine

- bessere Platzierung zu erreichen. Mit anderen Worten: Sie bieten zwar Deskription, aber keine Theorie.
- (3) Bemerkenswert ist die Diskrepanz zwischen diesem Ist-Zustand und den allseits kursierenden Annahmen über die Veränderungspotenziale von Digitalisierung. Fantasien einer ganz anderen Welt und Dramatisierungen der grundstürzenden Veränderungen der Ökonomie, der Arbeitswelt dominieren große Teile der Öffentlichkeit, während sich real – zumindest in dem hier näher untersuchten Bereich – nur recht langsam Änderungen ergeben. Offensichtlich fehlen in den Zukunftsszenarien wichtige Faktoren, die in der Veränderungslogik von Staat und Verwaltung aber zentrale Rollen spielen.
  - (4) Es spricht vieles dafür, dass wir es auch in den nächsten Jahren nicht mit einem Regimewechsel, einer Revolutionierung öffentlicher Tätigkeit, sondern mit einem Regimewandel, einer meist mühsamen, vielleicht auch in einzelnen Bereichen schnellen bis überstürzten Transformation zu tun bekommen. Es spricht außerdem einiges dafür, dass die digitale Transformation von Staat und Verwaltung langsamer verlaufen wird als in den privaten Haushalten oder insbesondere in Wirtschaft und Unternehmen („Industrie 4.0“). Man darf unterstellen, dass es nicht nur Veränderungswille ist, der diese Reformgeschwindigkeit bestimmt. Es müssen auch reale Hindernisse berücksichtigt werden, die dazu führen können, dass weder die wunderbaren Zukunftswelten noch die Gefahren der Digitalisierung in dem prognostizierten Maße eintreten.
  - (5) Zu den realen Hindernissen der Digitalisierung gehört unter anderem der für das Regierungssystem in Deutschland typische exekutive Föderalismus, der den Ländern gerade im Bereich der Verwaltung viele Freiheiten lässt und nur wenig Anreize für konzertierte Digitalisierungsstrategien und eine einheitliche Implementation von digitalen Lösungen bietet. Mechanismen der horizontalen und vertikalen Koordination können den Zentrifugalkräften nur entgegenwirken, nicht aber gleichgerichtete Strategien und einheitliche Vorgehensweisen garantieren. Dies haben u. a. die Erfahrungen mit dem IT-Planungsrat gezeigt, der 2010 auf der Basis von Art. 91c GG als Gremium zur gleichberechtigten Zusammenarbeit von Bund und Ländern bei der Digitalisierung von Verwaltungsleistungen eingerichtet wurde. In Anbetracht der bislang ernüchternden Bilanz der Arbeit des IT-Planungsrats trat im Juli 2017 eine Ergänzung des Art. 91c GG in Kraft, die dem Bund erweiterte Kompetenzen bei der Gestaltung des informationstechnischen Zugangs zu den Verwaltungsleistungen von Bund und Ländern zuweist. Zwar wollen Bund, Länder und Gemeinden garantieren, dass ein Mindestmaß an Zusammenarbeit der verschiedenen Systeme, Techniken und Organisationen möglich wird und gemeinsame Standards gelten – in der Vergangenheit hat sie dieses gemeinsame Ziel aber nicht daran gehindert, ihre je eigenen Wege zu gehen.
  - (6) Ein weiterer hemmender Faktor stellt die fragmentierte Leistungserbringerlandschaft dar, die mittlerweile in vielen Bereichen vorzufinden ist. Die Fragmentierung resultiert entweder aus tradierten Subsidiaritätsprinzipien oder ist Ergebnis von Auslagerungs- und Privatisierungsprozessen im Kontext der Verwaltungmodernisierung der 1990er- und frühen 2000er-Jahre. In Kombina-

tion mit der in vielen Politikfeldern dominanten wettbewerblichen Steuerungslogik erzeugt die zerfaserte Leistungserbringerlandschaft ähnliche Effekte wie der Föderalismus: es werden bewusst Insellösungen geschaffen und nicht-interoperable Systeme implementiert, um sich auf diese Weise mögliche Wettbewerbsvorteile zu sichern.

- (7) Ein drittes Hindernis für die Digitalisierung ergibt sich aus den organisatorischen und prozeduralen Merkmalen von Entscheidungsprozessen in der Ministerialverwaltung. Im internationalen Vergleich zeichnet sich die typische Arbeitsweise der deutschen Ministerialverwaltung bei der Politikvorbereitung und -implementation durch ein besonders ausgeprägtes Ressortprinzip aus. Die interministerielle Abstimmung erfolgt nach dem Modus der negativen Koordination, d. h. Handlungsvorschläge und Entscheidungsvorlagen werden von der federführenden Einheit eigenständig erarbeitet und erst im Anschluss anderen Ministerien vorlegt; diese wiederum prüfen in erster Linie, welche negativen Folgen die Vorlage für den eigenen Bereich hat – nicht die Qualität der Vorlage an sich. Eine solche Arbeitsweise fördert ein Entscheidungsverhalten, das vor allem auf die eigenen Organisationsinteressen ausgerichtet ist und daher Prozesse der horizontalen Koordination erschwert. Die Bearbeitung von Politikproblemen, die – wie die Digitalisierung – mehrere Politikfelder berühren oder quer zu den Strukturen der klassischen Politikfelder liegen und deshalb politikfeldübergreifender Koordination bedürfen, verläuft oftmals stark verzögert. Im Fall der Digitalisierung von Staat und Verwaltung werden die Herausforderungen der horizontalen Koordination beispielsweise bei Fragen des ressortübergreifenden Datenaustauschs oder der Implementation von ressortübergreifenden IT-Lösungen deutlich.
- (8) Die öffentlichen Verwaltungen haben seit den späten 1980er-Jahren eine intensive Phase der Modernisierung erlebt. Die Impulse erwiesen sich aber nicht als so stark, dass die Verwaltungen heute stromlinienförmig den Maßstäben des Neuen Steuerungsmodells oder dem internationalen NPM-Standard entsprechen würden. Gleichzeitig haben die vielfältigen Reformaktivitäten zu einer Reformmüdigkeit auf Seiten der Mitarbeiter\*innen geführt, die daher weiteren Reformmaßnahmen reserviert gegenüberstehen. Wie die Erfahrungen mit dieser Reformwelle in die Digitalisierungspolitik hineinspielen, ist noch genauer zu erforschen. Und welche Mischung dabei aus den Prinzipien der Rechtlichkeit der Verwaltung, dem Druck ökonomisch-betriebswirtschaftlicher Rationalität und *Output*-Orientierung, wie er durch *New Public Management* und Folgemodelle erzeugt wurde, und den Möglichkeiten und auch Einschränkungen eines digitalen Verwaltungsvollzuges erwachsen, ist noch offen. Es ist keineswegs ausgemacht, dass die Digitalisierung alle vorherigen Reformbewegungen überrollt oder überwiegt. Plausibel erscheint angesichts des weiterhin vorherrschenden ökonomischen Drucks und der *Output*-Orientierung, dass Digitalisierungsmaßnahmen in der öffentlichen Verwaltung vor allem dort implementiert werden, wo sie in hohem Maße Rationalisierungspotenziale versprechen, wohingegen Digitalisierungsprojekte mit einer stärker partizipativen Ausrichtung in der Tendenz vernachlässigt werden.

- (9) Angesichts der Vielfalt der Digitalisierungsformen sind normative Fragen je nach Spielart unterschiedlich zu beantworten. Unter demokratietheoretischen Gesichtspunkten kann es sein, dass eine bestimmte Variante von Digitalisierung vollkommen problemlos ist und die demokratische Gestaltung von Staat und Verwaltung weder behindert noch groß befördert, sondern einfach nur unterstützend, vereinfachend und gemäßigt beschleunigend wirkt (z. B. *E-Mail*). Zugleich kann eine andere sozio-technische Spielart wie die von einzelnen Unternehmen beherrschten *Social-Media*-Kanäle aufgrund ihres Monopolcharakters und der fehlenden Mitwirkung der Nutzer an den zentralen Entscheidungen der Gestaltung der Netzwerke eher eine „postdemokratische Technologie“ darstellen (Stalder 2016). Wenn sich staatliche Akteure auf eine solche Spielart einlassen, dann kann dies Folgen für die Ausgestaltung von politischen und administrativen Prozessen haben, die einen Machtverlust der Bürger\*innen mit sich bringen. Die Relationen zwischen Nationalstaaten und transnationalen privaten Plattformmonopolisten sind bei allen Digitalisierungsbestrebungen zu bedenken. Für eine reflektierte interdisziplinäre Staats- und Verwaltungswissenschaft scheint ein Kriterien- und Prüfkatalog erforderlich zu sein, der die demokratietheoretische Verträglichkeit bestimmter digitaler Konstellationen zu beurteilen hilft.

---

## Literatur

- Aust, Stefan, und Thomas Ammann. 2016. *Digitale Diktatur: Totalüberwachung Datenmissbrauch Cyberkrieg*. Berlin: Ullstein.
- Bauer, Michael, und Edgar Grande. 2018. *Perspektiven der Verwaltungswissenschaft*. Baden-Baden: Nomos.
- Brown, Alan W., Jerry Fishenden, Mark Thompson, und Will Venters. 2017. Appraising the impact and role of platform models and Government as a Platform (GaaP) in UK Government public service models. Towards a Platform Assessment Framework (PAF). *Government Information Quarterly* 34(2): 167–182.
- Burke, Peter. 2015. *Die Explosion des Wissens. Von der Encyclopédie bis Wikipedia*. Bonn: Bundeszentrale für politische Bildung.
- Casey, Michael, und Paul Vigna. 2017. *Cryptocurrency. Wie virtuelles Geld unsere Gesellschaft verändert*, 2. Aufl. Berlin: Ullstein.
- Dengler, Katharina, und Britta Matthes. 2015. Folgen der Digitalisierung für die Arbeitswelt. Substituierbarkeitspotenziale von Berufen in Deutschland. IAB-Forschungsbericht Nr. 11/2015. Nürnberg: IAB.
- Djeffal, Christian. 2017. Leitlinien der Verwaltungsinnovation und das Internet der Dinge. HIIG discussion paper series no. 2017-04. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2970379](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2970379). Zugegriffen am 20.10.2019.
- Douma, Eva. 2018. *Sicheres Grundeinkommen für alle. Wunschtraum oder realistische Perspektive?* Bonn: Bundeszentrale für politische Bildung.
- Eberl, Ulrich. 2016. *Smarte Maschinen. Wie Künstliche Intelligenz unser Leben verändert*. München: Carl Hanser Verlag.
- Frey, Carl Benedikt, und Osborne, Michael A. 2013. The future of employment. How susceptible are jobs to computerization? Oxford Martin School (OMS) working paper. Oxford: University of Oxford.

- Guggenberger, Bernd. 1994. Das Staatsziel Umweltschutz. Erster Schritt zu einer „konjunktur-unabhängigen“ Umweltpolitik. In *Der Souverän auf der Nebenbühne. Essays und Zwischenrufe zur deutschen Verfassungsdiskussion*, Hrsg. Bernd Guggenberger und Andreas Meier, 241–248. Opladen: Westdeutscher Verlag.
- Hilbert, Martin, und Priscila López. 2011. The world's technological capacity to store, communicate, and compute information. *Science* 332(6025): 60–65.
- Hofstetter, Yvonne. 2016. *Das Ende der Demokratie. Wie künstliche Intelligenz die Politik übernimmt und uns entmündigt*. München: C. Bertelsmann.
- Kucklick, Christoph. 2015. *Die granulare Gesellschaft. Wie das Digitale unsere Wirklichkeit auflöst*. Berlin: Ullstein.
- Kurz, Constanze, und Frank Rieger. 2011. *Die Datenfresser. Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückverlangen*. Frankfurt a. M.: Fischer.
- Mayer-Schönberger, Viktor, und Thomas Ramge. 2017. *Das Digital. Markt, Wertschöpfung und Gerechtigkeit im Datenkapitalismus*. Berlin: Econ.
- Mohabbat Kar, Resa, Basanta Thapa, und Peter Parycek, Hrsg. 2018. *(Un)Berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft*. Berlin: Kompetenzzentrum Öffentliche IT.
- Morozov, Evgeny. 2013. *Smarte neue Welt. Digitale Technik und die Freiheit des Menschen*. München: Karl Blessing.
- Morozov, Evgeny. 2015. Digital technologies and the future of data capitalism. *Social Europe*, 23 June 2015. <https://www.socialeurope.eu/digital-technologies-and-the-future-of-data-capitalism>. Zugegriffen am 20.10.2019.
- Nullmeier, Frank. 2017. Digitale Ökonomie und ihre Folgen für die Entwicklungsrichtung der gesetzlichen Rentenversicherung. *Deutsche Rentenversicherung* 72(3): 249–272.
- OECD. 2015. *Achieving public sector agility at times of fiscal consolidation*. Paris: OECD Publishing.
- O'Flynn, Janine. 2007. From new public management to public value. Paradigmatic change and managerial implications. *The Australian Journal of Public Administration* 66(3): 353–366.
- O'Reilly, Tim. 2010. Government as a platform. In *Open government. Collaboration, transparency, and participation in practice*, Hrsg. Daniel Lathrop und Laurel Ruma. Sebastopol: O'Reilly Media.
- Peinl, René. 2018. Privatleben 4.0. In *Digitalisierung. Segen oder Fluch? Wie die Digitalisierung unsere Lebens- und Arbeitswelt verändert*, Hrsg. Dietmar Wolff und Richard Göbel, 225–252. Heidelberg: Springer.
- Reiter, Renate, und Tanja Klenk. 2019. The manifold meanings of ‚post-New Public Management‘. A systematic literature review. *International Review of Administrative Sciences* 85(1): 11–27.
- Schaar, Peter. 2007. *Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft*. München: Bertelsmann.
- Schallbruch, Martin. 2018. *Schwacher Staat im Netz. Wie die Digitalisierung den Staat in Frage stellt*. Wiesbaden: Springer.
- Schirrmacher, Frank, Hrsg. 2015. *Technologischer Totalitarismus. Eine Debatte*. Berlin: Suhrkamp.
- Schmidt, Eric, und Jared Cohen. 2013. *The new digital age. Reshaping the future of people, nations and business*. New York: Alfred A. Knopf.
- Stalder, Felix. 2016. *Kultur der Digitalität*. Berlin: Suhrkamp.
- Welzer, Harald. 2017. *Die smarte Diktatur. Der Angriff auf unsere Freiheit*. Frankfurt a. M.: Fischer.
- Wewer, Götztrik. 2014. *Open Government, Staat und Demokratie. Aufsätze zu Transparenz, Partizipation und Kollaboration*. Berlin: edition sigma.
- Wirtschaft für Grundeinkommen. 2018. <http://www.wirtschaft-fuer-grundeinkommen.com/supporters>.
- Zuboff, Shoshana. 2015. Big other. Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology* 30(1): 75–89.

---

## **Teil II**

### **Spielarten der Digitalisierung**



---

# Daten, Metadaten, Interoperabilität

Herbert Kubicek, Andreas Breiter und Juliane Jarke

## Inhalt

1 Einführung .....	28
2 Begriffliche Grundlagen .....	28
3 Modellcharakter und Kontextabhängigkeit .....	31
4 Interoperabilität von Daten .....	33
5 Metadaten und Interoperabilität in der Praxis .....	35
6 Zusammenfassung und Schlussfolgerungen .....	38
Literatur .....	39

---

## Zusammenfassung

Häufig ist von Daten die Rede, ohne dass der Terminus definiert wird. Es macht jedoch einen großen Unterschied, ob damit quantitative Angaben oder maschinenlesbare Zeichen gemeint sind. Auch wird meist nicht näher darauf eingegangen, dass der Umgang mit Daten im Wesentlichen auf Metadaten beruht und für den Austausch und die Zusammenführung unterschiedlicher Datenbestände Interoperabilität hergestellt werden muss. Dieser Artikel versucht, entsprechende Grundlagen zu schaffen. Zunächst werden die unterschiedlichen Daten-Begriffe gegenübergestellt. Dann wird auf den Modellcharakter und die Kontextabhängigkeit von Daten eingegangen, bevor Grundlagen der Interoperabilität und die Bedeutung von Metadaten in verschiedenen Anwendungsbereichen dargestellt

---

H. Kubicek (✉)

ifib: Institut für Informationsmanagement Bremen GmbH, Universität Bremen, Bremen, Deutschland  
E-Mail: [kubicek@ifib.de](mailto:kubicek@ifib.de)

A. Breiter

Universität Bremen und Institut für Informationsmanagement Bremen, Bremen, Deutschland  
E-Mail: [abreiter@ifib.de](mailto:abreiter@ifib.de)

J. Jarke

ifib: Institut für Informationsmanagement Bremen GmbH, Universität Bremen, Bremen, Deutschland  
E-Mail: [jjarke@ifib.de](mailto:jjarke@ifib.de)

---

werden. Abschließend wird kurz auf die wohl größte Herausforderung in diesem Zusammenhang eingegangen: auf die Qualität von Daten.

---

### Schlüsselwörter

Big Data · Informationsbegriff · Semantik · Semiotik · Modelle

---

## 1 Einführung

Staat und Verwaltung sind ohne extensive Erhebung und Verarbeitung von Daten nicht denkbar. Ob jemand Bürgerin oder Bürger eines Staates ist, wird seit Jahrhunderten anhand von Daten dokumentiert, die in Registern gespeichert und in amtlichen Dokumenten ausgewiesen werden. Alle ordnungspolitischen Funktionen von Staat und Verwaltung basieren auf Daten und erzeugen Daten. Politische Entscheidungen und Gesetzesvorhaben beruhen auf der Analyse von Daten oder werden durch diese ausgelöst. Staat und Verwaltung nutzten von Anfang an die maschinelle Datenverarbeitung, *EDV* (*Elektronische Datenverarbeitung*), *ADV* (*Automatisierte Datenverarbeitung*), IT (Informationstechnik) genannt. Die erste umfassende Anwendung maschineller Datenverarbeitung war die Volkszählung in den USA im Jahr 1890. Das Urteil des Bundesverfassungsgerichts zur geplanten Volkszählung 1983 in Deutschland hat der staatlichen Datenverarbeitung durch die Prinzipien der Zweckbindung und Erforderlichkeit enge Grenzen gesetzt. Mit dem Internet wurde die bis dahin weitgehend verwaltungsinterne Datenverarbeitung sowohl zu anderen Verwaltungen als auch für Bürgerinnen und Bürger sowie die Wirtschaft geöffnet. Digitalisierung ist insofern eine Fortsetzung von sechzig Jahren Verwaltungsautomation. Mit *Open Data* soll nun nicht nur die Transparenz von Staat und Verwaltung verbessert, sondern auch wirtschaftliches Wachstum durch innovative digitale datengestützte Dienste gefördert werden. Und mit *Big Data* und Algorithmen aus dem Bereich der *Künstlichen Intelligenz* sollen neue und mächtigere Analyse- und Prognosemöglichkeiten entstehen. Stets hat die Erweiterung des Potenzials automatisierter Datenverarbeitung zu Visionen neuer Chancen und zu Befürchtungen neuer Risiken geführt. Kritiker überschätzen dabei häufig die Möglichkeiten der Nutzung und die Aussagekraft von Daten, Befürworter unterschätzen die hohen Voraussetzungen einer bereichsübergreifenden Realisierung der erhofften Wirkungen. Zu Fehleinschätzungen führen ein unscharfer Datenbegriff, eine mangelnde Berücksichtigung des Charakters von Daten als selektive Modelle sowie die unzureichende Auseinandersetzung mit der Bedeutung von Metadaten und der Interoperabilität von Daten aus unterschiedlichen Quellen.

---

## 2 Begriffliche Grundlagen

Das Wort „*Daten*“ hat in verschiedenen wissenschaftlichen Disziplinen, Politikfeldern und Verwaltungsbereichen unterschiedliche Bedeutungen. In Lexika werden Daten definiert als quantitative Angaben oder durch Beobachtungen, Messungen,

statistische Erhebungen gewonnene Angaben, meistens Zahlenwerte. Dies entspricht dem Verständnis von Daten in der Amtlichen Statistik. Etymologisch ist das Wort eine Pluralbildung von „Datum“, lateinisch „gegeben“, (von *dare* = geben) bzw. als Substantiv „das Gegebene“. Darin liegt schon sprachlich eine Ambivalenz. Einerseits werden Daten als etwas Gegebenes angesehen, von dem man auszugehen hat: Die Daten einer Person (Name, Geburtsdatum etc.) oder die Rahmendaten in einer Volkswirtschaft. Gleichzeitig wird ausgedrückt, dass Daten gegeben, also erzeugt und zugeordnet werden, und zwar in einem sozialen Prozess. Volkswirtschaftliche Rahmendaten können durch staatliche Intervention und Gesetzgebung verändert werden.

Nach der Datenschutzgrundverordnung sind in Fortführung früherer Legaldefinitionen *personenbezogene Daten* nicht nur Zahlenwerte, sondern alle „Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person ... beziehen“ (Artikel 4, Ziffer 1). Der Informationsbegriff bezieht sich nicht auf eine bestimmte materielle Form. Daten sind in diesem Sinne elektronische Daten in Datenbanken ebenso wie Akten, und auch Audio-, Bild- und Videoaufzeichnungen. Den Anlass für die Datenschutzgesetzgebung und das später im Volkszählungsurteil geschaffene *Recht auf informationelle Selbstbestimmung* bildeten die enorm gestiegenen Auswertungsmöglichkeiten elektronisch gespeicherter Daten, wie sie jetzt mit *Big Data* und maschinellem Lernen noch einmal eine neue Dimension erreichen. Im Volkszählungsurteil wurden der Verarbeitung personenbezogener Daten mit den Prinzipien der *Zweckbindung* und *Erforderlichkeit* deutliche Grenzen gesetzt. Es dürfen nur die Daten erhoben werden, die für einen definierten Zweck erforderlich sind, und sie dürfen auch nur für diesen Zweck verwendet werden. 2001 wurden in einer Novellierung des Bundesdatenschutzgesetzes die Prinzipien „*Datenvermeidung* und *Datensparsamkeit*“ eingeführt, wonach die Erhebung, Verarbeitung und Nutzung von Daten und die Gestaltung von DV-Systemen an dem Ziel auszurichten sind, mit so wenig personenbezogenen Daten wie möglich auszukommen und wo immer möglich eine Pseudonymisierung oder Anonymisierung vorzusehen (§ 3a BDSG). In Artikel 5 der seit Mai 2018 geltenden Datenschutzgrundverordnung (DSGVO) finden sich das Zweckbindungsgebot in ähnlicher Formulierung und das Erforderlichkeitsprinzip als Grundsatz der „*Datenminimierung*“. Artikel 25 verlangt eine nach dem jeweiligen Stand der Technik ausgerichtete Gestaltung und datenschutzfreundliche Voreinstellungen, was durch Zertifizierung nachgewiesen werden kann. Diese Verpflichtung gilt für jede Art der Digitalisierung im öffentlichen Bereich.

In der *Informatik* wird unter Bezug auf die *Semiotik* zwischen Zeichen, Daten und Informationen unterschieden (z. B. Krcmar 2015, S. 11 ff.). Ein *Zeichen* ist etwas Sicht- oder Hörbares, mit dem jemand aufgrund einer Konvention auf etwas aufmerksam macht, z. B. eine arabische oder römische Ziffer oder ein *Bit* in einem digitalen System. Diese Zeichen entstammen einem gewachsenen oder vereinbarten Zeichenvorrat und können in unterschiedlichen Kulturräumen und Kontexten unterschiedliche Bedeutung haben. Das Zeichen X kann einen Buchstaben oder eine Zahl darstellen. Nach der semiotischen Theorie werden Zeichen nach bestimmten Regeln miteinander in Beziehung gesetzt, die Syntax oder Grammatik genannt werden. Aus dem Zeichenvorrat {0, 1, 2, 6, 8} kann eine Zeichenfolge im Format „12.06.2018“ oder „6.210,68“ gebildet werden.

Wofür die nach Syntaxregeln erzeugten Daten stehen, deren Bedeutung, nennt man *Semantik*. Die semantische Festlegung definiert die erste Zeichenfolge als Datum und die zweite als Währung, nicht als Länge einer Strecke. Daten sind in der Informatik jedoch eine besondere Art von Zeichen, nämlich solche, die maschineninterpretierbar sind. Dazu muss für jedes Datum die Syntax und Semantik festgelegt und kommuniziert werden. Die Syntax legt die Anzahl der Zeichen in einer Zeichenfolge und ihre Untergliederung durch Sonderzeichen (Punkte, Komma) fest. Semantisch wird „12.06.2018“ als Datum in der deutschen Schreibweise und nicht in der englischen definiert, bei der der Monat vor dem Tag genannt wird. Und der Betrag „6.210,68“ als Währung in Euro in deutscher Schreibweise, mit der Trennung von Euro und Cent durch ein Komma. Es ist leicht erkennbar, dass es ohne diese Deklarationen zu Missverständnissen zwischen Computersystemen in Deutschland und England kommen kann. Man spricht in diesem Zusammenhang auch von einer Codierung der Daten und der Verwendung von Codes, wie einer Liste von Währungen, aber auch für Warengruppen und Gebiete nach Postleitzahlen, oder beim Amtlichen Gemeindeschlüssel (AGS) des Statistischen Bundesamtes.

Im Kontext der Digitalisierung ist es wichtig, Daten von Texten klar abzugrenzen. In der *Open-Data*-Literatur wird pointiert unterschieden: *Texte* sind für Menschen verständlich, Daten für Maschinen. Texte sind *maschinenlesbar*, aber nicht maschineninterpretierbar und können deshalb nur bedingt weiterverarbeitet werden. Ein Textverarbeitungsprogramm kann jeden Text mit einer vereinbarten Zeichenmenge aus einem anderen Rechner syntaktisch korrekt wiedergeben, wenn das Format erkannt wird. Aber es kann die inhaltliche Bedeutung (Semantik) nicht ohne Weiteres erkennen. Mit Methoden der sogenannten Künstlichen Intelligenz (KI) sind neue Möglichkeiten entstanden, Texte zu verarbeiten, und weitere zu erwarten. So können auf Maschinellem Lernen basierende Spracherkennungsprogramme unter Berücksichtigung des Kontextes einzelner Wörter Texte zunehmend besser in eine andere Sprache übersetzen. Ob es sich bei dieser Interpretationsleistung um „Verstehen“ handelt, darüber streiten Sprachphilosophen, Hirnforscher und Kognitionsinformatiker seit Jahrzehnten.

Nach der Lehre der Semiotik unterscheiden sich Informationen von Daten durch ihren Zweck- und Handlungsbezug (Pragmatik). Dieselben Daten können für eine Person in einer bestimmten Situation relevantes handlungsbezogenes Wissen und damit eine wertvolle Information sein und für andere Personen völlig belanglos und uninteressant. Im ingenieurwissenschaftlichen Verständnis der ISO-Standards (*International Organization for Standardization*) sind Informationen hingegen generell Wissen, unabhängig davon, ob sie handlungsrelevant sind. In der Betriebswirtschaftslehre wird beklagt, dass Unternehmen zu viele Daten, aber zu wenig Informationen haben. Es ist Aufgabe des *Informationsmanagements*, dies zu ändern, also Informationen zur richtigen Zeit, am richtigen Ort, in der richtigen Qualität bereitzustellen (Krcmar 2015). Für die Verwaltung gilt dies genauso. In beiden Bereichen werden *Big-Data*-Analyseverfahren als Mittel angesehen, um aus Daten Informationen zu machen.

Der Daten-Begriff in der internationalen technischen Normung bezieht sich nicht auf die Semiotik. Nach ISO/IEC 2382-1 „Informationstechnik – Begriffe“ (seit

1993) sind *Data*: „a reinterpretable representation of information in a formalized manner, suitable for communication, interpretation, or processing“ – eine wieder interpretierbare Darstellung von Information in formalisierter Art, geeignet zur Kommunikation, Interpretation oder Verarbeitung. Dabei wird der Begriff „Information“ nicht definiert.

In den Wirtschafts- und Rechtswissenschaften wird diskutiert, ob Daten *materielle* oder *immaterielle Güter* sind. Sicher ist, dass die physischen Objekte, auf denen Daten gespeichert werden (Datenträger), von den Daten selbst zu trennen sind. Strittig ist, ob und wie diese Daten wie Sachen zu behandeln sind, an denen man *Eigentum* erwerben kann, oder ob es sich um immaterielle, geistige Objekte handelt, an denen ein *Urheberrecht* besteht, aus dem die Überlassung von Nutzungsrechten abgeleitet werden kann. Da dies auch eine Rechtsunsicherheit in der Praxis zur Folge hat, wo Daten ein hohes wirtschaftliches Wachstumspotenzial zugeschrieben wird, wird über *Datengesetze* und neue Eigentumsformen *sui generis* diskutiert. Im Koalitionsvertrag von CDU, CSU und SPD von 2017 haben die Regierungsparteien angekündigt, die Frage, ob und wie ein *Eigentum an Daten* ausgestaltet sein kann, zügig anzugehen (Zeile 6085). Das Hauptproblem besteht darin, dass bei neueren digitalen Anwendungen die Erzeugung von Daten nicht mehr einem Urheber oder Eigentümer zugeordnet werden kann. Ein Beispiel sind die Bewegungsdaten von Kraftfahrzeugen, die durch ein vom Hersteller entwickeltes Programm auf einem vom Eigentümer mit dem Auto gekauften Datenträger gespeichert und nur durch das Fahrverhalten des Besitzers erzeugt werden. Ökonomen bezweifeln daher, dass Daten als Privatgüter anzusehen sind und schlagen stattdessen vor, sie als öffentliche Güter zu behandeln (Jentzsch 2018). In einem Gutachten für die Konrad-Adenauer-Stiftung stellt Karl-Heinz Fezer (2018) ein Eigentumsrecht *sui generis* des Bürgers oder Verbrauchers zur Diskussion, der durch sein Verhalten die Daten generiert und daher an daraus resultierenden Erlösen beteiligt werden soll.

Offen ist auch die Frage, ob Daten wie anderes Vermögen *vererbt* werden und ob Erben Eigentum an *online* gespeicherten Daten der Erblasser erwerben und daher den Zugang zu diesen Daten vom jeweiligen *Provider* verlangen können. Im Juli 2018 hat der Bundesgerichtshof entschieden, dass die Daten des *Facebook-Accounts* einer verstorbenen Tochter an die Eltern herauszugeben sind, weil es sich um eine Frage des Erbrechts handele und diese Daten auf einem externen Speicher genau so zu behandeln sind wie ein Tagebuch im Zimmer der Tochter, das in das Eigentum der Erben übergeht. *Facebook* hatte dies mit Verweis auf seine Verpflichtung auf das Telekommunikationsgeheimnis zunächst verweigert.

---

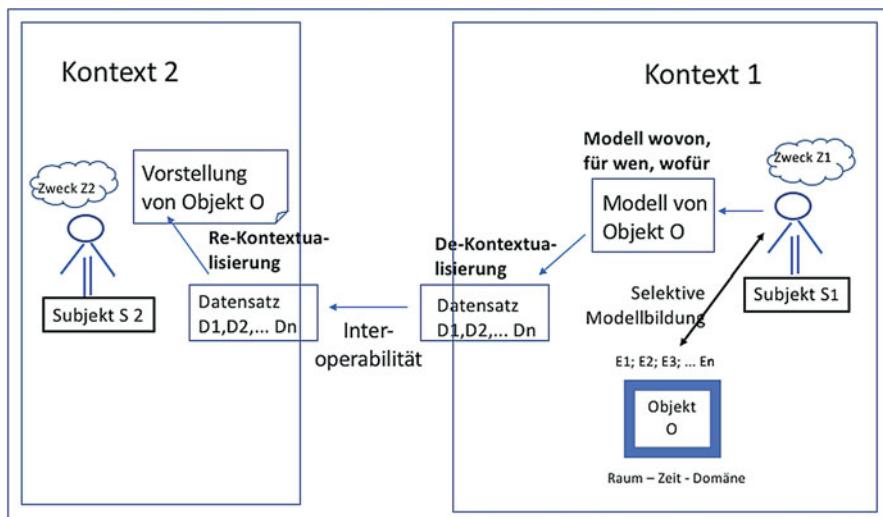
### 3 Modellcharakter und Kontextabhängigkeit

Die Unter- und Überschätzung von Daten resultiert aus einer ungenügenden Beschäftigung mit ihrer Selektivität und Kontextabhängigkeit. Diese ergibt sich aus dem Modellcharakter von Daten und hat Folgen für die Möglichkeit des Datenaustauschs zwischen verschiedenen verarbeitenden Stellen. Diese müssen durch Ver-

einbarungen zur Interoperabilität bilateral oder bereichsbezogen erst geschaffen werden (Abb. 1).

Zur Entwicklung von digitalen Anwendungen gehört die sogenannte Modellierung des Gegenstandsbereichs. Sie führt zu Datenmodellen, für die es verschiedene Modellierungssprachen gibt, wie z. B. die *Universal Modeling Language* (UML). Datenmodelle stellen dar, welche Daten mit welchen Beziehungen zueinander verarbeitet werden sollen. Sie sind eine Grundlage für die Anlage von Datenbanken. In der Informatik wird nicht immer deutlich gemacht, welch große Tragweite solche Modellierungsentscheidungen haben. Auch in der aktuellen Diskussion über *Big Data* wird mehr über die Algorithmen als über die Daten diskutiert, aus denen die Algorithmen Informationen machen (sollen).

In der Lehre der Semiotik stehen Zeichen in einer Dreiecksbeziehung zwischen einem Bezeichner (Subjekt) und etwas Bezeichnetem (Objekt). Diese bilden den Kontext. Nach Steinmüller (1993, S. 211 ff.) sind Daten Modelle von etwas für jemanden, die zu einem bestimmten Zweck geschaffen werden („Modell wovon – für wen – wofür“). Wie alle Modelle sind sie daher selektive Abbilder der jeweiligen Objekte. Einige Eigenschaften (E1, E2, ...) werden in das Modell aufgenommen und als Daten in einem Datensatz definiert (D1, D2, ...), aus dem dieser Kontext allerdings nicht mehr unmittelbar erkennbar ist, sie werden de-kontextualisiert. Über die Semantik wird dieser Kontext nur teilweise erfasst. Im Datenschutzrecht wird dieser Aspekt durch den Zweck der Verarbeitung erfasst und mündet in das Zweckbindungsgebot. Es ist verboten, Daten, die für einen bestimmten Zweck erhoben worden sind, ohne Erlaubnis für einen anderen Zweck – und damit in einem anderen Kontext – zu verwenden. Ein Beispiel ist die Wohnadresse einer Person, die als Anschrift angegeben wurde. Im Rahmen des sogenannten Kredit-*Scoring* werden



**Abb. 1** Daten als kontextabhängige Modelle und Interoperabilität. (Quelle: Eigene Darstellung)

diese von Kreditauskunfteien aber auch als ein Indikator für die Kreditwürdigkeit der in einer bestimmten Nachbarschaft wohnenden Personen verwendet, also aus einem Kontext in einen anderen übertragen, obwohl nicht sicher ist, dass diese Daten im neuen Kontext dieselbe Validität haben. Mit der Neufassung des BDSG wurde in § 31 der Schutz der Betroffenen beim *Scoring* gestärkt. Anschriftendaten dürfen für die Wahrscheinlichkeitsberechnung nur verwendet werden, wenn die Betroffenen zuvor darüber unterrichtet wurden.

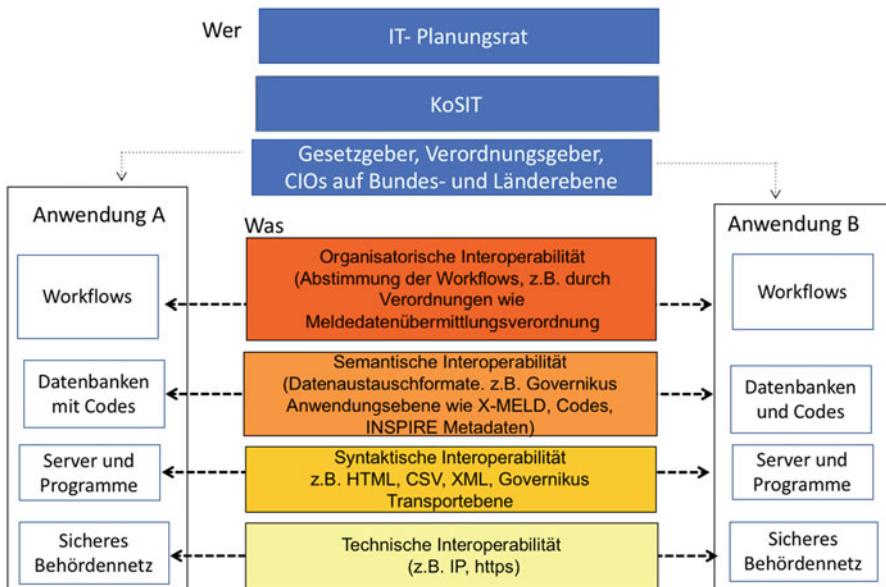
Die Selektivität, die Kontextabhängigkeit und der Zweckbezug von Daten („Modell wovon – für wen – wofür“) werden innerhalb der Sozialwissenschaften in den sog. *Critical Data Studies*, überwiegend im angelsächsischen Raum, thematisiert. Diese betonen, dass Daten nicht „gegeben“ sind, sondern „generiert“ werden und niemals „roh“ sind. Gitelman (2013) bezeichnet Rohdaten als *Oxymoron*, als einen Widerspruch in sich selbst. Daten sind nicht neutral oder objektiv, sondern existieren immer in Abhängigkeit von den Ideen, Instrumenten, Praktiken, Kontexten und dem Wissen, die sie generieren, verarbeiten und analysieren (Kitchin 2014). Sie sind keine rein technischen Artefakte, die einen Einfluss auf soziale Praxis haben, sondern werden innerhalb sozialer Praxis erzeugt, interpretiert und verarbeitet. Innerhalb der *Critical Data Studies* wird daher ein Schwerpunkt auf die Analyse der rekursiven Beziehung von Daten und Gesellschaft gelegt (Dalton et al. 2016; Jarke 2018), also danach gefragt, wie soziale Akteure Daten prägen und wie diese Daten wiederum soziale Wirklichkeit formen. Dabei wird ein weiterer Datenbegriff als der in der Informatik verwendet.

---

## 4 Interoperabilität von Daten

Wenn Daten im engeren Sinne von einer Quelle aus einem Kontext an eine andere Stelle zur maschinellen Weiterverarbeitung übermittelt werden, müssen die syntaktischen und semantischen Regeln vereinheitlicht, standardisiert werden. Es müssen Datenaustauschformate nach bestimmten Standards geschaffen werden. Sie machen unterschiedliche Quell- und Zielsysteme kompatibel oder interoperabel. Die Alternative wäre eine physische Zentralisierung der Daten in einer zentralen Datenbank, wie dies zum Beispiel Belgien und Österreich mit den Melddaten in einem zentralen nationalen Register getan haben. Wenn man dies, wie in Deutschland, politisch nicht will, muss man mit rechtlichen Mitteln Interoperabilität zwischen den vielen hundert kommunalen Melderegistern herstellen. In diesem Fall wurde mit der Melddatenübermittlungsverordnung der Standard X-MELD für den Austausch von Melddaten im Rahmen der Rückmeldung zwischen der Wegzugs- und Zuzugs-kommune verpflichtend vorgeschrieben.

Im Einzelnen werden verschiedene *Ebenen der Interoperabilität* zwischen Systemen unterschieden, für die es unterschiedliche Arten von Standards gibt (Abb. 2). Auf der syntaktischen Ebene muss vereinbart werden, welche Zeichen und Formate verwendet werden und durch welche Zeichen einzelne Datenfelder voneinander abgegrenzt werden. Auf der semantischen Ebene muss vereinbart werden, aus welchen inhaltlichen Feldern ein Datensatz in welcher Reihenfolge besteht und



**Abb. 2** Ebenen der Interoperabilität und ihre Governance. (Quelle: Eigene Darstellung)

mit welchen Codes die Daten in den einzelnen Feldern erzeugt werden. Weiterverarbeitung erfolgt zu bestimmten Zwecken. Der pragmatische Aspekt wird durch die organisatorische Interoperabilität erfasst, indem die *Workflows* der Datenentstehung und der -verwendung aufeinander abgestimmt werden.

Davon zu unterscheiden ist die Organisation von Interoperabilität, auch als *Governance* bezeichnet, d. h. explizite Regelungen, wer Vorschläge wo einbringt, wer den Abstimmungsprozess zwischen den zu Beteiligenden organisiert, wer die Anwendung der Standards verbindlich macht und wer die Einhaltung überwacht (ausführlicher Kubicek et al. 2011).

Für die Bundesverwaltung hat der IT-Beauftragte der Bundesregierung in Abstimmung mit den Ressorts einen SAGA (Standards und Architekturen für *E-Government*-Anwendungen) genannten Katalog der verpflichtend gemachten Standards zusammengestellt. Da viele *E-Government*-Anwendungen IT-Systeme von Bund, Ländern und Gemeinden betreffen, wurden 2009 mit der Föderalismusreform II die rechtlichen Voraussetzungen für eine lückenlose und medienbruchfreie elektronische Kommunikation zwischen den Behörden von Bund, Ländern und Kommunen geschaffen und mit dem Staatsvertrag über die Errichtung des *IT-Planungsrates* umgesetzt. Bund und Länder koordinieren in diesem Gremium ihre IT-Planung, verabschieden Standards und vereinbaren Pilotprojekte, bei denen jeweils ein Bundesland federführend ist. Für die Standardisierung gemeinsamer *E-Government*-Dienste wurde die *Koordinierungsstelle für IT-Standards* (KoSIT) gegründet, die u. a. auf Initiative der Fachministerkonferenzen tätig wird.

## 5 Metadaten und Interoperabilität in der Praxis

Interoperabilitätsstandards erlauben einen korrekten Austausch syntaktisch und semantisch definierter Daten für vereinbarte Zwecke. Sie erläutern jedoch nicht den Kontext, die Inhalte der Daten oder ihre Qualität. Dies ist Aufgabe sogenannter *Metadaten*: Daten über Daten. Auch hier gibt es zwei Ebenen: die inhaltliche Definition des Metadatensatzes und die *Governance* des Entwicklungs- und Verbreitungsprozesses. Denn Metadaten werden für Daten ganzer Bereiche oder Sektoren entwickelt, betreffen Daten vieler zumeist ähnlicher, aber geografisch verteilter Stellen und müssen daher auch interoperabel sein.

Der bekannteste Fall von Metadaten ist der *Bibliothekskatalog* (OPAC) mit Referenzdaten der Objekte im Bestand. Ein Metadatensatz beinhaltet hier Angaben zu Autor, Titel, Umfang, Verlag, ISBN oder ISSN und Standort sowie Zuordnung zu einem Themenbereich und passende Schlagwörter. Die beiden letzten Aspekte erweisen sich im Gegenstandsbereich der Bibliotheken, der alle Lebensbereiche und Wissensgebiete umfasst, als besonders schwierig für eine verbindliche Klassifizierung und Standardisierung. Für die Verschlagwortung ist ein *Thesaurus*, ein normierter und gepflegter Schlagwortbestand mit Synonymen und Homonymen, erforderlich. Die gut vernetzten deutschen Bibliotheken haben eine Schlagwortnormdatei als gemeinsamen Thesaurus geschaffen. Angesichts der *Online-Kataloge* im Internet wurde Mitte der 1990er-Jahre auf internationaler Ebene ein Metadatenstandard für Webressourcen entwickelt. Der Dublin Core Metadatensatz enthält 15 Felder zur einheitlichen Kennzeichnung von Ressourcen (<http://dublincore.org/>). Verantwortlich für Entwicklung, Weiterentwicklung und Pflege ist die *Dublin Core Metadata Initiative* (DSMI), die sich aus Freiwilligen aus Bibliotheken in der ganzen Welt zusammensetzt und in mehreren Arbeitsgruppen wirkt. Die Anwendung außerhalb von Bibliotheken ist gering. Google und andere Suchmaschinen haben den Bedarf nach einem derartigen offenen System aufgefangen.

Überwiegend sind Interoperabilitätsstandards auf der semantischen Ebene ange-siedelt und Metadaten bereichsspezifisch. Am weitesten fortgeschritten ist die Standardisierung von Daten und Metadaten für *Umwelt- und Geodaten*. Hier ist die Abstimmungsnotwendigkeit besonders groß. Messwerte von Umweltbelastungen werden dezentral erfasst, sollen aber gemeinsam für größere Flächen bundesweit angezeigt und ausgewertet werden. Karten, für die Geo-Daten dezentral von Vermessungsämtern erhoben und in Katasterämtern aufbereitet und mit Inhalten gefüllt werden, sollen ebenfalls auf Landes- und Bundesebene aggregiert und mit weiteren Daten angereichert werden. Für Umweltdaten im Sinne der EU-Richtlinie über den Zugang der Öffentlichkeit zu Umweltinformationen (Richtlinie 2003/4/EG) wurde 2003 eine Vereinbarung zwischen Bund und Ländern geschlossen, die den gemeinsamen Betrieb sowie die Entwicklung und Pflege des Metainformationssystems *Umwelt-Datenkatalog* (UDK) und des Umweltinformationsnetzes Deutschland (*German Environmental Information Network* [GEIN]) regelt. Von 2006 bis 2014 hat das *PortalU* (wie „Umwelt“) die dezentralen Angebote der Verwaltungen nach den Umweltinformationsgesetzen der Länder und des Bundes unter einem gemein-

samen Dach zugänglich gemacht. Die inhaltliche und technische Verantwortung lag bei der Koordinierungsstelle PortalU im Niedersächsischen Ministerium für Umwelt und Klimaschutz, die von Bund und Ländern gemeinsam finanziert wurde. Diese haben 2014 die Verwaltungsvereinbarung gekündigt, so dass das Portal ohne öffentliche Angabe von Gründen eingestellt wurde.

Für *Geo-Daten* gilt seit 2007 die EU-Richtlinie INSPIRE, die durch *Geodatenzugangsgesetze* auf Bundes- und Landesebene umgesetzt wurde und vorschreibt, wie durch Harmonisierung und Interoperabilität der Daten, Metadaten und Daten-dienste eine einheitliche Geodateninfrastruktur geschaffen wird. Auch hier haben Bund und Länder über eine Verwaltungsvereinbarung die organisatorischen Voraus-setzungen für die Vernetzung von raumbezogenen Daten im Rahmen einer Geo-Daten-Infrastruktur Deutschland (GDI-DE) geschaffen. Betreiberorganisation ist die Koordinierungsstelle GDI-DE im Bundesamt für Kartografie und Geodäsie (BKG), die im Auftrag eines gemeinsamen Entscheidungs- und Steuerungsgremiums von Bund, Ländern und Kommunen tätig ist. In der Richtlinie wurden Fristen für die nationale Umsetzung einheitlicher Definitionen von genau definierten Geo-Basisdaten und Geo-Anwendungsdaten vorgegeben. 2016 wurde der letzte Umsetzungsbericht veröffentlicht.

Deutlich weniger standardisiert und durch behördliche Informationssysteme durchdrungen ist die *Bildungsverwaltung*. Erst durch Änderungen der Landes- und des Bundesstatistikgesetzes in den letzten fünf Jahren wird eine einheitliche Daten-lieferung eingefordert. Das gilt sowohl für die Schule (einheitliche Schüler-ID) als auch den Hochschulbereich (z. B. Erfassung von Promovierenden). Erst durch das Nationale Bildungspanel besteht die Möglichkeit zu Längsschnittstudien (<https://www.neps-data.de/>). Es gibt eine Oligopolstruktur bei den Softwareherstellern und wenig Interesse an länderübergreifender Standardisierung. Hierbei spielen landes-politische Aspekte (Kultushoheit) sowie datenschutzrechtliche Fragen eine Rolle. Zudem fehlen Abstimmungsgremien, in denen ein Aushandlungsprozess zwischen Herstellern, Verwaltung und Nutzern erfolgen könnte – weder die Kultusminister-konferenz noch die Gemeinsame Wissenschaftskonferenz sind hierzu hinreichend aufgestellt. Ein neues Feld, durch das eine stärkere Dynamik erwartet werden kann, sind *Offene Forschungsdaten*, die sowohl durch EU-weite Ansätze (*EU Science Cloud*) als auch Bund-Länder-Initiativen für Nationale Forschungsdateninfrastruk-turen forciert werden.

Einerseits hoch standardisiert, andererseits stark individualisiert sind Gesund-heitsdaten und damit auch die Gesundheitsverwaltung. Während medizinische Ver-sorgungsdaten weltweiten Standards unterliegen und durch Krankenhausinfor-mationssysteme und Systeme der Krankenkassen verarbeitet werden, sind die Schnittstellen zu anderen Versorgungseinrichtungen wie Apotheken, niedergelasse-nen Ärzten etc. kaum realisiert worden. Die Einführung der elektronischen Gesund-heitskarte verzögert sich seit Jahrzehnten. Noch komplexer stellt sich die Situation für persönliche Daten der Bürger und Bürgerinnen dar, die im Zuge der „Selbstver-messung“ („Quantified Self“) gesammelt werden. Je nach *App* und Anbieter werden Daten nach unterschiedlichen Standards erhoben, ihre Kalibrierung wird system-bezogen vorgenommen und Datenaustausch findet in der Regel nicht statt – teilweise

kann die Nutzerin auf die eigenen Daten im geschlossenen Ökosystem eines Herstellers nicht mehr zugreifen (Lupton 2016).

Eine besondere Herausforderung an die Interoperabilität von Metadaten besteht bei den sogenannten *Offenen Verwaltungsdaten* (*Open Government Data*). Nach einer Verwaltungsvereinbarung zwischen dem Bund und einigen Ländern sollen alle Daten, die nicht speziellen Beschränkungen unterliegen, nicht nur auf ihren jeweiligen Landesportalen über Datenkataloge zur Weiternutzung bereitgestellt, sondern die Metadaten auch an das Bundesportal *gov.data.de* gemeldet werden. Vier Länder, Bayern, Hessen, Niedersachsen und Sachsen-Anhalt, sind nicht beigetreten. Durch diese Zusammenführung sollen Entwickler, Wissenschaftler\*innen, Journalist\*innen und andere mit Hilfe eines zentralen Datenkatalogs erkennen, wo sie bestimmte Datensätze finden. Die Landesportale speisen sich wiederum teilweise aus kommunalen Datenportalen und erfassen diese Daten ebenfalls nicht selbst, sondern auch nur die Metadaten. Wie gut das Bundesportal Interessenten bei der Suche und dem Auffinden von Datensätzen unterstützt, hängt also entscheidend von diesen Metadaten ab. Diese sind aber auf der anderen Seite eine Hürde bei der Bereitstellung von Daten, weil sie von den datenhaltenden Stellen nach einheitlichen Regeln definiert und eingegeben werden müssen. Bisher gibt es unterschiedliche Metadaten-Standards für Offene Verwaltungsdaten. Neben dem von der *Open Knowledge Foundation* in Großbritannien (OKF) entwickelten Datenkatalog CKAN (*Comprehensive Knowledge Archive Network*) mit einem eigenen Metadatensatz, der von vielen kommunalen Portalen verwendet wird, hat der IT-Planungsrat nach einem ersten Standardisierungsversuch mit einem eigenen nationalen Metadatensatz 2018 einen für Bund und Länder verbindlichen Metadatenstandard verabschiedet. Dabei handelt es sich um eine deutsche Adaption des EU-Standards DCAT-AP, der das bisherige Metadatenmodell OGD.1.1 ablösen soll (*Data Catalogue Application Profile* des *W3C Data Catalog DCAT*). Als Vorteile nennt das für die Erarbeitung dieses Vorschlags federführende Portal Sachsen einen noch einfacheren Einstieg in die Veröffentlichung durch wenige Pflichtfelder, die Einführung der Kategorie „empfohlene“ Informationen als Kompromiss zwischen Verbindlichkeit und Flexibilität, die Existenz einer ganzen Reihe verbindlicher Vokabulare und die Interoperabilität zu anderen europäischen Portalen. Mit nur fünf Angaben als Pflichtfelder in diesem Metadatensatz ist die Aussagekraft für Interessenten sehr begrenzt. Generell fehlt auch im Vergleich zu anderen Bereichen eine Verpflichtung zur Einhaltung selbst dieser minimalen Metadaten.

Besondere politische Beachtung findet die Interoperabilität von Daten bei den verschiedenen Sicherheitsbehörden auf Länder- und Bundesebene sowie auf internationaler Ebene. Immer wieder wird nach Berichten über Straftaten, die bei einem Datenaustausch zwischen Behörden eventuell hätten vermieden werden können, eine bessere Abstimmung und teilweise auch eine Zusammenführung von Dateien gefordert und häufig wohl auch vorgenommen. Einzelfälle belegen, dass die interoperable Vernetzung zwar Möglichkeiten schafft, aber noch nicht garantiert, dass auch alle vorgesehenen Daten tatsächlich weitergegeben werden.

Aktuell stehen die Verwaltungen von Kommunen, Landes- und Bundesbehörden mit dem „Once Only-Prinzip“ vor der wahrscheinlich größten datenbezogenen

Verwaltungsreform, deren Bedeutung jedoch noch nicht allen Beteiligten deutlich zu sein scheint. *Once Only* heißt, die Verwaltung darf nur einmal nach bestimmten Daten fragen und muss, bevor sie Bürger\*innen oder Unternehmen fragt, prüfen, ob die begehrten Daten nicht bereits bei einer anderen Stelle vorliegen. Um Millionen von Anfragen zwischen Behörden zu vermeiden, läuft das darauf hinaus, für bestimmte Daten nur noch ein zentrales Register einzurichten. In Belgien wurde dazu ein Gesetz erlassen, das für definierte Daten landesweit eine einzige authentische Quelle (*one authentic source*) vorschreibt. In anderen Ländern heißen sie Basisregister. Dabei geht es nicht nur um Personenstammdaten und Melderegister. In der Gesamtheit der Implementierungen in der EU gibt es weitere zentrale Register für Daten über ausländische Einwohner\*innen, Personenstand, Unternehmen, Liegenschaften, Einkommen, Bezug von Sozialleistungen, die den von Bürger\*innen und Unternehmen zu leistenden bürokratischen Aufwand erheblich reduzieren können. Während auf EU-Ebene das *Once Only*-Prinzip ein Grundprinzip des E-Government-Aktionsplans 2016 bis 2020 ist und Mitgliedstaaten wie Belgien, Estland oder die Niederlande die gesetzlichen, technischen und organisatorischen Voraussetzungen für die Umsetzung geschaffen haben, gibt es in Deutschland nur vage Absichtserklärungen des IT-Planungsrats. Ein zentrales Bundesmelderegister wurde bisher von den Bundesländern abgelehnt. Nach wie vor muss man bei jedem Antrag bei jeder Behörde immer wieder dieselben Angaben zur Person und Adresse machen, obwohl sie nach dem erwähnten X-MELD-Datensatz einfach abgefragt werden könnten. Das E-Government-Gesetz hat dazu die datenschutzrechtlichen Voraussetzungen geschaffen, doch der Widerstand gegen die Aufgabe eigener Datenbestände ist groß.

---

## 6 Zusammenfassung und Schlussfolgerungen

Die Kontextabhängigkeit von Daten hat nicht nur eine semantische Dimension, sondern vor allem eine pragmatische, auf die Verwendung bezogene. In verschiedenen Handlungskontexten, Verwaltungsbereichen und Politikfeldern werden ganz unterschiedliche Anforderungen an die Qualität von Daten sowie die Garantie und Haftung für diese Qualität gestellt. An die Korrektheit und Aktualität von Fahndungsdaten, Lebensmittelwarnungen oder Messungen von Luftbelastungen in Verbindung mit Fahrverboten werden andere Anforderungen gestellt als an Daten der Amtlichen Statistik und wieder andere als an einen Veranstaltungskalender auf einem kommunalen Internetportal. Datenhaltende Stellen können in manchen Fällen, wie bei den Offenen Daten, die Gewährleistung ausschließen, in anderen Fällen nicht. Der kurze Überblick über die Interoperabilität von Daten zeigt auch, dass es große bereichsspezifische Unterschiede in den Bemühungen um eine hohe Datenqualität gibt.

Für die aktuelle Diskussion zu Digitalisierung, *Big Data* und *Open Data* sind daraus mindestens zwei Schlussfolgerungen zu ziehen:

- Pauschale Aussagen über die Bedeutung oder die Folgen von *Big Data* und *Open Data*, wie sie häufig getroffen werden, sind unseriös und irreführend, wenn

einzelne Beispiele verallgemeinert werden. Erforderlich ist eine Differenzierung nach Herkunfts- und Verwendungskontexten, um das Potenzial und dessen Realisierungsmöglichkeiten verlässlich einschätzen zu können.

- Es fehlen Beispiele für eine angebliche datengetriebene („data driven“) Digitalisierung bzw. Verwaltungsreform. Die hier geschilderten Beispiele zeigen eher, dass Verwaltungen in vielen Bereichen sich schwertun, die erforderlichen Daten zusammenzutreiben.

---

## Literatur

- Dalton, Craig M., Linnet Taylor, und Jim Thatcher. 2016. Critical data studies. A dialog on data and space. *Big Data & Society* 3(1). <https://doi.org/10.1177/2053951716648346>.
- Fezer, Karl-Heinz. 2018. *Repräsentatives Dateneigentum. Ein zivilgesellschaftliches Bürgerrecht*. Sankt Augustin/Berlin: Konrad Adenauer Stiftung. [https://www.kas.de/c/document\\_library/get\\_file?uuid=f828a351-a2f6-11c1-b720-1aa08eaccff9&groupId=252038](https://www.kas.de/c/document_library/get_file?uuid=f828a351-a2f6-11c1-b720-1aa08eaccff9&groupId=252038). Zugegriffen am 07.10.2019.
- Gitelman, Lisa, Hrsg. 2013. „Raw Data“ Is an Oxymoron. Cambridge, MA: MIT Press.
- Jarke, Juliane. 2018. Digitalisierung und Gesellschaft. *Soziologische Revue* 41(1): 3–20.
- Jentzsch, Nicola. 2018. *Dateneigentum – Eine gute Idee für die Datenökonomie?* Berlin: Stiftung Neue Verantwortung e. V. [https://www.stiftung-nv.de/sites/default/files/nicola\\_jentzsch\\_daten\\_eigentum.pdf](https://www.stiftung-nv.de/sites/default/files/nicola_jentzsch_daten_eigentum.pdf). Zugegriffen am 07.10.2019.
- Kitchin, Rob. 2014. *The data revolution. Big data, open data, data infrastructures and their consequences*. Los Angeles: Sage.
- Krcmar, Helmut. 2015. *Informationsmanagement*, 6. Aufl. Berlin/Heidelberg: Springer Gabler.
- Kubicek, Herbert, Ralf Cimander, und Hans Jochen Scholl. 2011. *Organizational Interoperability in E-Government. Lessons from 77 European Good-Practice Cases*. Heidelberg: Springer.
- Lupton, Deborah. 2016. *The quantified self*. Cambridge: Polity.
- Steinmüller, Wilhelm. 1993. *Informationstechnologie und Gesellschaft. Einführung in die Ange-wandte Informatik*. Darmstadt: Wissenschaftliche Buchgesellschaft.



---

# Staatliche Regulierung durch Big Data und Algorithmen

Sebastian Haunss und Lena Ulbricht

## Inhalt

1 Klärung der Begriffe .....	42
2 Theoretische Grundlagen .....	43
3 Praktische Anwendungsfelder .....	44
4 Perspektiven für Staat und Verwaltung .....	47
Literatur .....	49

---

## Zusammenfassung

Beim Einsatz von *big data* und Algorithmen in Staat und Verwaltung ist zwischen unterschiedlichen Aspekten der technischen Instrumente und verschiedenen Dimensionen von Regulierung zu unterscheiden. Auf dieser Grundlage lässt sich feststellen, wo bereits Veränderungen und Wirkungen sichtbar werden und welche Reichweite diese Veränderungen haben. Die am weitesten reichenden Veränderungen staatlicher Regulierung durch *big data* und Algorithmen zeigen sich bisher außerhalb Europas, doch auch in deutschsprachigen Ländern gibt es zahlreiche Beispiele.

Anhand der Diskussion verschiedener Anwendungsfälle ist festzustellen, dass *big data* von staatlichen Organisationen bisher weitgehend dafür eingesetzt

---

S. Haunss (✉)

SOCIUM Forschungszentrum Ungleichheit und Sozialpolitik, Universität Bremen, Bremen, Deutschland

E-Mail: [sebastian.haunss@uni-bremen.de](mailto:sebastian.haunss@uni-bremen.de)

L. Ulbricht

Weizenbaum-Institut für die vernetzte Gesellschaft, Wissenschaftszentrum Berlin für Sozialforschung, Berlin, Deutschland

E-Mail: [lena.ulbricht@wzb.eu](mailto:lena.ulbricht@wzb.eu)

wird, um konkrete Regeln zu setzen und zu implementieren und im Rahmen algorithmischer Regulierung Regeln stärker nach Zielgruppen zu differenzieren. Weitergehende Programme, die eine *big data*-basierte Regulierung vielfältiger Lebensbereiche zum Ziel haben, existieren bisher in demokratischen Staaten noch nicht.

### Schlüsselwörter

Big data · Algorithmic regulation · Regulierung · Social credit · Entscheidung

## 1 Klärung der Begriffe

*Big data* meint die massenhafte Sammlung und Auswertung der vielfältigen Daten, deren Umfang, Diversität und Erhebungsfrequenz durch die Digitalisierung aller Lebensbereiche rapide zunimmt (boyd und Crawford 2012). Staatliche Verwaltungen arbeiten schon sehr lange mit Datensätzen, die zumindest zwei der drei gängigen Kriterien für *big data – volume, variety und velocity* – erfüllen: Bei Zensus-, Melde-, Steuer- und Sozialversicherungsdaten handelt es sich um Datensätze großen Volumens sowie großer Vielfalt. In der Regel fehlt diesen Daten zwar die dritte Dimension, die hohe Geschwindigkeit der Datengenerierung, diese wird allerdings auch nicht von allen Definitionen vorausgesetzt. Durch die Verfügbarkeit großer und diverser Datensätze im Zuge der Digitalisierung würde sich für staatliche Verwaltungen zunächst einmal wenig ändern. Allerdings geht es in der Debatte um *big data* nicht allein um die Daten selbst, sondern zu einem wesentlichen Teil um die Möglichkeiten der Datenanalyse, die sich in den letzten Jahren dramatisch verändert haben. Fortschritte im Bereich der explorativen Datenanalyse und des maschinellen Lernens erlauben es heute, viel größere Datenbestände in viel kürzerer Zeit zu analysieren. Die sprichwörtliche Nadel im Heuhaufen zu finden, stellt für aktuelle Analysemethoden kein Problem mehr da.

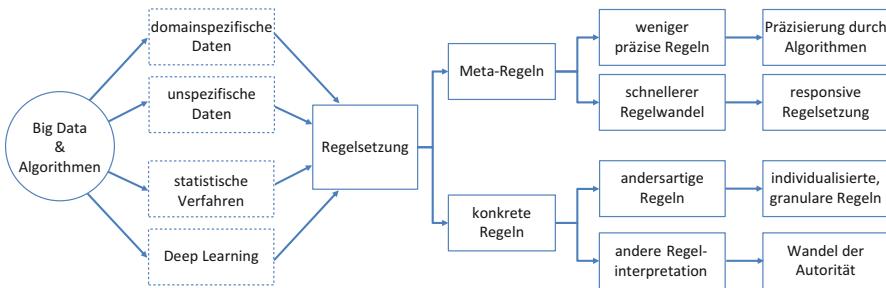
Algorithmen bezeichnen computergestützte Verfahren, die einen Input nach bestimmten Regeln zu einem Output transformieren. Algorithmen können die Bedingungen staatlicher Regulierung verändern. Die sogenannte *algorithmic regulation* beschreibt Entscheidungssysteme, die auf adaptiver computergestützter Informationsverarbeitung beruhen und für Regulierung eingesetzt werden, also für die absichtsvolle Beeinflussung von Verhalten (Yeung 2017). Regulierung umfasst entsprechend ganz verschiedene Praktiken unterschiedlichen Formalitätsgrades: Gesetze und Verordnungen, aber auch informale Instrumente der Verhaltensbeeinflussung, „harte“ sowie „weiche“ Steuerung. Natürlich wird *big data* je nach Instrument in unterschiedlichem Ausmaß eingesetzt. In welcher Hinsicht *big data* und Algorithmen staatliche Regulierung bereits prägen, lässt sich nicht allein mit Blick auf den deutschsprachigen Raum betrachten. Zwar gibt es hier erste Erfahrungen, doch ist die Debatte stark von Erfahrungen im Ausland geprägt. Für die Erprobung von *big data* und Algorithmen in neuen Bereichen staatlicher Steuerung spielen Erfahrungen in anderen Ländern meist eine wichtige Rolle.

## 2 Theoretische Grundlagen

*Big data*-Verfahren werden heute schon in ganz verschiedenen Politikfeldern genutzt, um zwischen regelkonformen Handlungen und Regelverstößen zu unterscheiden, um Werturteile zu fällen und um Weltbilder und Sinnzuschreibungen zu fixieren. Man kann also drei Dimensionen der Wirkung von *big data* unterscheiden: eine regulative, eine normative und eine kulturell-kognitive (Ulbricht et al. 2018). Wenn es um ihren Einfluss auf die Regelsetzung geht, ist zu beachten, welche Aspekte von *big data* Regulierung beeinflussen: Geht es eher um die *Art der Daten* oder um die Form der *Analyse der Daten*? Die Größe des Datensatzes ist dabei nicht unbedingt das ausschlaggebende Kriterium. Zu unterscheiden ist vielmehr, ob die Daten domainspezifisch sind, sie also (nur) in dem Bereich und für den Zweck, für den sie erhoben worden sind, genutzt werden, oder ob es sich um unspezifische bzw. domainübergreifende Daten handelt. Private Krankenkassen in den USA ziehen etwa zunehmend unspezifische Daten über ihre Versicherten heran, etwa Konsumdaten, um Tarife und Leistungen zu bestimmen; öffentliche Krankenkassen in den USA sowie alle Krankenkassen in Deutschland beschränken sich weitgehend noch auf gesundheitsspezifische Daten. Hinsichtlich der *Analysemethoden* geht es darum, zu unterscheiden, ob klassische statistische Verfahren und regelgebundene explorative Analysetechniken zur Anwendung kommen oder ob Verfahren künstlicher Intelligenz und maschinellen Lernens (etwa *deep learning* oder hochkomplexe *decision trees*) zum Einsatz kommen, bei denen die Entscheidungsregeln nicht mehr vollständig von außen vorgegeben sind.

Innerhalb der *big data*-basierten Regulierung muss man grundsätzlich unterscheiden, ob es um den Einfluss auf konkrete, einzelne Regeln geht oder um den Einfluss auf den Regelsetzungsprozess selbst. Es stellt sich also die Frage, ob *big data* neue oder veränderte Meta-Regeln hervorbringt. Auf dieser Meta-Ebene könnte die Nutzung solcher Verfahren dazu führen, dass Regeln so konstruiert werden, dass ihre Auslegung und Präzisierung in die Datenanalyse verlagert wird, dass es also zu formal weniger präzisen Regeln kommt, die erst in der Anwendung datengetrieben präzisiert werden. Gleichzeitig könnten Regelsetzungsverfahren auch stärker responsiv gestaltet werden und es könnte damit zu einem schnelleren Regelwandel kommen.

Hinsichtlich des Einflusses auf konkrete, einzelne Regeln ist zu unterscheiden, ob *big data* zu grundsätzlich andersartigen Regeln führt oder „nur“ zu einer veränderten Interpretation bzw. Auswirkung je nach gesellschaftlicher Subgruppe von im Grundsatz gleich bleibenden Regeln. Dem Versprechen nach soll *big data* dazu dienen, Regulierung mit feinerer Granularität auf kleinere gesellschaftliche Gruppen anzupassen (Morozov 2014). Regeln müssten dafür beispielsweise nicht die Bevölkerung als Ganzes, sondern nur noch einzelne Bevölkerungsgruppen betreffen. Eine veränderte Regelinterpretation hätte dagegen vor allem eine Verschiebung der Autorität zur Folge. Wenn *big data* im Sinne algorithmischer Regulierung dazu genutzt wird, Entscheidungen über Regelanwendungen zu treffen, verlagert sich die Regulierungskompetenz von den bisherigen Institutionen weg in die Regeln, die die Entscheidung der Maschine bestimmen. Das wäre eine Autoritätsverlagerung weg von



**Abb. 1** Der Einfluss von Big Data auf Regulierung. (Quelle: Eigene Darstellung)

Verwaltungsmitarbeiter\*innen hin zu Entwickler\*innen der *big data*-Verfahren oder – im Falle von *deep learning* – in die Maschine selbst. Abb. 1 fasst diese unterschiedlichen Aspekte schematisch zusammen.

Ein Wandel der Regelsetzung oder -interpretation kann unterschiedlich weit reichen: von der vollständigen Übertragung von Verantwortung auf die Maschine bis hin zu hybriden Formen geteilter Verantwortung zwischen Mensch und Maschine. Um zu ermessen, wie weitreichend der Einfluss von *big data* und Algorithmen auf Regulierung ist, kommt es daher darauf an, Automatisierung und Eingriffstiefe zu beurteilen: Am weitreichendsten sind Systeme, in denen Entscheidungen vollautomatisch, ohne menschliche Intervention getroffen werden. Weniger weitreichend ist der Einfluss bei Systemen, die zwar Vorschläge machen, die Entscheidung aber letztendlich bei der menschlichen Anwenderin des Systems belassen. Darüber hinaus geht es darum, ob *big data*-basierte Systeme nur einzelne, spezifische und abgegrenzte Lebensbereiche betreffen oder ob sich ihr Einfluss gleich auf mehrere Lebensbereiche erstreckt.

### 3 Praktische Anwendungsfelder

Am weitesten ist algorithmische Regulierung in Deutschland bislang in der Sicherheitspolitik verbreitet; andere Politikbereiche erwägen und erproben entsprechende Verfahren erst. Dabei spielen Erfahrungen aus anderen Ländern eine wichtige Rolle. Eine wichtige Funktion von *big data* ist, Bürger\*innen zu Regulierungszwecken zu klassifizieren. Bislang beruhten entsprechende staatliche Klassifizierungen meist auf relativ großen und fixierten Kategorien, wie etwa Geburtskohorten, Einkommensgruppen und Staatsangehörigkeit. Nunmehr erproben staatliche Akteure die Klassifizierung zunehmend feiner granulierter Gruppen, zum Teil in dynamischer Weise. In den USA, Großbritannien und Neuseeland werden *big data* und Algorithmen beispielsweise eingesetzt, um besser einschätzen zu können, wie groß das Risiko ist, dass ein Kind oder Jugendlicher in nächster Zeit Gewalt erfährt oder vernachlässigt wird. Ausgewertet werden Daten aus der Sozialverwaltung, gepaart mit Informationen über die Strafgeschichte von Familienangehörigen und zuweilen angereichert durch Befragungen von betroffenen Jugendlichen. Daten über Online-Verhalten und

aus sozialen Netzwerken werden bislang nicht verwendet. Je nach Anwendungskontext werden die Informationen mit einfachen statistischen Verfahren, aber auch unter Verwendung maschinellen Lernens ausgewertet. Am Ende steht meist ein Risikowert, der allerdings keine automatischen Folgen hat. Der Score ist vielmehr eine Information unter vielen, die Sozialarbeiter\*innen heranziehen, um zu entscheiden, welche der folgenden Maßnahmen sie treffen, wenn sie eine Eingabe bezüglich eines Kindes erhalten: keine Handlung, eine weitere Prüfung der Unterlagen, Entsendung einer Sozialarbeiterin vor Ort, erste Maßnahmen zur Entfernung eines Kindes aus seiner Familie etc. Es handelt sich also nicht um eine vollautomatisierte Umsetzung, sondern um ein sogenanntes *human in the loop*-Modell, bei dem ein Mensch die letzte Entscheidung trifft. Allerdings gibt es Hinweise darauf, dass Menschen nur selten von der maschinellen Empfehlungen abweichen, die sogenannte *over-reliance*. Das liegt zum Teil an dem Versprechen von Objektivität, das derartige Verfahren mit sich bringen, aber auch an der Verantwortungsstruktur: Bei Fehlern, wenn etwa Kinder trotz Meldungen ans Sozialamt zu Opfern werden, ist die Sozialverwaltung oder das zuständige Personal weniger unter Legitimierungsdruck, wenn es der maschinellen Empfehlung gefolgt ist, als wenn es von ihr abgewichen ist. Entsprechend monieren Kritiker des Einsatzes von *big data* und Algorithmen in der Kinder- und Jugendhilfe, dass die maschinelle Empfehlung eine zu große Bedeutung erhalte, die aufgrund der Intransparenz, ungewissen Wirksamkeit und möglichen unerwünschten Effekten problematisch sei (McKinlay 2017). Tatsächlich gibt es in den USA Staaten, die beschlossen haben, eine entsprechende Software wieder auszusetzen. Ähnliche algorithmische Verfahren werden in den USA auch zur Vorhersage der Rückfallwahrscheinlichkeit von Straftätern eingesetzt. Dazu zählt etwa der *COMPAS Score*, der zahlreiche spezifische sowie unspezifische Daten und ein Verfahren des maschinellen Lernens verwendet. Auch hier treffen Staatsanwält\*innen und Richter\*innen die letzte Entscheidung und der Risikoscore ist *de jure* nur eine Information von vielen, die die Entscheidung begründen sollen. Doch es gibt auch Kritik, dass der maschinell erzeugte Score im Entscheidungsprozess letztlich den Ausschlag geben könnte (Angwin et al. 2016).

Das bisher wohl weitreichendste Programm zum Einsatz von *big data* in staatlichen Verwaltungen ist der vom Staatsrat der Volksrepublik China 2014 veröffentlichte Plan für ein *social credit system* (State Council 2014). Darin werden Richtlinien für die Schaffung eines umfassenden *scoring*-Systems formuliert, mit dessen Hilfe bis zum Jahr 2020 die Kreditwürdigkeit von Organisationen und Personen in insgesamt 20 Bereichen, von Industrie und Handel, Steuern, Fertigungssicherheit über Umweltschutz, Lebensmittel, Medizin bis hin zu Sozialversicherung, Bildung und Forschung beurteilt werden soll. Kern des geplanten Systems ist die Erhebung von Daten in verschiedenen gesellschaftlichen Bereichen und Kontexten und die systematische Verknüpfung dieser Daten über Bereichsgrenzen hinweg. Ziel des Projekts ist die Schaffung von Vertrauen und einer „Aufrichtigkeitskultur“, es geht also über rein ökonomische Erwägungen hinaus. Bisher wird das System in China noch nicht flächendeckend umgesetzt, aber es existieren in einzelnen Großstädten und Regionen Pilotprojekte, von denen manche schon zwischen 2007 und 2011 begonnen haben (Creemers 2018). Diese Pilotprojekte gehen teilweise weit über den

im staatlichen Planungsdokument skizzierten Rahmen hinaus und erfassen auch alltägliche Verhaltensdaten der Bürger\*innen. Im Rahmen des „Massenkredits“ in Suining (Creemers 2018) sowie im *social credit system* Rongchengs (Mistreanu 2018) wurde jeweils allen Bürger\*innen im Einzugsbereich ein Startwert von 1000 zugewiesen, der dann durch regelkonformes und vorbildliches Verhalten erhöht werden konnte. Verspätete Kreditrückzahlungen, aber auch eher alltäglichen Regelverstöße wie Schwarzfahren oder bei Rot über die Ampel gehen führen dagegen zu Punktabzügen. Unterschreitet man einen bestimmten Wert, kommt man auf eine „schwarze Liste“ und wird damit von bestimmten Leistungen ausgeschlossen. Voraussetzung für diese weitreichenden Systeme sind ein eindeutiger Identifizierungscode für jede\*n Bürger\*in sowie der Ausbau biometrischer Datenbanken, mit deren Hilfe alltägliche Regelverstöße, die von Überwachungskameras und Sensoren aufgezeichnet werden, automatisch Individuen zugeordnet werden können. Allerdings stammen die Daten in den bisherigen Pilotprojekten zum allergrößten Teil nicht von Sensoren und Kameras, sondern werden ganz traditionell von Verwaltungsmitarbeiter\*innen eingegeben. In solchen Pilotprojekten entstehen Systeme, die sehr weitreichend sind und die individuelle Verhaltensdaten aus einer großen Zahl von Lebensbereichen miteinander verknüpfen. Mit diesem *social credit system* entwickelt sich in gewisser Weise ein „transparenter“ Überwachungsstaat, der das Verhalten seiner Bürger\*innen in (fast) allen Lebensbereichen zentralisiert und standardisiert erfasst und zugleich mit dem dadurch entstehenden Score auch umfassend Auskunft über das (aggregierte) Ergebnis der Überwachung erteilt. In Kombination mit *data mining*-Techniken und maschinellem Lernen, die in den bisher existierenden Systemen erst sehr begrenzt zum Einsatz kommen (Creemers 2018), könnte hier ein wahrhaft dystopisches *big data*-basiertes Kontrollinstrument entstehen, mit dem sich Muster normabweichenden Verhaltens zuverlässig identifizieren lassen – auch wenn noch offen ist, welche der in den Pilotprojekten eingesetzten Techniken und Datenquellen tatsächlich landesweit zum Einsatz kommen werden. In Deutschland und anderen Ländern Europas oder Nordamerikas gibt es keine vergleichbaren Projekte zu Erhebung und Speicherung von individuellen Daten. Allerdings haben die Enthüllungen von Geheimdienstpraktiken der US-amerikanischen NSA und des Britischen GCHQ durch Edward Snowden gezeigt, dass die staatlichen Fähigkeiten zur Sammlung und Verknüpfung persönlicher Daten aus den verschiedensten Lebensbereichen schon weit fortgeschritten sind, wenngleich auch bisher keine Programme existieren, diese Daten in ähnlicher Weise zur Kontrolle der eigenen Bevölkerung zu nutzen.

Am weitesten fortgeschritten ist der Einsatz von *big data* in Deutschland in der Sicherheitspolitik. Ein Großteil der Bevölkerung – alle, die mit dem Flugzeug reisen – wird mit Verfahren der Mustererkennung darauf untersucht, ob sie möglicherweise ein Risiko darstellen, an Terrorismus oder schwerer Kriminalität beteiligt zu sein. Zu diesem Zweck werten Sicherheitsbehörden die sogenannten „Fluggastdaten“ aus, die von Fluggesellschaften und Reiseveranstaltern erhoben werden müssen. Aktuell werden diese noch mit Datenbanken über verdächtige Personen abgeglichen; perspektivisch sollen aber Verfahren eingesetzt werden, die durch maschinelles Lernen Muster erkennen. Anders als sonst in der Ermittlungsarbeit üblich, werden bei

Fluggästen keine Daten zur strafrechtlichen Vorgeschichte erhoben, sondern eine lange Liste an Konsum-, Verhaltens- und Netzwerkdaten. Analog zur entsprechenden Praxis in den USA und anderen angelsächsischen Ländern sollen die durch *big data* ermittelten Muster dazu dienen, allen Fluggästen einen Risikowert zuzuschreiben. Auf dessen Grundlage werden sodann unterschiedliche Regeln angewendet: Manche Personen werden eingehender überwacht, ohne etwas davon zu bemerken, andere werden an Flughäfen peniblen Kontrollen ausgesetzt; wieder andere werden am Besteigen des Flugzeugs gehindert. Ein Teil der Flugreisenden, jene mit geringem Risikowert, können wiederum mit einer schnellen Abfertigung rechnen. Hier zeigt sich, wie anhand von *big data* eine Granularisierung von Regeln entsteht. Auch früher wurden Fluggäste an Flughäfen unterschiedlich behandelt. Neu ist, dass große Bevölkerungsgruppen geprüft werden und dass der Risikowert einer Person aus Datenspuren entsteht, die diese in ganz anderen Kontexten hinterlassen hat.

Mit Blick auf Meta-Regeln, also parlamentarische Gesetzgebungsverfahren, Entscheidungsverfahren innerhalb von Verwaltungseinheiten, politischen Parteien oder Interessengruppen, spielt *big data* bislang noch eine untergeordnete Rolle. Unter dem Titel *legal technology* kommt zwar zunehmend Software zum Einsatz, die Jurist\*innen beim Verfassen und Prüfen von rechtlichen Normen helfen soll. Dabei geht es aber (noch) nicht um die algorithmisch gesteuerte Definition der Inhalte als vielmehr um die interne und externe Kohärenz rechtlicher Normen, etwa um Verweise auf andere Regeltexte. Allerdings zeigt sich der Markt dynamisch und es werden Ideen und Technologien entwickelt, in denen Mustererkennung und maschinelles Lernen Normentwicklung und -interpretation unterstützen oder gar übernehmen sollen, die *legal technologies 3.0* (Goodenough 2015).

Während die formalen Verfahren der Regelsetzung durch *big data* noch nicht beeinflusst werden, gibt es Hinweise, dass dies bei informalen Verfahren bereits anders aussieht. Bei der inhaltlichen Vorbereitung von politischen Entscheidungen bedienen sich staatliche Behörden, Parteien sowie Interessengruppen zunehmend Analyseverfahren, die auf *big data* beruhen (Kreiss 2016; Karpf 2016). Ziel der Analysen ist es, Probleme zu identifizieren, politische Präferenzen zu erfassen, die Auswirkungen politischer Interventionen zu messen etc. Diese Verfahren der *people analytics*, des *micro-targeting* und der *sentiment analysis* ersetzen andere Verfahren der Bevölkerungs- und Problemanalyse nicht, treten jedoch hinzu und nehmen so Einfluss auf Regelsetzungsverfahren. Auch in Deutschland gehören sie ins Repertoire politischer Akteure (Kruschinski und Haller 2017).

---

## 4 Perspektiven für Staat und Verwaltung

Bisher sind es vor allem privatwirtschaftliche Akteure, die versuchen mit Hilfe von *big data* das Verhalten ihrer Kund\*innen zu verstehen und zu beeinflussen. Politik und Verwaltungen demokratischer Staaten greifen bisher noch recht zurückhaltend auf große und diverse Datensätze und die mit *big data* assoziierten Analysemethoden (Verfahren des maschinellen Lernens) zurück. Parteien nutzen insbesondere in den USA schon extensiv *big data* zur Identifizierung und Beeinflussung wechsel-

bereiter Wähler\*innen. Einzelne autoritäre Regime bauen aktuell weitreichende Programme zur Nutzung großer und vielfältiger Datenmengen zur umfassenden Kontrolle der eigenen Bevölkerung auf. Grundsätzlich ist der staatliche Einsatz von *big data* im Bereich der inneren und äußeren Sicherheitspolitik am weitesten fortgeschritten. Der Grund dafür ist zum einen die lange Tradition des Einsatzes mustererkennender Verfahren wie beispielsweise der Rasterfahndung und zum anderen die in diesen Bereichen leichter aufrechtzuerhaltende Fiktion, die umfassende Auswertung personenbezogener Daten würde nur einen kleinen, devianten Teil der Bevölkerung betreffen. In Deutschland ist die Sicherheitspolitik das einzige Politikfeld, in dem *big data-basierte* Analysen bisher regelmäßig angewandt werden. Der gemeinsame Nenner algorithmischer Regulierung im staatlichen Bereich ist es, Regeln stärker zu differenzieren: nach geografischen Gebieten oder nach Subpopulationen. Die entsprechende Praxis von Überwachung, Disziplinierung und *social sorting* wird bereits kritisch durch sozialwissenschaftliche Forschung begleitet.

Die Erwartung, dass *big data* im staatlichen Bereich zu einer Renaissance kybernetischer Steuerung führen würde (Mayer-Schönberger und Cukier 2013), hat sich indes als überzogen erwiesen. Beispiele für vollautomatisierte algorithmische Regulierung gibt es bislang nicht, stets gibt es einen „menschlichen Filter“ (*human in the loop*). Es gibt freilich Kontexte, in denen die Anreize so gesetzt sind, dass die menschlichen Entscheider\*innen sich *de facto* kaum über die maschinelle Empfehlung hinwegsetzen können.

Mit Blick auf die Rolle von *big data* für Meta-Regeln zeigt sich deutlich, dass *big data*-basierte Verfahren andere Verfahren der Evidenzproduktion bislang nicht verdrängen, sondern nur hinzutreten. Somit ist ihr Einfluss begrenzt und es entsteht Raum dafür, ihre Vor- und Nachteile zu erproben. Unterschiedliche Strukturen der (Sozial-)Staatlichkeit fördern oder hemmen den Einsatz von *big data*. In Deutschland wirkt beispielsweise der umfassend ausgebauten Wohlfahrtsstaat einer Ausbreitung privatwirtschaftlicher *scoring*-Verfahren entgegen (Fourcade und Healy 2017). Zudem setzen strenge Datenschutzregeln der Verknüpfung und Zweckentfremdung von Daten in Deutschland enge Grenzen für die Verwendung von *big data* durch staatliche Akteure. Jenseits der Sicherheitspolitik erproben deutschsprachige Länder algorithmische Regulierung in Form prädiktiver Scores im öffentlichen Sektor, etwa zur Prävention von Langzeitarbeitslosigkeit (Österreich), häuslicher Gewalt (Schweiz) und Einbruchdiebstahl (Deutschland, Österreich, Schweiz). Unspezifische Daten kommen jedoch bisher nicht zum Einsatz. Da mit der weiteren Ausbreitung vernetzter Sensoren (*Internet of Things*) die Verfügbarkeit personenbezogener, nutzergenerierter und domainunspezifischer Daten noch deutlich zunehmen wird, hängt die weitere Entwicklung des Einsatzes von *big data* in Staat und Verwaltung wesentlich davon ab, ob gleichzeitig auch Schranken der Verwendung dieser Daten etabliert und implementiert werden, wie sie beispielsweise in der europäischen Datenschutzgrundverordnung enthalten sind.

## Literatur

- Angwin, Julia, Jeff Larson, Surya Mattu, und Lauren Kirchner. 2016. Machine Bias. *ProPublica*. [www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing](http://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing). Zugegriffen am 09.01.2019.
- Boyd, danah, und Kate Crawford. 2012. Critical questions for big data. Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society* 15(5): 662–679.
- Creemers, Rogier. 2018. *China's social credit system. An evolving practice of control*. <https://ssrn.com/abstract=3175792>. Zugegriffen am 17.05.2018.
- Fourcade, Marion, und Kieran Healy. 2017. Categories all the way down. *Historical Social Research* 42(1): 286–296.
- Goodenough, Oliver R. 2015. Legal technology 3.0. *Huffington Post*, 04.02.2015. [www.huffingtonpost.com/oliver-r-goodenough/legal-technology-30\\_b\\_6603658.html](http://www.huffingtonpost.com/oliver-r-goodenough/legal-technology-30_b_6603658.html). Zugegriffen am 17.01.2019.
- Karpf, David. 2016. *Analytic activism. Digital listening and the new political strategy*. New York: Oxford University Press.
- Kreiss, Daniel. 2016. *Prototype politics. Technology-intensive campaigning and the data of democracy*. New York: Oxford University Press.
- Kruschinski, Simon, und André Haller. 2017. Restrictions on data-driven political micro-targeting in Germany. *Internet Policy Review* 6(4). <https://doi.org/10.14763/2017.4.780>.
- Mayer-Schönberger, Viktor, und Kenneth Cukier. 2013. *Big data. A revolution that will transform how we live, work and think*. London: John Murray.
- Mckinlay, Steve T. 2017. Evidence, explanation and predictive data modelling. *Philosophy & Technology* 30(4): 461–473.
- Mistreanu, Simina. 2018. Life inside china's social credit laboratory. *Foreign Policy*. <https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/>. Zugegriffen am 15.05.2018.
- Morozov, Evgeny. 2014. The rise of data and the death of politics. *The Observer*, 19. Juli 2014. <https://www.theguardian.com/technology/2014/jul/20/rise-of-data-death-of-politics-evgeny-morozov-algorithmic-regulation>. Zugegriffen am 09.01.2019.
- State Council. 2014. *Planning outline for the construction of a social credit system (2014–2020)*, GF No. (2014)21, Beijing: State Council of the People's Republic of China. China Copyright and Media. <https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/>. Zugegriffen am 15.05.2018.
- Ulbricht, Lena, Sebastian Haunss, Jeanette Hofmann, Ulrike Klinger, Jan-Hendrik Passoth, Christian Pentzold, Ingrid Schneider, Holger Straßheim, und Jan-Peter Voß. 2018. Dimensionen von Big Data. Eine politikwissenschaftliche Systematisierung. In *Big Data und Gesellschaft. Eine multidisziplinäre Annäherung*, Hrsg. Barbara Kolany-Raiser, Reinhard Heil, Carsten Orwat und Thomas Hoeren, 151–231. Wiesbaden: Springer VS.
- Yeung, Karen. 2017. „Hypernudge“. Big data as a mode of regulation by design. *Information, Communication & Society* 20(1): 118–136.



---

# Künstliche Intelligenz

Christian Djeffal

## Inhalt

1	Begriff .....	52
2	Konzeptionelle Grundlagen .....	53
3	Nutzung von KI in Staat und Verwaltung .....	56
4	Rechtliche Aspekte .....	58
5	Perspektiven für Staat und Verwaltung .....	59
	Literatur .....	61

---

## Zusammenfassung

Künstliche Intelligenz steht für eine Forschungsfrage, die auf die selbstständige Lösung von Problemen durch technische Systeme abzielt. Ein Forschungszweig der Informatik setzt sich schwerpunktmäßig mit dieser Frage auseinander und hat im Laufe der Zeit verschiedene Lösungsansätze erarbeitet. In der öffentlichen Verwaltung im deutschsprachigen Raum werden bereits einige KI-Anwendungen eingesetzt. Schon heute zeichnet sich ein großes Potenzial für staatliches Handeln und für die Modernisierung der Verwaltung durch diese Technologien ab. Wie eine KI-gestützte Verwaltung aussieht, wird jedoch nicht durch die Technologie determiniert, sondern hängt von ihrer Gestaltung in den kommenden Jahren ab.

---

## Schlüsselwörter

Maschinelles Lernen · Automation · Künstliche Neuronale Netze ·  
Augmentation · Algorithmen

---

C. Djeffal (✉)

Munich Center for Technology in Society, Technische Universität München, München, Deutschland  
E-Mail: [christian.djeffal@tum.de](mailto:christian.djeffal@tum.de)

## 1 Begriff

Der Begriff der künstlichen Intelligenz (*Artificial Intelligence*) ist seit seiner Prägung umstritten und prägt trotzdem die aktuelle Diskussion. Am 4. Dezember 2018 veröffentlichte die Bundesregierung ihre „Strategie Künstliche Intelligenz“, in der sie die öffentliche Verwaltung als eines von zwölf Handlungsfeldern identifizierte (Bundesregierung 2018, S. 1, 31). Nach der Arbeitsdefinition von Klaus Mainzer geht es bei künstlicher Intelligenz um Systeme, die „selbstständig effizient Probleme lösen“ können (Mainzer 2016, S. 3). Künstliche Intelligenz steht insofern für eine Forschungsfrage. Diese hat mittlerweile eine solche Bedeutung erlangt, dass sich eine Subdisziplin der Informatik mit ihr beschäftigt, welche im Laufe der Jahre verschiedene Technologien, Architekturen und Systeme hervorgebracht hat. Diese rückten zeitweise in den Vordergrund und wurden als Essenz oder eigentlicher Inhalt der KI-Forschung angesehen. Früher traf das auf Entscheidungsbäume und Expertensysteme zu, während heute insbesondere das maschinelle Lernen und künstliche neuronale Netze Konjunktur haben. Als künstliche neuronale Netze bezeichnet man ein mathematisches Modell, das sich durch Eingaben selbst verbessern kann. Alle diese Technologien, Systeme und Architekturen können als Antworten auf die Forschungsfrage verstanden werden. Ein System, das alle denkbaren Probleme allumfassend lösen kann, ist bisher nicht entwickelt worden. Deshalb ist die Forschungsfrage weiterhin relevant. Geprägt wurde der Begriff 1955 von vier Wissenschaftlern in einem Antrag an die Rockefeller Stiftung, dessen zentrale Passage auch heute noch bezeichnend ist:

„Die Studie soll auf der Grundlage der Vermutung durchgeführt werden, dass jeder Aspekt des Lernens oder jedes anderen Merkmal der Intelligenz prinzipiell so genau beschrieben werden kann, dass eine Maschine zur Simulation hergestellt werden kann. Es wird versucht herauszufinden, wie man Maschinen dazu bringen kann, Sprache zu benutzen, Abstraktionen und Konzepte zu bilden, Arten von Problemen zu lösen, die heute dem Menschen vorbehalten sind, und sich selbst zu verbessern“ (McCarthy et al. 1955).

Es geht also um das selbstständige technische Lösen von Problemen. Das Besondere dieser Definition liegt in ihrer Offenheit. Tatsächlich handelt es sich bei KI um *Querschnittstechnologien*. Sie haben keinen bestimmten Zweck, sondern können mit vielen anderen technischen Einrichtungen und ferner in ganz verschiedenen Kontexten eingesetzt werden. Zum einen bedient sich die Informatik einer Reihe von Technologien zum Lösen von komplexen Problemen. Zum anderen sind auch die Einsatzmöglichkeiten in der soziotechnischen Wirklichkeit vielfältig. Künstliche Intelligenz wurde vom Ergebnis und nicht von der Technik her definiert. Welche Probleme das sind und auf welche Weise sie gelöst werden, ist grundsätzlich offen. Dieser essentielle und oft vernachlässigte Aspekt kann anhand des Datenschutzes illustriert werden: Auf der technischen Ebene kann es vorkommen, dass künstliche neuronale Netze anhand von personenbezogenen Daten trainiert werden. Im Gegensatz dazu kommen andere Technologien wie etwa *Generative Adversarial Networks* auch ohne das Training durch personenbezogene Daten aus. KI-Anwendungen können ebenfalls zu Gefahren für den Datenschutz führen. So können etwa intelli-

gente *Scraper* Daten aus öffentlich zugänglichen Quellen extrahieren und selbstständig Profile bilden. Umgekehrt werden gerade KI-Anwendungen entwickelt, die die Datenschutzpräferenzen von Individuen abfragen und automatisiert in sozialen Netzwerken durchsetzen können.

Die unterschiedlichen Zwecksetzungen von künstlicher Intelligenz sind in der Informatik kontrovers diskutiert worden. Ein Teil des Diskurses stellte darauf ab, dass der Zweck von KI-Anwendungen *Automation* sei, also selbstständige Handlungen von Maschinen. Demgegenüber definierten andere *Augmentation* als Ziel von KI, also die Erweiterung menschlicher Fähigkeiten durch die Maschine.

---

## 2 Konzeptionelle Grundlagen

Ausgehend von der Frage nach der selbstständigen Problemlösung haben sich verschiedene Ansichten in der Informatik entwickelt. Die „starke KI-These“ versucht bis heute erfolglos, alle Aspekte des menschlichen Denkens durch KI nachzubilden und eine sogenannte „generelle künstliche Intelligenz“ zu formen. Demgegenüber fokussieren sich die Anhänger der „schwachen KI-These“ auf bestimmte Problemstellungen. Demnach soll künstliche Intelligenz immer nur bestimmte Probleme rational lösen. Technologien künstlicher Intelligenz spielen für viele Mode- und Trendbegriffe und andere Konzepte eine wichtige Rolle, ohne dass diese deckungsgleich sind. So bezeichnet der Begriff *Big Data* im Wesentlichen große Datenmengen. Große Datenmengen können für KI auf unterschiedlichen Ebenen eine Rolle spielen. Sie können zum Training von künstlichen neuronalen Netzen (KNN) verwendet werden. So werden KNN zum Beispiel trainiert, bestimmte Tiere auf Bildern zu erkennen, indem riesige Datensätze mit Tierbildern und Beschreibungen in das System eingespeist werden. Umgekehrt können KI-Anwendungen auch große Datenmengen produzieren, etwa wenn Bilder oder Texte erkannt werden. Komplexere Auswertungen großer Datenmengen werden ebenfalls durch KI-Anwendungen vorgenommen. Dabei kann KI insbesondere bestimmte Muster erkennen. Betont werden muss aber, dass KI keineswegs mit *Big Data* gleichzusetzen ist. Weder müssen Anwendungen notwendigerweise mit großen Datenmengen trainiert werden, noch muss sich KI auf die Auswertung großer Datenmengen beziehen. Ähnliches gilt für das sogenannte Internet der Dinge. Damit wird eine Technikvision von ubiquitär vernetzten Gegenständen bezeichnet. Diese können auch KI-Anwendungen enthalten, das ist aber keinesfalls notwendig. KI-Verfahren werden oft als *Algorithmen* bezeichnet. Unter diesem Begriff versteht man eigentlich feste Verfahren zur Lösung eines Problems. Als Heuristiken werden richtigerweise Verfahren bezeichnet, die auf der Grundlage von Unsicherheiten und Wahrscheinlichkeiten Entscheidungen fällen.

Um KI-Systeme zu verstehen, werden sie oft nach dem Agenten-Modell dargestellt. Der Agent nimmt seine Umwelt über Sensoren wahr, verarbeitet diese Informationen und wirkt dann durch Aktorik auf seine Umwelt ein. Einen graphischen

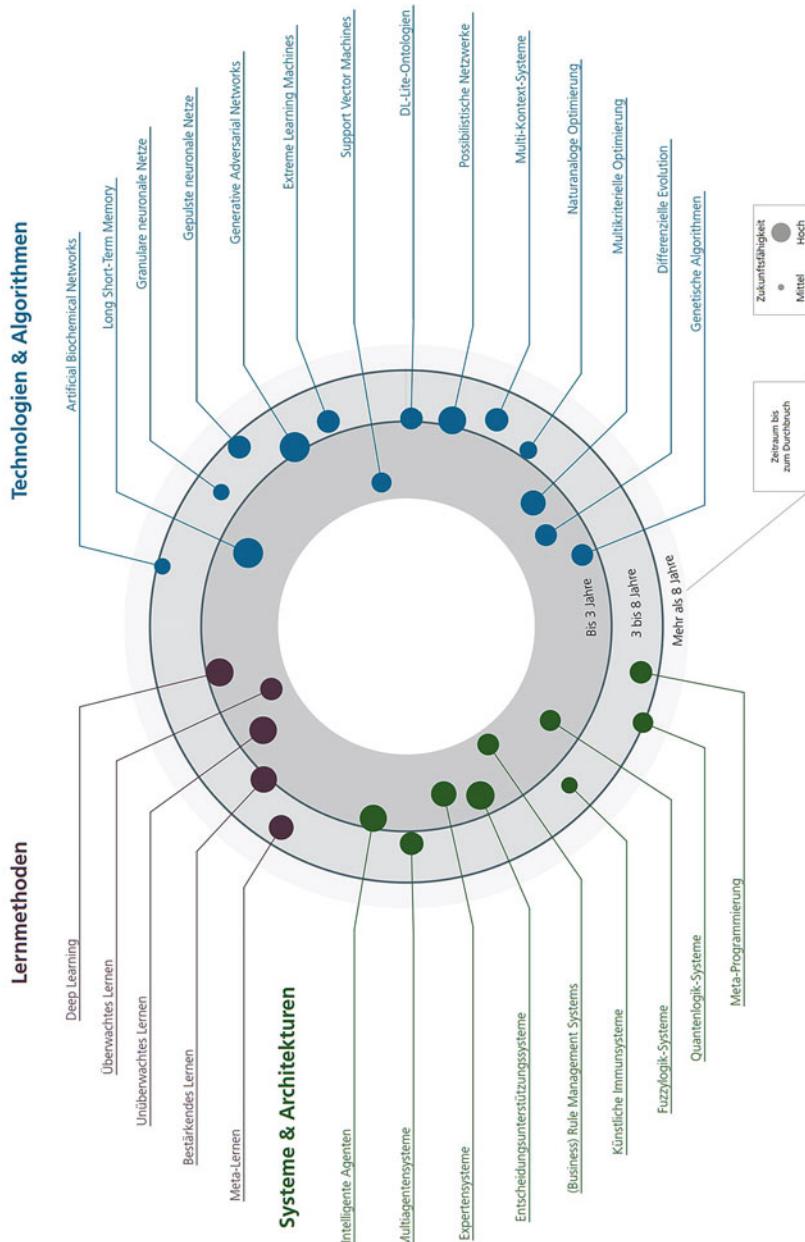
Überblick über Methoden, Technologien und Architekturen gibt das OEFIT-Trendsonar (Welzel und Grosch 2018) (Abb. 1):

Besonders das maschinelle Lernen sorgt nach wissenschaftlichen Durchbrüchen seit 2011 für eine zunehmende Verbesserung und Erweiterung der jeweiligen Systeme. Während wir uns in manchen Bereichen bereits daran gewöhnt haben, dass Maschinen den Menschen ersetzen und sogar übertreffen können, wurden in den letzten Jahren neue Bereiche für künstliche Intelligenz erschlossen: Auf Feldern wie der Umsetzung von Sprache in Text oder der Übersetzung oder der Bilderkennung haben KI-Anwendungen in den vergangenen Jahren große Fortschritte gemacht. Das macht sich auch im Bereich der Verwaltung bemerkbar. Zwar wird bereits seit den 1950er-Jahren über die Automatisierung der Verwaltung diskutiert, doch wie die untenstehenden Beispiele zeigen, kam es insbesondere in den letzten Jahren zu einer qualitativen und quantitativen Steigerung des Einsatzes von KI-Anwendungen.

In der jüngeren Vergangenheit widmete sich eine Vielzahl von Berichten und Strategien den Chancen und Risiken künstlicher Intelligenz. Chancen und Risiken von KI kann man allerdings nur richtig einordnen, wenn man den oben erwähnten Charakter von KI als Querschnittstechnologie ernst nimmt. Denn sowohl auf der Ebene der Entwicklung als auch auf der Ebene der soziotechnischen Einbettung bestehen so viele technische und soziale Optionen und Gestaltungsmöglichkeiten, dass es in vielen Fällen weniger um Chancen und Risiken von KI als solcher geht. Denn diese sind kontingent und hängen von ihrer Entwicklung, Verwendung und Einbettung ab. Elektrizität kann als Technologie diesen Querschnittscharakter veranschaulichen. Braunkohlekraftwerke oder Wasserkraftwerke haben bei der Produktion von Elektrizität ganz unterschiedliche Auswirkungen auf die Umwelt. Strom kann in Braunkohlekraftwerken oder Solaranlagen auf Dächern gewonnen werden. Elektrizität kann zum Betreiben medizinischer Geräte oder elektrischer Stühle verwandt werden. Genauso kann künstliche Intelligenz die Grundlage für Exoskelette für Schwerbehinderte oder für tödliche Waffensysteme sein. Es gibt zahlreiche Handlungs- und Gestaltungsmöglichkeiten von künstlicher Intelligenz in der öffentlichen Verwaltung. Nach tatsächlichen Entscheidungen richten sich auch Chancen und Risiken.

Natürlich hat die technische Entwicklung bestimmte Pfade eingeschlagen, die heute gewisse Chancen und Risiken als typisch erscheinen lassen (Mittelstadt et al. 2016). Diese weisen jeweils auch die in der Verwaltung eingesetzten Systeme auf. Mit dem Einsatz von KI wird eine steigende Effizienz von Prozessen und mithin eine Kostenersparnis assoziiert, ferner eine steigende Effektivität, also eine Optimierung des Verhältnisses von eingesetzten Ressourcen und Ergebnissen. Entlastet werden sollen Menschen besonders von repetitiven „mechanischen“ Aufgaben, die unter dem Stichwort Massenverwaltung diskutiert werden. KI-Anwendungen werden im Vergleich zur menschlichen Erledigung eine hohe Zuverlässigkeit, Geschwindigkeit und eine permanente Verfügbarkeit zu Gute gehalten.

Was die Nachteile angeht, wird oft die mangelnde Transparenz der Systeme und die Nachvollziehbarkeit ihrer Entscheidungen moniert. Insbesondere künstliche neuronale Netze werden trainiert und entwickeln eigene Entscheidungsmodelle,



**Abb. 1** OEFIT-Trendsonar. (Quelle: Welzel und Grosch 2018, S. 6 f.)

die nicht ohne Weiteres eingesehen und verstanden werden können. Besonders bei Systemen, die Entscheidungen treffen oder empfehlen, kann dies Ungleichbehandlungen und Diskriminierungen zur Folge haben. Grund dafür kann zum Beispiel sein, dass die Daten, die zum Trainieren lernender Systeme benutzt werden, nicht repräsentativ sind. KI-Anwendungen kann auch die Sensitivität für bestimmte Kontexte fehlen, insbesondere wenn es zu unvorhergesehenen Fällen kommt, auf die die Anwendungen nicht trainiert wurden. Dies kann auch Anlass zu Lücken der IT-Sicherheit geben. Das autonome Erkennen von Straßenverkehrsschildern konnte etwa schon durch kleine Aufkleber auf diesen Schildern getäuscht werden. Ein weiterer Nachteil ist die Kehrseite der Effizienz- und Effektivitätssteigerung. Künstliche Intelligenz könnte dazu führen, dass wesentlich weniger Möglichkeiten für Erwerbstätige bestehen. Voraussagen gehen davon aus, dass verschiedene Berufe größtenteils durch KI-Anwendungen ersetzt werden können. Das würde auch auf bestimmte Aufgaben der Verwaltung zutreffen, die heute noch von Sachbearbeiter\*innen erledigt werden.

---

### **3 Nutzung von KI in Staat und Verwaltung**

Die Frage nach der Nutzung von künstlicher Intelligenz in Staat und Verwaltung lässt sich normativ und tatsächlich beantworten. Die normative Frage, ob und unter welchen Voraussetzungen KI eingesetzt werden soll, muss die rasante Technologieentwicklung und die vielen Alternativen ihrer soziotechnischen Einbettung beachten. Der Maßstab des gelungenen Einsatzes von künstlicher Intelligenz hängt also von einem soziotechnischen Vergleich ab. Dieser zielt darauf ab, den Zustand vor und nach der Digitalisierung unter einer umfassenden Berücksichtigung aller Vor- und Nachteile für Rechte und Interessen zu bewerten. Ein solcher soziotechnischer Vergleich wird oft nur auf der Basis von Experimenten und Studien möglich sein. Aus dieser Perspektive ist es etwa müßig, darüber zu streiten, ob Maschinen Entscheidungen über Menschen fällen können. Vielmehr ist zu fragen, an welcher Stelle in einem konkreten Prozess KI-Anwendungen eingesetzt werden können und welche Ressourcen zur Verfügung stehen, um die Entscheidungen zu prüfen und zu korrigieren. Gestaltungsmöglichkeiten bei Verfahren und Organisation sowie bei der Qualifikation der Mitarbeiter sind dabei ebenso wichtig wie die Technikgestaltung.

Schon in der heutigen Verwaltungspraxis im deutschsprachigen Raum werden zahlreiche Anwendungen von künstlicher Intelligenz eingesetzt, die komplexe Aufgaben übernehmen können. Dabei werden KI-Anwendungen zu ganz verschiedenen Zwecken genutzt. Dazu gehört etwa die Vorhersage von Risiken und Gefahren, die Überwachung des öffentlichen Raums und die Simulation zukünftigen Verhaltens.

Die Vorhersage von Gefahren und Risiken spielt seit jeher im Sicherheitsrecht eine große Rolle. Unter dem Stichwort „*predictive policing*“ werden KI-Anwendungen zusammengefasst, die der Erkennung von polizeilichen Risiken und Gefahren dienen (Rademacher 2017). So können etwa ortsbegogene Risiken für Einbruchdiebstähle bestimmt werden. Hier werden beispielsweise in Deutschland die Systeme Precobs oder SKALA eingesetzt. Diese Systeme zeigen Risikostufen

für verschiedene Bereiche an und übertragen sie auf *Heatmaps*. Bei der Planung von Streifenfahrten können Polizeibeamte besonders gefährdete Orte einbeziehen. Der österreichische Zoll konnte mit ähnlichen Analysen die Effektivität seiner Kontrollen steigern. In der Schweiz werden Anwendungen zur Vorhersage des Verhaltens bestimmter Personen genutzt. Systeme wie DyRiAS oder Octagon weisen Gewalttätern einen personenbezogenen Risiko-Score zu, der Grundlage für die Entscheidung über etwaige Gefährderansprachen ist. Im Steuerverfahren in Deutschland ist die Risikoerkennung durch KI bereits Teil des normalen Verwaltungsverfahrens geworden, insbesondere bei dem Risikomanagementsystem „Veranlagung 2.0“, das entscheidet, wer seine Belege zur Steuerprüfung einreichen muss.

Künstliche Intelligenz kann mittels Videotechnik auch zur Identifikation und Authentifizierung von Personen verwendet werden. Bereits im Einsatz ist das sog. Easypass-System, eine automatisierte Grenzkontrolle, die Reisepässe scannt und sie mit dem Gesicht des Reisenden abgleicht. So ist eine schnelle Authentifizierung möglich. Nach einem automatischen Datenbankenabgleich kann die Einreise gestattet werden. Getestet wird am Berliner Bahnhof Südkreuz die Möglichkeit, Videoüberwachung mit einer Gesichtserkennung auszustatten, sodass gesuchte Personen automatisiert identifiziert werden können. In jüngerer Zeit haben sich KI-Anwendungen auch beim Erkennen von sozialen Situationen ausgezeichnet. So können beispielsweise Verkehrsunfälle auf vielbefahrenen Straßen automatisch erfasst und an die betreffende Leitstelle gemeldet werden. Intelligente Videotechnik kann mittlerweile auch Handlungen von Menschen erkennen. Dies wird in Mannheim getestet. Mit dem Projekt „Mannheimer Weg 2.0“ sollen automatisch bestimmte Bewegungsmuster wie etwa Schlagen oder Fallen registriert und einem Mitarbeiter gemeldet werden, um die Innenstadt sicherer zu machen.

Im Rahmen von Videoüberwachung wird künstliche Intelligenz zur Anonymisierung eingesetzt. So können etwa Kamerasysteme, die freien Parkraum überwachen sollen, datenschutzfreundlich ausgestaltet werden. Denn der Personenbezug von Daten kann ausgeschlossen werden, wenn Nummernschilder oder Gesichter von Fahrern unkenntlich gemacht werden.

KI-Anwendungen werden zudem in der Verkehrslenkung eingesetzt. Insbesondere intelligente Verkehrsbeeinflussungsanlagen auf Fernstraßen nehmen über Sensoren verschiedene Daten wahr und regeln auf dieser Basis den Verkehr, etwa indem sie Überholverbote oder Geschwindigkeitsbegrenzungen anzeigen. Hier werden heute schon automatisiert *Verwaltungsakte* (Allgemeinverfügungen) erlassen. Wie die Verwaltungspraxis unten zeigt, wird sowohl für interne als auch für externe Angelegenheiten zunehmend auf automatische Entscheidungsfindung zurückgegriffen. Automatisiert werden hierbei insbesondere strukturierte Entscheidungen der Massenverwaltung, die ohnehin stark vorgeprägt sind, etwa durch Verwaltungsvorschriften. Dies schlägt sich im Moment insbesondere in der Sozial- und der Steuerverwaltung nieder, wo verschiedene Entscheidungen automatisiert werden.

KI-Anwendungen zur Simulation zukünftigen Verhaltens verschiedener Akteure finden z. B. in den Bereichen Verkehrssteuerung, Bevölkerungsschutz und Katastrophenvorsorge Anwendung. Durch KI lässt sich beispielsweise simulieren, wie sich

Straßenbaumaßnahmen auf den Verkehr auswirken. Ebenso kann die Auswirkung von Naturkatastrophen simuliert werden.

Auch verwaltungsintern gibt es bereits zahlreiche Anwendungsfelder von künstlicher Intelligenz. Ein Bereich, in welchem dies sehr ausgeprägt ist, ist die IT- und Cybersicherheit. Komplexe Angriffe werden in der Regel durch Systeme aufgedeckt, die Anomalien erkennen können. Das *Bundesamt für die Sicherheit in der Informationstechnik* (BSI) hat 2018 ein eigenes Referat für künstliche Intelligenz eingerichtet. In den Behörden können auch die meisten KI-Anwendungen verwendet werden, die für das Büroumfeld von Organisationen in Wirtschaft oder Wissenschaft entwickelt wurden: von der Spracherkennung für Diktiersysteme bis zur Nutzung von *Suchmaschinen*. Die Aufgaben, die verwaltungsintern Suchmaschinen zukommen, werden im Außenverhältnis als *e-Discovery* bezeichnet: KI-Technologien ermöglichen das rasche Durchsuchen von großen Datenbeständen. Dies spielt insbesondere dort eine Rolle, wo die Verwaltung die Befugnis zur Durchsuchung von Datenbeständen besitzt, wie etwa in der Strafverfolgung oder in kartellrechtlichen Verfahren.

Auch in der Kommunikation der Verwaltung mit dem Bürger kommen KI-Anwendungen zum Einsatz. Für Anfragen von Bürger\*innen werden Chatbots als weitere Alternative zur Verfügung gestellt, die bestimmte Fragen im Rahmen von Konversationen beantworten können. Die Systeme stehen rund um die Uhr zur Verfügung und haben Schnittstellen zu *Messenger*-Diensten. Solche *Chatbots* werden zum Beispiel vom Land Berlin eingesetzt. Auch in anderen Kommunen werden Systeme getestet wie etwa der *Chatbot „Botty Bonn“*, der „*WienBot*“ oder der „*Kumpel Krefeld*“. Im Bürgerbüro Ludwigsburg und der Stadtbibliothek Köln werden Serviceroboter getestet, die Bürger\*innen je nach ihrem Anliegen den Weg weisen oder sie sogar zum richtigen Ort begleiten.

---

## 4 Rechtliche Aspekte

Die Rolle des Rechts bei KI-gestützten Verwaltungsreformen darf nicht auf seine begrenzende Funktion reduziert werden. Grundsätzlich kann das Verhältnis der Funktion des Rechts zur Technik mit den Schlagworten „Grund, Grenze und Gestaltung“ umschrieben werden (Djeffal 2017, S. 811). Als Grund fungiert das Recht immer dann, wenn es zur Anwendung der Technologie motiviert oder sogar verpflichtet. Im menschenrechtlichen Bereich zeichnen sich bereits einige Pflichten ab, die einen Einsatz von KI-Anwendungen in der öffentlichen Verwaltung motivieren oder sogar verpflichtend vorschreiben können. Art. 4 Absätze g und h der UN-Behindertenrechtskonvention enthält eine Technologieklausel, in der sich die Unterzeichnerstaaten u. a. verpflichten, inklusive Informations- und Kommunikationstechnologien zu fördern und zur Verfügung zu stellen. So können Systeme mit Bilderkennung und Sprachausgabe Blinden schon heute situativ helfen, indem bestimmte Bildausschnitte etwa einer Handykamera beschrieben werden. Die Charta der Grundrechte und Grundfreiheiten der Europäischen Union postuliert in Art. 41 ein *Recht auf eine gute Verwaltung*. Dies umfasst laut Abs. 1, dass „Angelegenheiten

... der Union unparteiisch, gerecht und innerhalb einer angemessenen Frist behandelt werden“. Es ist sehr gut denkbar, dass dies auch die Einbindung von KI-Anwendungen umfasst, wenn diese entsprechende Vorteile bieten.

Die begrenzende Funktion des Rechts gegenüber der Technologie ist die gebräuchigste Funktion. Was automatisierte Entscheidungen angeht, findet diese begrenzende Funktion allgemeinen Ausdruck in § 54 des Bundesdatenschutzgesetzes (BDSG), in Art. 22 der Datenschutzgrundverordnung (DSGVO) und in § 35a des Verwaltungsverfahrensgesetzes des Bundes (VwVfG). Den weitesten Anwendungsbereich hat dabei § 35a VwVfG, der sich auf den Erlass von Verwaltungsakten bezieht. Demgegenüber regeln Art. 22 DSGVO und § 54 BDSG nur nachteilige Entscheidungen, diese Vorschriften sind ferner nur bei der Verarbeitung personenbezogener Daten anwendbar. Allen Vorschriften gemein ist, dass es eine rechtliche Grundlage bzw. einen Erlaubnistratbestand für den betreffenden Fall geben muss. Die Grenzen müssen damit unter Wahrung der Rechte und Interessen der Einzelnen für bestimmte Anwendungen oder Arten von Anwendungen ausgelotet werden.

Dies wird es notwendig machen, dass diese Rechte und Interessen der Adressaten von Entscheidungen bereits bei der Entwicklung der Technologie berücksichtigt werden. Hier kann das Recht eine weitere Funktion entfalten, wenn es zur Technikgestaltung fruchtbar gemacht wird. Während im Datenschutzrecht und im IT-Sicherheitsrecht bereits entsprechende Pflichten bestehen, lässt sich dies gedanklich auf weitere Bereiche ausweiten. In ihrer Strategie zur künstlichen Intelligenz fordert die Europäische Kommission auch zentrale Elemente wie Rechtsstaatlichkeit, Demokratie und *Grund- und Menschenrechte* bei der Gestaltung von KI-Systemen zu berücksichtigen. Diese Strategie erfordert ebenfalls eine umfassende Folgenabschätzung (Nemitz 2018, S. 18–19).

---

## 5 Perspektiven für Staat und Verwaltung

Schon auf dem heutigen Stand der technischen Möglichkeiten zeigt sich das Potenzial von KI-Technologien, die triadierte Verwaltung grundlegend zu verändern. Diese neue Verwaltung, an der künstliche Intelligenz einen großen Anteil hat, wird als „Smart Government“ bezeichnet (Lucke 2016). Basierend auf *Querschnittstechnologien* geben KI-Anwendungen aber nicht per se Zwecke oder Richtungen vor (Djeffal 2018, S. 9, 14). Daraus erwachsen große Chancen, die Entwicklung von KI-Technologien und die Bedingungen ihrer Anwendungen in Staat und Verwaltung zu beeinflussen. Diese Gestaltungschancen der Verwaltung bestehen auf verschiedenen Ebenen.

Auf der technischen Ebene kann die Verwaltung im Rahmen einer sog. Metagovernance Maßstäbe setzen, die sich auch auf andere Akteure auswirken. Eine solche Vorbildwirkung könnte die Verwaltung z. B. im Bereich der IT-Sicherheit erzielen. Aber auch indirekt können öffentliche Verwaltungen einen großen Einfluss ausüben, insbesondere über die Vergabe von Aufträgen. Über die Definition von Anforderungen und Vergabekriterien kann die Verwaltung faktische Standards setzen. Besonders in Ländern, die ihre Vergaben im Bereich der IT bündeln oder sich intensiv über Vergabekriterien austauschen, konnte die Durchsetzung höherer Standards erreicht werden.

Bei den tatsächlichen Anwendungen von künstlicher Intelligenz in der öffentlichen Verwaltung geht es um die soziotechnische Einbettung der Systeme. Die Technik muss bewusst gestaltet und in das individuelle und gesellschaftliche Leben eingefügt werden. Ein wichtiges Thema ist dabei, wie Bürger in diese Prozesse eingebunden werden. Schon heute gibt es in unterschiedlichen Verwaltungszweigen verschiedene Möglichkeiten der Information, Partizipation, Mitbestimmung und Mitgestaltung. Gelungene Entwicklungen setzen in jedem Fall Räume für Experimente und Erprobung der Technik voraus. In dieser Hinsicht könnten sich der föderale Staatsaufbau und die kommunale Selbstverwaltung als Vorteil herausstellen.

Im unternehmerischen Umfeld wird die Beteiligung von Nutzer\*innengruppen besonders als Anregung zu kreativen Lösungen und zur Förderung der Akzeptanz eingesetzt. Denn insbesondere die Akzeptanz hängt nicht nur mit der Funktionsfähigkeit der jeweiligen Anwendungen zusammen, auch das Vertrauen der handelnden Personen und der Bevölkerung hat einen großen Einfluss. In manchen Verwaltungszweigen ist der Einsatz von automatischen Einrichtungen nur stückweise durch die Medien öffentlich geworden. Hier wurde besonders deutlich, dass ein transparenter Umgang Akzeptanz und Vertrauen schaffen kann. Dies ist auch deshalb notwendig, weil der Verwaltung durch künstliche Intelligenz mehr Handlungsmöglichkeiten und auch mehr Handlungsmacht zukommt. KI-Systeme können permanent, ubiquitär und automatisch eingesetzt werden. Sie können Menschen nicht nur bei der Erfüllung von Aufgaben ersetzen, sondern in manchen Bereichen „übermenschliche“ Fähigkeiten entwickeln. Vor diesem Hintergrund sind Transparenz, Offenheit und Möglichkeiten zur Mitbestimmung oder Beteiligung auch aus demokratischen Gründen geboten.

Schon heute wird die Debatte um die Chancen und Risiken von KI wesentlich von der öffentlichen Verwaltung geprägt. Das „Social Credit Score“-System Chinas ist ein Beispiel. US-amerikanische Systeme zur Unterstützung von Straflichtern, bei denen KI-Anwendungen Rückfallwahrscheinlichkeiten berechnen, werden für Entscheidungen zu Bewährung und Haftverleichterung herangezogen. Dem System konnten eine limitierte Funktionsfähigkeit und eine diskriminierende Wirkung gegenüber ethnischen Minderheiten nachgewiesen werden. Während bisher eher negative Auswirkungen der Verwaltungspraxis öffentlich diskutiert wurden, werden eine Reihe von positiven Beispielen in der jüngeren Debatte unter dem Schlagwort „AI for good“ zusammengefasst. Dabei geht es um KI-Anwendungen, die gezielt dazu eingesetzt werden, besondere Missstände und Probleme anzugehen. Im Lichte dieser internationalen „Großwetterlage“ wird die öffentliche Bewertung von KI-Anwendungen in der Verwaltung auch davon abhängen, ob hier ein eigener – vielleicht europäischer Ansatz – gefunden werden kann, der den KI-gestützten Reformvorhaben Profil und Leitbild gibt.

Wie bei der Verwaltungsdigitalisierung allgemein, werden auch beim zunehmenden Einsatz von KI-Anwendungen die positiven Effekte dort am größten sein, wo man bestehende Prozesse nicht einfach abbildet, sondern vor dem Hintergrund technischer Möglichkeiten neu erprobt und neu denkt. Dies erfordert an vielen Stellen, dass man sowohl Verwaltungsverfahren als auch Verwaltungsorganisation

entsprechend gestaltet. Wenn etwa Art. 22 DSGVO ein Recht zur Überprüfung automatisierter Entscheidungen verleiht, muss im Verwaltungsverfahren darauf geachtet werden, wie dieses Recht verfahrensmäßig effektiv umgesetzt werden kann. Ein wichtiger Teil dieser Umsetzung hängt auch von den organisatorischen Voraussetzungen ab. Denn eine sinnvolle menschliche Prüfung erfordert eine entsprechende Befähigung der Behörden, Entscheidungen automatischer Einrichtungen verstehen, kritisieren und prüfen zu können. Von der Schulung der Mitarbeiter\*innen bis hin zur organisatorischen Einbettung in speziellen Einheiten oder sogar Behörden gibt es viele Handlungsmöglichkeiten und auch -notwendigkeiten. Wichtig ist es insbesondere, den entsprechenden Sachverstand in den jeweiligen Behörden zu verankern.

Wie sich KI-Anwendungen in Staat und Verwaltung niederschlagen, hängt deshalb auch nicht zuletzt von den Zwecken ab, die mit künstlicher Intelligenz verfolgt werden. Im internationalen Vergleich zeigt sich, dass kosten- und effizienzgetriebene Automatisierungsprozesse fehlschlügen und am Ende sogar zu Kostensteigerungen führten, wie etwa beim australischen „Centrelink-Skandal“. Hier wurden in Australien automatisiert Bescheide zur Rückzahlung von Sozialhilfeleistungen an Bürger\*innen versandt, wenn sich ein Widerspruch zwischen verschiedenen Datenbanken ergab. Das System war allerdings sehr fehleranfällig und es waren nicht genug Prüfungen vorgesehen, die Fehler verhinderten. Über 20.000 Bescheide mussten in kurzer Zeit aufgehoben werden, es bestand auch eine hohe Dunkelziffer an Menschen, die sich nicht effektiv wehren konnten. Als Querschnittstechnologie gibt KI der Verwaltungsreform allerdings gerade keine Zwecke vor, sondern schafft neue Möglichkeiten. Bei der Realisierung dieser Möglichkeiten sind Grundsätze der *Grund- und Menschenrechte*, der *Rechtsstaatlichkeit* und der *Demokratie* nicht darauf beschränkt, den äußeren Rahmen der Verwaltungsreform durch KI zu bilden. Sie können vielmehr zum Movens und zu zentralen Zwecken selbst erhoben werden. Die Offenheit von KI-Technologien und die vielfältigen Möglichkeiten, die sie bieten, können Regierung und Verwaltung genauso zur Treiberin wie zur Getriebenen im Reformprozess machen.

---

## Literatur

- Bull, Hans-Peter. 1964. *Verwaltung durch Maschinen. Rechtsprobleme der Technisierung der Verwaltung*. Köln: Grote.
- Bundesregierung. 2018. Strategie Künstliche Intelligenz der Bundesregierung. <https://www.ki-strategie-deutschland.de/home.html>. Zugegriffen am 10.10.2019.
- Djeffal, Christian. 2017. Das Internet der Dinge und die öffentliche Verwaltung. Auf dem Weg zum automatisierten Smart Government? *Deutsches Verwaltungsblatt* 132(13): 808–816.
- Djeffal, Christian. 2018. *Künstliche Intelligenz in der öffentlichen Verwaltung*. Berichte des NEGZ Nr. 3. Berlin: NEGZ.
- Hill, Hermann. 2015. Scientific Regulation – Automatische Verhaltenssteuerung durch Daten und Algorithmen. In *Verwaltungsressourcen und Verwaltungsstrukturen. Auf dem Weg zum Digitalen Staat – auch ein besserer Staat?*, Hrsg. Hermann Hill, 267–287. Baden-Baden: Nomos.
- Hoffmann-Riem, Wolfgang. 2017. Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht. *Archiv des Öffentlichen Rechts* 142(1): 1–42.

- Lucke, Jörn von, Hrsg. 2016. *Smart Government*. Berlin: epubli.
- Mainzer, Klaus. 2016. *Künstliche Intelligenz – wann übernehmen die Maschinen?* Wien: Springer.
- Martini, Mario. 2017. Algorithmen als Herausforderung für die Rechtsordnung. *Juristenzeitung* 72(21): 1017–1025.
- McCarthy, John, Marvin L. Minsky, Nathaniel Rochester, und Claude L. Shannon. 1955. *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*. <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>. Zugegriffen am 10.10.2019.
- Mittelstadt, Brent D., Patrick Allo, Mariarosaria Taddeo, Sandra Wachter, und Luciano Floridi. 2016. The ethics of algorithms. Mapping the Debate. *Big Data & Society* 3(2): 1–21.
- Mohabbat Kar, Resa, Basanta Thapa, und Peter Parycek, Hrsg. 2018. *(Un)Berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft*. Berlin: Kompetenzzentrum Öffentliche IT.
- Nemitz, Paul. 2018. *Constitutional Democracy and Technology in the Age of Artificial Intelligence*. Royal Society Philosophical Transactions.
- Rademacher, Timo. 2017. Predictive Policing im deutschen Polizeirecht. *Archiv des öffentlichen Rechts* 142:179–190.
- Welzel, Christian, und Dorian Grosch. 2018. *Das ÖFIT-Trendsonar künstliche Intelligenz*. Berlin: Kompetenzzentrum Öffentliche IT/Fraunhofer FOKUS. <https://www.oeffentliche-it.de/documents/10181/14412/Das+%C3%96FIT-Trendsonar+K%C3%BCnstliche+Intelligenz>. Zugegriffen am 10.10.2019.
- Wischmeyer, Thomas. 2018. Regulierung intelligenter Systeme. *Archiv des Öffentlichen Rechts* 143(1): 1–66.



---

# Blockchain in der öffentlichen Verwaltung

Dieter Rehfeld

## Inhalt

1 Klärung des Begriffs .....	64
2 Konzeptionelle Grundlagen .....	65
3 Praktische Anwendungsfelder .....	67
4 Umsetzungsstand und Auswirkungen .....	69
5 Perspektiven für Staat und Verwaltung .....	71
Literatur .....	72

---

## Zusammenfassung

Die Blockchain ist eine neuartige Kombination altbewährter Technologien, die spezifische konzeptionelle und technische Merkmale aufweist. Sie besteht aus einer sicheren Datenstruktur, den Blöcken, die in einer kontinuierlichen Liste gespeichert und in einem dezentralen Netz von Knoten verarbeitet werden. Eine digitale Zeichenfolge bildet eindeutige Eigentumsrechte ab. Diese Rechte werden digital übertragen und einem neuen Besitzer zugeordnet. Eine gleichzeitige Übertragung an einen zweiten Empfänger ist ausgeschlossen (*Double-Spending-Problem*). Auch die öffentliche Verwaltung gewährt, verändert, dokumentiert und überträgt Rechte. Diese werden in Registern verwaltet und sind ebenso eindeutig zugeordnet. Bescheinigungen, Nachweise und Beglaubigungen werden im Geschäftsbetrieb benötigt und verursachen Transaktionskosten. Diese können durch eine Nutzung der Blockchain reduziert werden.

---

D. Rehfeld (✉)

regio iT gesellschaft für informationstechnologie mbh, Aachen, Deutschland  
E-Mail: [Dieter.Rehfeld@regioit.de](mailto:Dieter.Rehfeld@regioit.de)

**Schlüsselwörter**

Transaktionskosten · Kryptografie · Genossenschaft · Eigentumsrechte · Hackathons

---

## 1 Klärung des Begriffs

Unter dem Pseudonym Satoshi Nakamoto hat ein bis heute unbekannter Verfasser 2008 in einem Aufsatz: „Bitcoin: A Peer to Peer Electronic Cash System“ gezeigt, wie Geld im Internet auf digitalem Wege sicher den Besitzer wechseln kann – ganz ohne Banken. Eine neutrale Instanz, ein Intermediär, ist nicht mehr erforderlich. Das Konzept von Nakamoto stellt sicher, dass es immer nur ein Eigentumsrecht an einer Geldeinheit gibt. Eine *Bitcoin*-Einheit kann nicht gleichzeitig an zwei Besitzer übertragen werden: Das „Double-Spending-Problem“ ist gelöst (Nakamoto 2008). Auch wenn das Konzept von Nakamoto inhaltlich auf die digitale Übertragung von Geldeinheiten zielt, lässt es sich allgemein auf das Handeln mit und Übertragen von Eigentumsrechten im weitesten Sinne adaptieren. Oder noch genereller: Eine digitale Zeichenfolge (*Bits*) kann eindeutig gehandelt, übertragen und einem Besitzer zugeordnet werden.

Die *Software*, die die technische Basis für das Nakamoto-Konzept bildet, wird mit „Blockchain“ bezeichnet. Sie besteht aus einer Datenstruktur, die ihre Datensätze, die Blöcke, in einer kontinuierlichen Liste speichert. Die Blöcke in dieser Liste sind über eine besondere Funktion, den sogenannten *Hashwerten*, fälschungs-sicher miteinander verknüpft. Die Blockchain-Datenbanken werden nicht zentral, sondern verteilt und dezentral gespeichert. Es wird mithin nicht zentral administriert und gespeichert, sondern durch ein besonderes Protokoll ein *Peer-to-Peer*-Netzwerk (P2P) betrieben. Die Datenbanken sind auf viele Rechner, sogenannte *Nodes*, verteilt. Um Transaktionen auf der Blockchain digital durchzuführen, benötigt jeder Nutzer eine Adresse. Bei dieser Adresse handelt es sich um den öffentlichen Schlüssel (*Public Key*) als Teil der asymmetrischen Kryptografie. Die öffentlich bekannten Kontonummern im allgemeinen *Banking* sind in der Blockchain die öffentlichen kryptografischen Schlüssel. Aber nur die Person, die den zugehörigen privaten Schlüssel besitzt, kann auf das mit dem Konto verknüpfte Eigentumsrecht zugreifen. Jede Transaktion, zum Beispiel ein Eigentumsrecht an digitalem Geld an eine andere Person zu übertragen, kann nur dann erfolgen, wenn mit dem zugehörigen privaten Schlüssel eine digitale Signatur erzeugt wurde. Mit Hilfe dieser digitalen Signatur wird das Recht am Eigentum an einer Geldeinheit von einem Konto auf ein anderes übertragen. Der *Private Key* ist das Sicherheitsmerkmal, mit dem sich der rechtmäßige Eigentümer zur Autorisierung ausweisen kann. So kann der Empfänger des Eigentumsrechts sicher sein, dass die Transaktion mit einem legitimierten Partner abgeschlossen wurde. Er kann aber noch nicht feststellen, ob sich das transferierte Eigentumsrecht tatsächlich im Besitz des Partners befunden hat oder ob es nicht beispielsweise schon ein anderes Mal vergeben wurde. Gelöst wird dieses Transaktionsproblem dadurch, dass nicht jede einzelne Transaktion durch eine Bank oder

eine Clearingstelle festgehalten, überprüft und genehmigt wird, sondern sämtliche Transaktionsdaten aufbewahrt werden. Die Rechte am Eigentum werden über die gesamte Historie der Transaktionsdaten in der Speicherlogik geführt. In diesem Fall besteht das verteilte Kontenbuch aus einer Kette von chronologisch gereihten Blöcken, die miteinander durch digitale Fingerabdrücke (*Hashwerte*) verbunden sind. Jeder neue Datenblock enthält den *Hashwert* des vorangegangenen Datenblocks. Dadurch entsteht eine Kettenstruktur, über die zum einen die Transaktionen eindeutig zurückverfolgt werden können. Zum anderen garantiert diese Verkettung, dass es nahezu unmöglich ist, einen Wert in einem Block zu ändern. Dies wäre nur möglich, wenn mit hoher Rechnerkapazität alle Blöcke neu gerechnet würden und darüber in dem verteilten Netzwerk auch noch Konsens hergestellt würde. Dabei kontrollieren sich alle Teilnehmer gegenseitig durch einen Abstimmungs- und Validierungsprozess, der in der Realität unter den Teilnehmern vollautomatisch digital erfolgt. Hier kommen sogenannte Konsensmechanismen zum Einsatz. Bekannte Konsensmechanismen sind „Proof of Work“ und „Proof of Stake“. Diese führen dazu, dass die dezentral und verteilt gespeicherten Daten extrem sicher und vertrauenswürdig sind. Eine nachträgliche Änderung ist nach dem heutigen Stand der Technik unmöglich. Diese extrem sichere Verkettung von Daten-Blöcken wird als Blockchain bezeichnet (Swan 2015; Drescher 2017).

Die Blockchain-Technologie ist eine Kombination altbewährter, wohlbekannter Technologien (Schoder et al. 2002; Wattenhofer 2016). Diese Technologie-Kombination wird nicht nur bei *Bitcoin* genutzt, mittlerweile gibt es eine Vielzahl von Abwandlungen und Weiterentwicklungen. Allgemein werden diese Lösungen unter der Bezeichnung „Distributed Ledger Technology“ zusammengefasst. Die in dieser Technologie verteilten Datenbanksysteme nutzen zur Kommunikation untereinander bekannte *Peer-to-Peer*-Technologien, setzen zur Identifizierung und Authentifizierung auf kryptographische Verfahren, sichern Daten gegen Verfälschung durch *Hashwert*-Konzepte und nutzen Zeitstempel (*Timestamp*), um die Reihenfolgen von Transaktionen zu organisieren. Die mathematische und technische Basis der *Distributed Ledger Technology* ist sehr gut dokumentiert (Wattenhofer 2016).

---

## 2 Konzeptionelle Grundlagen

Eine wesentliche Aufgabe der öffentlichen Verwaltung ist es, Rechte – im weitesten Sinne Eigentumsrechte – zu gewähren, zu verändern, zu dokumentieren und zu übertragen. So wird registriert, wer Besitzer eines Kraftfahrzeuges ist, wem ein Grundstück gehört, wer mit wem verheiratet ist, wer einen Kindergartenplatz erhalten hat, wer einen Führerschein besitzt oder wer eine Werbeanlage im Straßenraum aufstellen darf. Diese Rechte werden in Registern nachvollziehbar dokumentiert. In den meisten Fällen ist es nur die öffentliche Verwaltung, die solche Rechte gewährt und dokumentiert. Neben dieser Rechtegewährung und -übertragung ist eine wesentliche öffentliche Funktion die Dokumentation, wie sich diese Rechte im Zeitverlauf verändern: Das Grundstück wird verkauft, das Fahrzeug wechselt den Besitzer, die

Ehe wird geschieden oder die Zeit zur Aufstellung der Werbeanlage ist abgelaufen. Das Konzept, Rechte zu besitzen und diese Rechte zu garantieren und durchzusetzen, repräsentiert ein Kernelement in jeder menschlichen Gesellschaft (Rehfeld 2016).

Im gesellschaftlichen und wirtschaftlichen Zusammenleben ist oft ein Nachweis erforderlich, dass jemand über bestimmte Rechte tatsächlich verfügt. Der Besitz von Rechten ist im Geschäftsleben vielfach die Voraussetzung, um neue Verträge einzugehen. So muss der Fahrer nachweisen, dass er im Besitz einer Fahrerlaubnis ist; der Anspruch auf ein Wegerecht ist notwendig, um die Ver- und Entsorgung eines Grundstücks zu sichern. Kindergeld wird länger gewährt, wenn nachgewiesen wird, dass der Sohn oder die Tochter noch studiert, und Grundbesitz ist oft die Voraussetzung für eine Kreditgewährung. In vielen Fällen geht es darum, diese Rechtenachweise als Bürger\*innen oder als Unternehmen zu erbringen. Sie sind Bestandteil von Verträgen und Geschäftsprozessen. Von Verwaltungsstellen Dokumente zu erhalten, bereitet Aufwand. Oft müssen Bescheinigungen beglaubigt werden, in manchen Fällen ist die Mitwirkung eines Notars zwingend erforderlich. Bescheinigungen und Beglaubigungen aus Registern verursachen mithin erhebliche Transaktionskosten. Dies sind nicht allein die Gebühren oder die direkten monetären Kosten, sondern auch die Zeit, die dafür aufgewendet werden muss.

Das Recht an einem Zahlungsmittel hat als Eigentumsrecht im Prinzip die gleiche Struktur wie die Rechte, die sich im Kontakt mit der öffentlichen Verwaltung ergeben. Das durch den Staat verbriegte Recht eines Bürgers oder eines Unternehmens muss auch eindeutig zuzuordnen sein. Wenn es sich verändert oder übertragen wird, muss dies ebenso transparent nachvollziehbar sein. Wenn das Konzept von Nakamoto auf öffentliche Dienstleistungen übertragen werden könnte, so würde das die Transaktionskosten deutlich verringern.

Der allgemeine Fall in der Blockchain ist das Verwalten und Klären von Rechten, ohne an ein bestimmtes Gut gebunden zu sein. Die Blockchain ermöglicht das Speichern und Verbreiten beliebiger digitaler Informationen über Eigentumsrechte. Dies ist der Anknüpfungspunkt für Lösungen in der öffentlichen Verwaltung. Eine besondere Rolle kommt hier den *Nodes* (Knoten) zu. Das sind Rechner, die sämtliche Transaktionen, die innerhalb des *Peer-to-Peer*-Netzwerks getätigten wurden, herunterladen und dann alle weiteren Transaktionen aufzeichnen. Sie überprüfen auch neue Transaktionen und stellen sicher, dass die Regeln des Netzwerks eingehalten werden.

Das *Peer-to-Peer*-Netzwerk der beteiligten Rechner kann offen (*public*) oder geschlossen (*private*) gestaltet werden. Im ersten Fall wäre das Netzwerk unter gewissen technischen Voraussetzungen für jedermann zugänglich, im zweiten Fall hätten nur bestimmte Institutionen oder Personen Zugriffsrechte auf die Daten. So könnte zum Beispiel die Aufgabe der *Nodes* auf öffentliche Rechenzentren beschränkt werden. Oder nur der Verwaltung das Recht eingeräumt werden, in die Blockchain zu schreiben. Auch sind Kombinationen denkbar. So können autorisierte und zugelassene Institutionen im Netzwerk über Schreib- und Leserechte verfügen, während andere Nutzer nur einen lesenden Zugang erhalten.

### 3 Praktische Anwendungsfelder

In der Literatur rund um die Blockchain im öffentlichen Sektor wird oft empfohlen, die Blockchain so einzusetzen, dass Grundbucheinträge, Personalausweise, Waffen- oder Kfz-Register, Patientenakten oder Geburtsurkunden gespeichert werden. Die Autoren, die dies empfehlen, sehen den Einsatz der Blockchain-Technologie im öffentlichen Sektor dort, wo derzeit zentrale staatliche oder öffentliche Institutionen die Umsetzung von Regeln sicherstellen. Es werden Anwendungsszenarien zu Eigentumsverhältnissen, Herkunfts nachweisen, digitaler Identität sowie Transparenz und Offenheit von Wahlen als Beispiele genannt. Oder es wird empfohlen, mit Hilfe der Blockchain zu prüfen, ob Zahlungen zur staatlichen Unterstützung berechtigt sind. Oder mittels der Blockchain sollen öffentliche Finanzhilfen besser nachvollziehbar verfolgt werden können. Allerdings muss festgehalten werden, dass es diese Art von Blockchain-Anwendungen in Deutschland bisher nicht gibt.

Kritisch sind die Vorschläge zu betrachten, die die Blockchain quasi als Registerersatz verstehen. Dies verstellt den Blick auf das eigentliche Potenzial der Technologie für die öffentliche Verwaltung: Dieses liegt vielmehr in der Anwendung als digitales Bescheinigungs- und Nachweiswesen von Rechten (Validierung von Rechten) in Verbindung mit den staatlichen und kommunalen Registern, denn in der Abschaffung von Registern. Das Gesetz zur Förderung der elektronischen Verwaltung, das E-Government-Gesetz, zielt in § 5 darauf, die Verwaltung effizienter zu gestalten. Nachweise können elektronisch vorgelegt und zwischen Behörden digital ausgetauscht werden.

Die grundsätzliche konzeptionelle Überlegung für eine praktische Nutzung der Blockchain im Nachweis- und Bescheinigungswesen besteht nun darin, dass Nutzer mit Hilfe einer „smarten Blockchain-App (*Govchain-App*)“ die für sie und für ihren Geschäftsvorfall beteiligten Register digital ansprechen und es unter ihrer Datensouveränität den Registern erlauben, die für den Geschäftsvorfall notwendigen Daten – und nur diese – auszutauschen. Um die *Govchain-App* zu nutzen, muss der Nutzerin einen Authentifizierungs- und Zulassungsprozess durchlaufen. Hier kann das nationale Bürgerkonto nach dem Onlinezugangsgesetz eine wichtige Rolle übernehmen. So könnte ein gewinnbringender Service der Bürger- und Servicekonten die „Freischaltung“ der *Govchain-App* sein. Die Blockchain-Technologie wird so genutzt, um zwischen Registern einen Nachweis zu organisieren. Diese Nachweis- und Bescheinigungsfunktion kann zwischen *Public-Public*-Registern erfolgen. Sie kann aber ebenso für einen *Public-Private*-Austauschprozess von Daten geöffnet werden. In diesem Ansatz ist wesentlich, dass die vorhandenen Register bestehen bleiben.

Im kommunalen Sektor in Deutschland finden sich schon heute einige praktische Beispiele zur Nutzung der Blockchain-Technologie. Diese wurden im Blockchain-Labor der kommunalen Rechenzentren entwickelt und praktisch getestet. Der Bundesverband VITAKO der kommunalen Rechenzentren hat dieses *Government Blockchain Lab* eingerichtet, um Zug um Zug konkrete Anwendungen zu entwickeln und zu testen. Ziel ist es, praktische Erfahrungen mit der Technologie zu sammeln und verschiedene Lösungen zu entwickeln, wie die Blockchain sinnvoll eingesetzt werden kann und wo sie Nutzen stiftet. Für die Kernverwaltung gibt es vielversprechende erste Anwendungen.

So wurde auf Basis der Blockchain-Technologie eine Lösung entwickelt, um Zeugnisse auf ihre Echtheit hin zu überprüfen. Immer häufiger werden digitale Unterlagen bei Bewerbungen eingereicht. Eine Echtheitsbestätigung ist oft nur aufwändig durchzuführen. Zukünftig kann unter Nutzung der *Public- und Private Key-Infrastruktur* ein Zeugnis von der ausstellenden Institution, also zum Beispiel einer Universität oder einer Schule, signiert werden. Das Zeugnis erhält bei der Ausstellung eine individuelle Transaktions-Identifikationsnummer (Transaktions-ID) und zum Beispiel im PDF-Format einen *Hashwert*. Dieser wird gemeinsam mit der Transaktions-ID, die nur der Besitzer erhält, in der Blockchain gespeichert. Nun kann der Besitzer des Zeugnisses dieses einem Dritten, zum Beispiel einem Arbeitgeber, zur Überprüfung weiterreichen.

Ein ähnliches Konzept wurde im Rahmen des Mobilitätsmanagements für Kommunen genutzt, um digitale intermodale Mobilität zu organisieren. Heute gehört es zum Standard bei Autovermietern, ein Mietfahrzeug digital bestellen zu können. Viele Schritte des Geschäftsvorfalls von der Buchung bis zur Bezahlung können online und digital durchgeführt werden. Selbst der Autoschlüssel kann über eine App digital übersandt werden. Allerdings ist es nach wie vor in der Regel notwendig, als Fahrer bei der Übernahme des Fahrzeuges an einem Schalter den Führerschein vorzuzeigen. Eine digitale Lösung der Führerscheinüberprüfung wäre auch für viele Unternehmen interessant. Die jährliche Überprüfung der Arbeitnehmer\*innen, ob die Fahrerlaubnis vorliegt, könnte vereinfacht werden.

Diese Beispiele zeigen, dass es möglich ist, eine Validierungsinfrastruktur aufzubauen, um Dokumente öffentlicher Institutionen (wie Zeugnisse) oder kommunale Nachweise (wie Führerscheine) via Blockchain zu validieren. Diese Vorgänge der Validierung weisen in der Regel immer die gleichen Anforderungen auf: Es sind Dokumente auf ihre Echtheit hin zu überprüfen oder Registereinträge aus staatlichen oder öffentlichen Registern nachzuweisen.

Auch kommunale Unternehmen entdecken aktiv die Blockchain-Technologie. So gibt es in der Elektromobilität Lösungen für das digitale Bezahlen von Ladesäulen und zur Abrechnung von Stromerzeugung sowie für die Lieferung von Nachbarschaftsstrom auf Basis der Blockchain-Technologie. Im Konzept der *Smart Cities* und des Internet der Dinge (*Internet of Things*) wird die Bedeutung von Daten aus der Kommune immer wichtiger. Es gibt den Bedarf, die Echtheit von Daten, ihre Quelle und ihr Erzeugungsdatum zu überprüfen. Hier gibt es im *Government Blockchain Labor* eine kommunale Lösung auf Basis der Blockchain-Technologie, die diese Daten wie ein Datennotar digital mit einem Qualitätssiegel versieht. Damit werden diese Daten auch für Datenmarktplätze handelbar.

Die Blockchain-Technologie kann besonders dann ihre Wirkung entfalten, wenn zahlreiche Stellen, wie beispielsweise alle Hochschulen, berechtigt sind, in die Blockchain zu schreiben und gleichzeitig für eine große Zahl von Nutzer\*innen, wie Bewerber\*innen und Arbeitgeber\*innen, ein Mehrwert generiert werden kann. Dafür ist es selbstverständlich notwendig, dass sich die Stellen und Nutzer, die den Service nutzen wollen, registrieren lassen und autorisiert werden. Dies gilt vor allem für die schreibenden Stellen. Die Organisation der Zulassung im Sinne eines „*Know your Customer (KYC)*“ muss erst noch aufgebaut werden. Hier könnte das geplante

Bürgerkonto nach dem Online-Zugangsgesetz ein sehr guter Einstieg für die Nutzung einer Validierungsinfrastruktur auf Basis der Blockchain sein. Dies gilt auch für die Freigabe der jeweiligen Register und für die Bereitstellung der Information für Validierung öffentlicher Dokumente. Mithin zeigt sich für die Nutzung der Blockchain-Technologie im öffentlichen Sektor, dass hier nicht die „reine Lehre“ der Blockchain zur Anwendung kommt. Es sind geschlossene *Communities*, die Daten zur Verfügung stellen.

---

## 4 Umsetzungsstand und Auswirkungen

Bei der Nutzung der Blockchain für ihre Aufgaben befindet sich die öffentliche Verwaltung in Deutschland erst am Anfang. Die Blockchain-Technologie fasziniert aber immer mehr IT-Spezialisten und Führungskräfte. Das zeigen zahlreiche Veranstaltungen und Foren zum Thema „Blockchain und öffentliche Verwaltung“. Die Technologie-Diskussion rund um die Blockchain hat mittlerweile auch die Politik erreicht. So findet sich im Koalitionsvertrag der christlich-sozialdemokratischen Bundesregierung vom März 2018 an sechs verschiedenen Stellen der Verweis auf die Blockchain. So heißt es zum Beispiel für die geplante *E-Government-Agentur*: „In der Bundesregierung werden wir innovative Technologien wie Distributed Ledger (Blockchain) erproben, so dass basierend auf diesen Erfahrungen ein Rechtsrahmen geschaffen werden kann.“ (Bundesregierung 2018, S. 45). Auch für die CDU/FDP-geführte Landesregierung in Nordrhein-Westfalen wird im Koalitionsvertrag (CDU NRW 2017, S. 33) festgehalten, dass Nordrhein-Westfalen vor allem Anwendungen in der öffentlichen Verwaltung durch Blockchain-Technologien sicherer machen möchte. Es besteht also auch auf den Ebenen Bund und Länder die Bereitschaft, sich aktiv mit der neuen Technologie auseinanderzusetzen. So hat zum Beispiel das Bundesamt für Migration und Flüchtlinge auf Basis von Blockchain in einem *Proof of Concept (POC)* gezeigt, dass im behördenübergreifenden Asylverfahren bei der Prozessverkettung durch den Einsatz der Blockchain-Technologie eine deutliche Verbesserung der Transparenz und der Datensicherheit erzielt werden konnte (BAMF 2018). Auch findet sich in den Ausschreibungen zu den Technologie-Förderprogrammen von Bund und Ländern immer häufiger explizit der Hinweis auf die Förderung der Blockchain-Technologie. Immer mehr *Hackathons* mit Startups und jungen Software-Entwicklern zu Blockchain nehmen Bezug zum öffentlichen Sektor. Der Prozess, Blockchain für die öffentliche Verwaltung zu nutzen, geht weiter. Flächendeckende Lösungen sind in absehbarer Zeit zu erwarten. Es werden aber ebenso auch kritische Aspekte diskutiert.

Es gibt aber auch eine Debatte darüber, ob die öffentliche Verwaltung durch die Blockchain in ihrer Kernaufgabe gefährdet wird. Manche Autoren sehen durchaus die Möglichkeit, die öffentliche Verwaltung könne durch die Blockchain ersetzt werden. Die Technologie wird als disruptiv eingeschätzt, denn schließlich stellen manipulationssichere Registerführung und Beglaubigungen gleichermaßen die zentrale Aufgabe der Verwaltung dar. Dies ist das Kernversprechen der Blockchain-Technologie. Mithin hat diese Technologie grundsätzlich das Potenzial, die durch

zentrale Organisationsparadigmen geprägten Verwaltungen nachhaltig zu verändern. Eine Blockchain-Technologie, die quasi ohne zentrale Instanz öffentlich einsehbar, manipulations- und ausfallsicher sowie für jedermann zugänglich ist, also die öffentliche Blockchain, stößt so sehr schnell auf kritische Aspekte. Die für das *Mining (Proof of Work)* in öffentlichen Blockchains erforderliche enorme Rechnerkapazität kann nur in wenigen großen Rechenzentren vorgehalten werden. Hier bestehen das Risiko der Kartellbildung bei öffentlichen Blockchains sowie die Frage, wie lange es eine Bestandsgarantie gibt. Es ist nicht ausgeschlossen, dass es Angreifern gelingt, genügend Knoten in einem Blockchain-Netzwerk zu kontrollieren. Auch besteht das Risiko, dass ein Angreifer die Zeitschalter einzelner Knoten manipuliert und durch falsche Zeitangabe die Aufzeichnung der Transaktionsfolge beeinflussen und fälschen kann. Wenn mehr als 51 % der Rechnerkapazität sich in Hand eines Kartells befindet, kann das Kartell entscheiden, was im Netzwerk geschieht. Die 51 %-Attacke oder *Majority Attack* ist die berühmteste aller Angriffe auf die Blockchain. (Fertig und Schütz 2019). Eine öffentliche Blockchain, auf der die zentralen Registereinträge einer Verwaltung abgebildet werden, wäre dann einem sehr hohen Risiko ausgesetzt, wenn die Profitabilität der privaten *Miner* nicht mehr gewährleistet ist und die Dauerhaftigkeit in Frage gestellt wird. Aus all diesen Gründen wird für die öffentliche Verwaltung der Einsatz einer öffentlichen Blockchain nicht empfohlen. Vielmehr wird dafür plädiert, eine geschlossene Blockchain-Infrastruktur aufzubauen, um einerseits die Vorteile der Technologie zu nutzen und andererseits die Funktionsfähigkeit öffentlicher Verwaltung sicherzustellen und nicht in die Hand privater *Miner* zu geben.

Der Datenschutz im Kontext der Blockchain wird aktuell ebenso intensiv diskutiert. Datenschützer beobachten vor allem die öffentlichen Blockchains mit Skepsis. In der öffentlichen Blockchain sind die Nutzer immer nur pseudonym, nicht anonym, gespeichert. Ein Merkmal der Blockchain ist, dass sie nicht vergisst. Dies wird von Datenschützer\*innen sehr kritisch gesehen (Quiel 2018). In der technischen Weiterentwicklung wird an Lösungen gearbeitet, um vollständig anonym zu agieren. Bei einer privaten Blockchain stellt sich die Lösung etwas anders da: Sowohl die Betreiber\*innen als auch die Nutzer\*innen sind bekannt. In den bisher diskutierten und beschriebenen Blockchain-Lösungen der öffentlichen Verwaltung wird auch davon ausgegangen, dass die zu validierenden Daten nicht direkt in der Blockchain abgebildet werden, sondern in den Registern verbleiben. Weiterhin gibt es für viele Daten, die in öffentlichen Registern gespeichert sind, wie zum Beispiel das Einwohnerwesen oder das Standesamtswesen, kein „Recht auf Vergessen“. Es ist Aufgabe der öffentlichen Register, gerade nicht zu vergessen. In der Literatur zu Blockchain und Datenschutz wird darauf verwiesen, dass bei einer Verarbeitung von Daten, die gemessen anhand eines konkreten objektiven Maßstabes für die Erfüllung eines Vertrages erforderlich sind oder bei überwiegend berechtigten Interessen des Verantwortlichen oder eines Dritten vorliegen (vgl. Art. 6 Abs. 1 lit.a. und f. DSGVO), eine Rechtsgrundlage besteht, um die Datenverarbeitung in einer privaten Blockchain zu erlauben. Wie die Einführung der Blockchain-Technologie steht auch die datenschutzrechtliche Diskussion dieser Technologie erst am Anfang (Quiel 2018).

## 5 Perspektiven für Staat und Verwaltung

Die Nutzung dieser Technologie in der öffentlichen Verwaltung sollte auf Basis einer privaten „Government Blockchain Infrastructure (Govchain)“ erfolgen. Diese Infrastruktur könnte so aufgebaut werden, dass die öffentlichen Rechenzentren – und hier vor allem die kommunalen Rechenzentren – die Aufgabe und Rolle der Knoten in der Blockchain übernehmen. Kommunen, Länder, der Bund oder die Hochschulen, aber auch öffentliche Unternehmen verfügen über eine große Anzahl von Rechenzentren, die das Rückgrat einer solchen Infrastruktur bilden könnten. Unter bestimmten Bedingungen könnten auch private Rechenzentren als beliehene und regulierte Akteure in ein solches Netzwerk einbezogen werden.

Für die konkrete Organisation einer sicheren privaten Blockchain-Infrastruktur der öffentlichen Verwaltung wird deshalb vorgeschlagen, als gesellschaftsrechtliche Organisationsform die Genossenschaft zu wählen. Mitglieder können nur Institutionen der öffentlichen Verwaltung werden. Die Genossenschaft hat den Vorteil, dass sie Mitglieder unterschiedlicher Rechtsformen aufnehmen kann. So können sowohl Rechenzentren in der Rechtsform eines Zweckverbandes, einer öffentlich-rechtlichen Anstalt, eines Regiebetriebes, aber auch in der Rechtsform der GmbH Mitglieder (Gesellschafter) der Genossenschaft werden. Die Genossenschaft selbst kann aber agieren wie ein Unternehmen. Sie kann die Aufnahme der *Nodes*, also der Rechenzentren in die private Blockchain, kontrollieren und Aufnahmekriterien formulieren. Sie kann Kontrollrechte aufgrund von vertraglichen Regeln wahrnehmen. Die *Government-Blockchain* kann als Infrastruktur-Unternehmen verstanden werden, das für das „*Internet of Value*“ die Beteiligung der öffentlichen Verwaltung organisiert und sichert. Auf Basis einer Genossenschaft kann sie in einem föderalen Staat wie der Bundesrepublik Deutschland länderübergreifend tätig werden, ohne dass es Staatsverträge bedarf. Die Genossenschaft kann Mitglieder aus Kommunen, Ländern und dem Bund vereinigen. Ein weiterer Vorteil der genossenschaftlichen Lösung wäre, dass sich zunächst diejenigen organisieren, die von den Vorteilen der Technologie für den öffentlichen Sektor überzeugt sind. Es wäre zunächst eine Allianz der Blockchain-Befürworter möglich und später, wenn überzeugende Anwendungen bestehen, können weitere Interessenten beitreten.

An die Genossenschaftsidee schließt auch die „govdigital e.G.“ mit Sitz in Berlin an, die die Blockchain-Technologie für die öffentliche Daseinsvorsorge nutzbar machen und die IT-Infrastruktur hierfür bereitstellen will. Gegründet wurde *govdigital* Mitte Dezember 2019 von zehn Konsortialpartnern: kommunalen, städtischen und Landes-Rechenzentren sowie länderübergreifenden Organisationen wie der Bundesdruckerei. Ziel ist es, im Sinne einer digitalen Daseinsvorsorge für öffentliche Verwaltungen und andere öffentliche Institutionen eine sichere und verbindliche bundesweite Kommunikation zu gewährleisten und einen dezentralen IT-Betrieb zu organisieren. Dabei befinden sich die Betreiber, gleichzeitig Mitglieder von *govdigital*, ausschließlich in der Hand öffentlicher Organisationen. Jeder dieser Betreiber stellt aus seinem zertifizierten Rechenzentrum die entsprechende IT-Infrastruktur zur Verfügung, bestehend aus Netzwerk, Firewall, Virenschutz, Internetzugang, Speicherplatz, CPU-Kapazität, Überwachung, Backup und weiteren

Administrationsleistungen. Dieses Zusammenspiel der verteilten Komponenten wird von *govdigital* nur orchestriert: Die Mitglieder bleiben Eigentümer der Infrastruktur-Elemente und behalten die organisatorische Hoheit.

Das Modell der Genossenschaft eignet sich besonders für die Erfüllung der gemeinsamen Ziele, es ist öffentlich und kommunal geprägt: Die Mitglieder begegnen sich auf Augenhöhe, gleichzeitig können jederzeit Interessenten hinzustoßen – bei vergleichbar geringem bürokratischen und finanziellen Aufwand. Perspektivisch könnte eine solche Blockchain-Genossenschaft von öffentlichen Rechenzentren auch auf Europa ausgeweitet werden.

Überhaupt müssen die mittelfristigen Perspektiven für die Blockchain-Technologie für die nächsten fünf Jahre europäisch betrachtet werden. Es ist bemerkenswert, mit welchem Engagement sich die Europäische Kommission dem Thema Blockchain widmet. Im April 2018 haben 22 europäische Staaten eine Deklaration unterzeichnet, um diese Technologie weiterzuentwickeln und eine breite Nutzung voranzutreiben. Europa will mit dieser „*Cooperation on a European Blockchain Partnership*“ bei einer grundlegenden Technologie eine treibende und führende Rolle spielen. Ziel der europäischen Partnerschaft ist es, Europa als weltweit führende Staatengemeinschaft bei der Entwicklung, Einführung und Anwendung der *Distributed Ledger Technology* zu positionieren. Im gesamten digitalen Binnenmarkt soll die Anwendung der Blockchain-Technologie im öffentlichen und privaten Sektor vorangetrieben werden. Sehr optimistisch, stellt Mariya Gabriel, EU-Kommissarin für digitale Wirtschaft und Gesellschaft, bei der Unterzeichnung der Partnerschaft fest: „In Zukunft werden alle öffentlichen Dienste die Blockchain-Technologie nutzen. Blockchain ist eine große Chance für Europa und die Mitgliedsstaaten, ihre Informationssysteme zu überdenken, das Vertrauen der Nutzer und den Schutz personenbezogener Daten zu fördern, neue Geschäftsmöglichkeiten und neue Führungsbereiche zu schaffen, von denen Bürger, öffentliche Dienste und Unternehmen profitieren.“ (European Commission 2018). Nach Darstellung der Europäischen Kommission wurden 2018 bereits 80 Millionen Euro in Projekte rund um Blockchain investiert und die EU-Kommission plant, in den nächsten Jahren weitere 300 Millionen Euro auszugeben, um die Entwicklung zu fördern. Auch wurde ein *EU Blockchain Observatory and Forum* gegründet, um europäisches, technisches und regulatorisches Wissen zu sammeln, um die Chancen und Risiken zu betrachten und das technische sowie regulatorische Potenzial zu diskutieren (EU Blockchain Observatory and Forum 2018).

---

## Literatur

- BAMF. 2018. *Unterstützung der Kommunikation und Zusammenarbeit im Asylprozess mit Hilfe von Blockchain. Eine Machbarkeitsstudie*. Nürnberg: Bundesamt für Migration und Flüchtlinge. <http://publica.fraunhofer.de/dokumente/N-519936.html>. Zugegriffen am 11.05.2020.
- Bundesregierung. 2018. Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land. Koalitionsvertrag zwischen CDU, CSU und SPD, 19. Legislaturperiode. <https://www.bundesregierung.de/resource/blob/975226/847984/5b8bc23590>

- <d4cb2892b31c987ad672b7/2018-03-14-koalitionsvertrag-data.pdf?download=1>. Zugriffen am 11.05.2020.
- CDU NRW. 2017. Koalitionsvertrag für Nordrhein-Westfalen 2017–2022. [https://www.cdu-nrw.de/sites/default/files/media/docs/nrwkoalition\\_koalitionsvertrag\\_fuer\\_nordrhein-westfalen\\_2017\\_-\\_2022.pdf](https://www.cdu-nrw.de/sites/default/files/media/docs/nrwkoalition_koalitionsvertrag_fuer_nordrhein-westfalen_2017_-_2022.pdf). Zugriffen am 11.05.2020.
- Drescher, Daniel. 2017. Blockchain *Grundlagen. Eine Einführung in die elementaren Konzepte in 25 Schritten*. Frechen: mitp Verlag.
- EU Blockchain Observatory and Forum. 2018. Blockchain *innovation in Europe*. [https://www.eublockchainforum.eu/sites/default/files/reports/20180727\\_report\\_innovation\\_in\\_europe\\_light.pdf](https://www.eublockchainforum.eu/sites/default/files/reports/20180727_report_innovation_in_europe_light.pdf). Zugriffen am 11.05.2020.
- European Commission. 2018. European countries join blockchain partnership. <https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership>. Zugriffen am 11.05.2020.
- Fertig, Tobias, und Andreas Schütz. 2019. Blockchain *für Entwickler*. Bonn: Rheinwerk Verlag.
- Nakamoto, Satoshi. 2008. Bitcoin: *A peer-to-peer electronic cash system*. <https://bitcoin.org/bitcoin.pdf>. Zugriffen am 11.05.2020.
- Quiel, Philipp. 2018. Blockchain-Technologie im Fokus von Art. 8 GRC und DS-GVO. Ein Zwiespalt zwischen Innovation und unionalem Datenschutzrecht? *Datenschutz und Datensicherheit* 42(9): 566–573.
- Rehfeld, Dieter. 2016. Die Blockchain. Hat sie das Potenzial, Gesellschaft und Wirtschaft neu zu gestalten? In *Transparente Staatstätigkeit*, Hrsg. Benjamin Fadavian, 25–42. Hamburg: tredition.
- Schoder, Detlef, Kai Fischbach, und René Tecihmann. 2002. *Peer to Peer. Ökonomische, technologische und juristische Perspektiven*. Berlin: Springer.
- Swan, Melanie. 2015. Blockchain. *Blueprint for a new economy*. Beijing: O'Reilly.
- Wattenhofer, Roger. 2016. *The science of the blockchain*. Charleston: Inverted Forest Publishing.



---

# Offene Daten (Open Data)

Herbert Kubicek und Juliane Jarke

## Inhalt

1 Klärung der Begriffe .....	76
2 Konzeptionelle Grundlagen .....	78
3 Gesetzgebung und Einsatzfelder .....	80
4 Auswirkungen und Kritik .....	82
5 Perspektiven für Politik, Staat und Verwaltung .....	87
Literatur .....	88

---

## Zusammenfassung

Als *Open Data*, auch *Open Government Data* (OGD), bezeichnet man die tendenziell unentgeltliche Bereitstellung von Daten der öffentlichen Verwaltungen im Internet zur beliebigen Weiterverarbeitung unter freien Lizenzen. Die Forderung stammt von zivilgesellschaftlichen Organisationen und Unternehmen und wird mit unterschiedlichen Nutzenerwartungen verbunden, insbesondere Wirtschaftswachstum, Transparenz und Partizipation sowie neuen bürgerrelevanten digitalen Verwaltungsdiensten. Politik und Verwaltung reagieren überwiegend positiv und bekennen sich zu diesen Zielen. Die Umsetzung ist jedoch sehr unterschiedlich und überwiegend zögerlich. Einer der Gründe dürfte darin liegen, dass die Umsetzung sowohl auf der Ebene der einzelnen Verwaltungen und mehr noch bei den geforderten behördenübergreifenden Portalen sehr komplex und aufwändig ist und bisher der Nachweis für die erhofften positiven Wirkungen

---

H. Kubicek (✉)

ifib: Institut für Informationsmanagement Bremen GmbH, Universität Bremen, Bremen, Deutschland

E-Mail: [kubicek@ifib.de](mailto:kubicek@ifib.de)

J. Jarke

ifib: Institut für Informationsmanagement Bremen GmbH, Universität Bremen, Bremen, Deutschland

E-Mail: [jjarke@ifib.de](mailto:jjarke@ifib.de)

nicht ausreichend erbracht wurde. Eine kritische Prüfung zeigt, dass die bisher vorgetragenen Begründungen für die umfassende proaktive Bereitstellung aller vorhandenen Daten (*Open by default*) nicht haltbar sind und die Ziele auch mit einer Überlassung auf Anfrage (*Open by demand*) zu niedrigeren Kosten erreichbar sind.

### Schlüsselwörter

Civic Apps · Civic Tech · Informationsfreiheit · Open Government · Transparenzportale

## 1 Klärung der Begriffe

Der aus den USA stammende Begriff *Open (Government) Data* (OGD) wird in zwei verschiedenen Bedeutungen verwendet. Zum einen ist er ein wesentliches Element des umfassenderen Konzepts *Open Government*, in der deutschsprachigen Literatur *Offenes Regierungs- und Verwaltungshandeln* (von Lucke und Geiger 2010), das auf US-Präsident Barak Obama zurückgeht. Danach sind Offene Verwaltungsdaten das Fundament für ein Regierungs- und Verwaltungshandeln, das Transparenz, Partizipation und Kooperation insbesondere mit der Zivilgesellschaft anstrebt (Abb. 1).

Obama hatte in seinem ersten Wahlkampf 2009 *Open Government* und *Open Data* als einen von ihm angestrebten „Change“ ankündigt. Noch am Tag seines Amtsantritts verpflichtete er alle Bundesbehörden, innerhalb von 45 Tagen mindestens drei relevante Datensätze unentgeltlich zur Weiterverarbeitung über ein zentrales Portal zur Verfügung zu stellen (Presidential Documents 2009). Als Randnotiz sei angemerkt, dass das Akronym OPEN aus dem von Obamas Vorgänger George W. Bush erlassenen *OPEN Government Act* von 2007 stammt (vollständig: **O**penness **P**romotes **E**ffectiveness in our **N**ational **G**overnment **A**ct of 2007), in dem mehrere Verordnungen zur Verbesserung der Effektivität des *Freedom of Information Act* in den Gesetzestext übernommen wurden.

**Abb. 1** Offene Verwaltungsdaten als Fundament für Offenes Regierungs- und Verwaltungshandeln. (Quelle: eigene Darstellung)



Bei diesem weiten Verständnis von „offenen Daten“ geht es vor allem um einen grundsätzlichen Kulturwandel der Verwaltungen von einer Kultur des Amtsgeheimnisses hin zu einer Kultur der Offenheit und Transparenz. Dabei kommt es nicht darauf an, was konkret mit „Daten“ gemeint ist. In der engeren Verwendung des Begriffs ist jedoch genau dies der zentrale Punkt. Es geht nicht mehr um die Dokumente, die schon seit vielen Jahren aufgrund des *Freedom of Information Act*, in Deutschland des *Informationsfreiheitsgesetzes* des Bundes und ähnlicher Gesetze einer Reihe von Bundesländern, zugänglich gemacht werden, sondern um Daten als Zeichen, die maschinell weiterverarbeitet werden können. Vereinfacht gesagt bestehen Dokumente aus Texten, die von Menschen, aber nicht von Maschinen verstanden werden können, während es bei Daten umgekehrt ist; sie sollen nicht direkt von Menschen verstanden werden, sondern von Maschinen, die von anderen Menschen so programmiert werden, dass daraus neue für Menschen verständliche digitale Anwendungen, sogenannte Apps entstehen.

Als Kriterien der Offenheit gelten international Anforderungen, die 2007 in den USA auf einer von der *Sunlight Foundation*, einer unabhängigen und gemeinnützigen Stiftung, die sich schon lange für freien Informationszugang einsetzt, und dem kommerziell interessierten Verlag *O'Reilly Media* veranstalteten Konferenz als *Open Government Data Principles* definiert wurden (<https://opengovdata.org>). Die Bereitstellung von Daten der Verwaltung bzw. die Daten selbst danach sollen den folgenden Prinzipien entsprechen:

1. **Vollständig:** Alle öffentlichen Daten werden verfügbar gemacht. Öffentliche Daten sind Daten, die nicht berechtigten Datenschutz-, Sicherheits- oder Zugangsbeschränkungen unterliegen.
2. **Primärquelle:** Die Daten werden an ihrem Ursprung gesammelt. Dies geschieht mit dem höchstmöglichen Feinheitsgrad, nicht in aggregierten oder modifizierten Formaten.
3. **Zeitnah:** Daten müssen so rasch wie notwendig zugänglich gemacht werden, um ihren Wert zu sichern.
4. **Zugänglich:** Daten werden so vielen Nutzer\*innen wie möglich für möglichst viele Verwendungszwecke bereitgestellt.
5. **Maschinell verarbeitbar:** Daten werden sinnvoll strukturiert, um automatische Verarbeitung zu ermöglichen.
6. **Nicht diskriminierend:** Daten sind für alle verfügbar, ohne dass eine Registrierung notwendig ist.
7. **Nicht proprietär:** Daten sind in einem Format zugänglich, über das niemand exklusive Kontrolle hat.
8. **Lizenzenfrei:** Daten unterliegen keinem Urheberrecht, Patent, Markenzeichen oder Geschäftsgeheimnis. Sinnvolle Datenschutz-, Sicherheits- und Zugangsbeschränkungen sind zulässig.

Seitdem wurden mehrere Kriterien hinzugefügt, wie die unentgeltliche Bereitstellung, die Vertrauenswürdigkeit der Daten u. a. m. (<https://opengov.data.org>). Teilnehmer der Konferenz waren 30 „Open Government Advocats“, d. h. zivilge-

sellschaftliche Organisationen und Internetfirmen, die diese Kriterien als Forderungen an Obama in seinem Wahlkampf für „Change“ erfolgreich platzieren konnten. In der Folge wurden weltweit Regierungen dazu bewegt, sich zu *Open Government* zu bekennen und ähnliche Verpflichtungen einzugehen. In der 2011 gegründeten *Open Government Partnership* (OGP) haben sich bis heute rund 70 nationale und 15 subnationale Regierungen zu einem offeneren Regieren und Verwalten und einem regelmäßig fortzuschreibenden Nationalen Aktionsplan verpflichtet. Auch die OECD, die Weltbank und die EU unterstützen die Forderungen. Deutschland arbeitet seit Dezember 2016 auf dieser Plattform mit (Wewer und Wewer 2019).

Die OGD-Bewegung fordert mit dem Prinzip der Vollständigkeit die proaktive Bereitstellung aller vorhandenen Daten, die keinen gesetzlichen Beschränkungen unterliegen („Open by default“). Dies gilt für Daten der amtlichen Statistik, für Umwelt- und Verkehrsdaten, für Wahlergebnisse und für Geodaten, an denen seit dem mobilen Internet ein großes wirtschaftliches Interesse bei Internetfirmen entstanden ist. Diese Daten sollen nicht nur von den jeweiligen Behörden auf ihren Internetseiten veröffentlicht werden, sondern auch über zentrale (nationale) Portale auffindbar gemacht werden. Auf diesen *Open Data-Plattformen* oder Portalen werden die Daten der Behörden jedoch nicht zentral gespeichert, sondern dort soll ein Datenkatalog bereitgestellt werden, in dem alle datenhaltenden Stellen ihre freigegebenen Daten mit sogenannten *Metadaten* so beschreiben, dass Interessenten erkennen können, um welche Daten es sich handelt, und über einen *Link* zu dem jeweiligen Speicherort diese Daten dann von dort herunterladen können. Ein *Datenkatalog* ist grundsätzlich wie ein Bibliothekskatalog, der die zugänglichen Bücher und ihre Standorte beschreibt. Nur sind Datensätze zur maschinellen Weiterverarbeitung nicht so einfach zu beschreiben wie Bücher. Zudem sollen die zentralen nationalen Portale nicht nur die Daten aus dem Zuständigkeitsbereich der verschiedenen Bundesministerien zusammenführen, sondern auch die aller Behörden auf Landesebene und in den Kommunen. Dazu sind bundeseinheitliche *Metadatensätze* zur Beschreibung der Daten erforderlich.

---

## 2 Konzeptionelle Grundlagen

Wie die Entstehungsgeschichte zeigt, ist *Open (Government) Data* nicht aus einer wissenschaftlichen Diskussion hervorgegangen, sondern von unterschiedlichen Gruppen von Aktivisten erfolgreich auf die politische Agenda gesetzt worden. Neben Bürgerrechtsgruppen, die sich für den freien Informationszugang zu Verwaltungsinformationen (*Freedom of Information/Informationsfreiheit*) engagieren, sind es maßgeblich auch Gruppen aus der *Civic Technology*-Szene, die nach *Open Source* und *Open Access* nun auch *Open Data* und *Open Government* fordern (Wewer und Wewer 2019, S. 231 f.). Sie sind davon überzeugt, dass man mit dem richtigen Einsatz von Informationstechnik und speziell des Internet eine gerechtere Welt schaffen kann. Der bekannteste Zusammenschluss ist die in Großbritannien

gegründete *Open Knowledge Foundation* mit „Chaptern“ in den meisten EU-Mitgliedstaaten. Das gemeinsame Dach für die Lobbyarbeit bilden die Initiativen im Rahmen der *Open Government Partnership*, in der sich Regierungen zur Zusammenarbeit mit zivilgesellschaftlichen Akteuren verpflichten.

Diese Bewegungen haben in der Politik zur Vergabe von Gutachten und in mehreren wissenschaftlichen Disziplinen zu Versuchen der Einordnung in vorhandene Konzepte und zu deren Weiterentwicklung geführt. So können heute mindestens drei verschiedene Ziele und Wertversprechen von *Open Data* beobachtet werden. Keines dieser drei Ziele ist unumstritten und für keines gibt es einen validen Nachweis der Zielerreichung. Sie werden in diesem Abschnitt zunächst referiert. Nach einem Überblick über den Umsetzungsstand werden sie im vierten Abschnitt kritisch diskutiert.

In der öffentlichen Diskussion über den Nutzen von OGD steht das eingangs erwähnte Transparenzversprechen im Vordergrund, das nach dem Konzept des *Open Government* verlorenes Vertrauen in die Politik wiedergewinnen und mehr *Partizipation* der Bürger\*innen und die Kooperation mit der Zivilgesellschaft ermöglichen soll (oben Abb. 1). Diese Begründung kann sich auf den rechts- und politikwissenschaftlichen Diskurs stützen, wonach Transparenz des staatlichen Handelns ein Ziel und Wert an sich sind, weil nur durch den freien Informationszugang die Bürger\*innen ihre demokratischen Rechte wahrnehmen können. Diesem Ziel wird bisher durch Informationszugangsgesetze Rechnung getragen, und nun soll es durch proaktive Bereitstellung von Daten erweitert werden. Während es kaum Einwände gegen den Grundsatz der Transparenz gibt, sind Ausmaß und Grenzen, die Abwägung mit anderen Grundrechten und vor allem die geeigneten Mittel zur Zielerreichung durchaus umstritten.

Eine zweite Begründung für OGD verspricht einen *volkswirtschaftlichen Wachstumseffekt*, der auch den Verwaltungen zugute kommt. So behauptete die ehemalige EU-Kommissarin Neelie Kroes, die Daten der Verwaltungen wären „Goldminen“ und dieses Gold müsse nur gehoben und verarbeitet werden. Sie sprach aufgrund von mehreren Gutachten von einem erwarteten 40-Milliarden-Euro-Wachstums-schub pro Jahr für die europäische Wirtschaft. Die Bundesregierung bezeichnetet in der Begründung zum *Open Data-Gesetz* Daten als „Treibstoff der Zukunft“ oder als das „neue Öl“ und zitiert eine Studie der Konrad-Adenauer-Stiftung, die ein Wert-schöpfungspotenzial zwischen 12,1 und 131 Milliarden Euro in den nächsten zehn Jahren errechnete. Wissenschaftlich handelt es sich um eine Mischung aus Innovationstheorie und Verwaltungsökonomie.

Einige der von der EU-Kommission in Auftrag gegebenen Studien betrachten speziell den Bereich der *Geodaten*. Hier können positive Wachstums- und Wert-schöpfungseffekte empirisch nachgewiesen werden. Tausende von mobilen Anwendungen mit standortbezogenen Daten sind erst aufgrund der Freigabe von Geo-Koordinaten möglich geworden. Auch öffentlich bereitgestellte meteo-rologische Daten erhöhen den Wert und damit die Nachfrage bei vielen Anwen-dungen. Diese führen zu Umsätzen der Unternehmen und zur Abführung von Umsatzsteuer, so dass diese Einnahmen die Kosten der Bereitstellung über-schreiten können. In Verallgemeinerung des Falls der Geodaten werden nach

Konzepte der volkswirtschaftlichen Wohlfahrtsökonomie Formeln verwendet, mit denen der volkswirtschaftliche Nutzen der Bereitstellung offener Daten nach dem Prinzip *Open by default* errechnet werden soll. So verwendet die zitierte Schätzung der Konrad-Adenauer-Stiftung die folgende Formel, nach der sich der Nutzen U aus dem Produkt aus Einkommen bzw. Kosten F und mehreren Multiplikatoren ergibt (Kuzev 2016). Ähnliche Berechnungen gibt es für Österreich und Berlin.

$$U = F \lambda_1 \lambda_2 \lambda_3 \varepsilon$$

U	Nutzen
F	Einkommen/Kosten
$\lambda_1$	Kostenmultiplikator
$\lambda_2$	Nutzenmultiplikator (direkt)
$\lambda_3$	Nutzenmultiplikator (indirekt)
$\varepsilon$	Elastizität

Als drittes Ziel wird die günstige Entwicklung von innovativen Bürgerdiensten (*public services*) genannt. Bisher werden Daten bereitgestellt, wenn ein ganz bestimmter Dienst entwickelt werden soll. Die proaktive Bereitstellung von Daten nach dem Prinzip *Open by default* wird mit Theorien zur *Open Innovation* begründet: Da es das Wesen von Innovationen ist, dass man sie nicht vorhersehen kann, kann man auch nicht vorab entscheiden, welche Informationen für die Entwicklung neuer *Apps* benötigt werden, sondern man muss alle Daten veröffentlichen, damit innovative und kreative Entwickler auf Ideen für neue *Apps* und Bürgerdienste kommen können. Um einzelne Verwaltungen zu motivieren, ihre Daten zu öffnen, wird ihnen von Organisationen wie der *Open Knowledge Foundation* angeboten, sie bei der Entwicklung innovativer digitaler Verwaltungsdienste zu unterstützen. In den USA scheint dies mit der Initiative *Code for America* gut zu funktionieren, die den Verwaltungen *Volunteers* und Praktikanten vermittelt. Auch einige deutsche Kommunalverwaltungen suchen aktiv den Austausch mit der OGD-Community, veranstalten Wettbewerbe und regelmäßige Treffen. *Civic Tech-Aktivisten* veranstalten sogenannte *Hackathons* und zeigen, wie man Verwaltungsdaten visualisieren oder mit anderen kombinieren kann. Einige Regierungen und Verwaltungen veranstalten *App*-Wettbewerbe und loben Preisgelder für die besten *App*-Ideen und Umsetzungen aus (zum Beispiel *Code for Germany*).

---

### 3 Gesetzgebung und Einsatzfelder

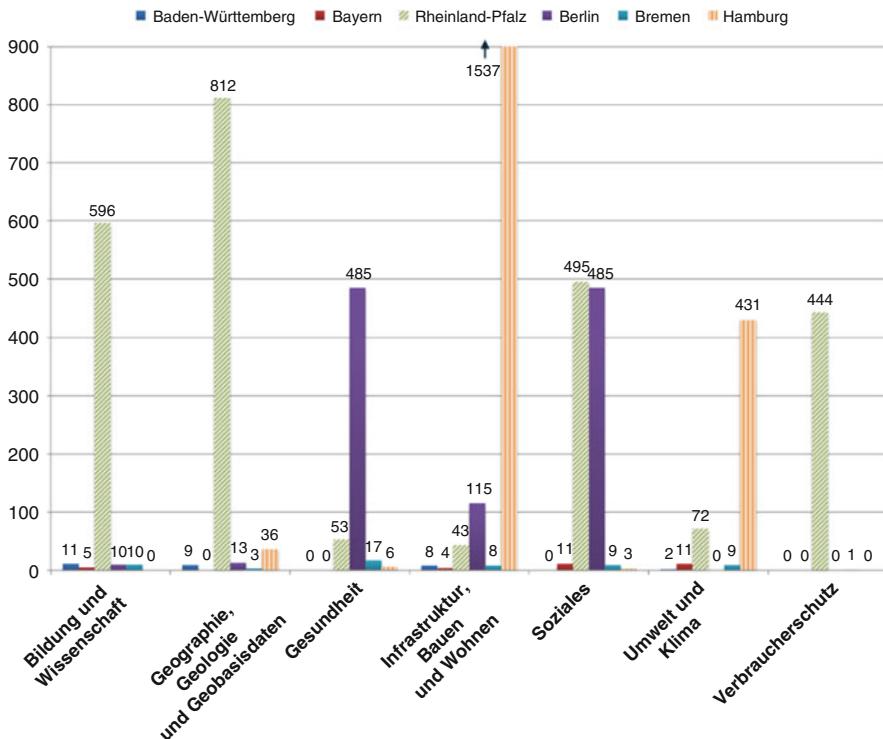
In Deutschland haben auf Bundesebene Zusammenschlüsse zivilgesellschaftlicher Organisationen wie das *Open Data Network* und das *Government 2.0* Netzwerk Deutschland, die *Open Knowledge Foundation* Deutschland und später der Arbeitskreis *Open Government Partnership* sowie zunächst auch die Piratenpartei erfolgreich für die Umsetzung ihrer Forderungen geworben (Kubicek 2017a). Nach einem ersten Bekanntnis der Bundesregierung zu *Open Government* und *Open Data* im Sinne Obamas auf dem IT-Gipfel in Dresden 2010 hat das BMI

2012 eine Konzeptstudie in Auftrag gegeben (Klessmann et al. 2012), einen *Open Data*-Wettbewerb *Apps4Deutschland* zusammen mit den genannten Organisationen gestartet und das Portal *Gov.Data.de* als Pilotprojekt gestartet. 2015 ging das Portal aufgrund eines Staatsvertrages mit mehreren Bundesländern in den Regelbetrieb. Im Frühjahr 2017 wurde ein *Open Data-Gesetz* verabschiedet, das allerdings keine Bereitstellungspflichten beinhaltet, sondern Anforderungen an eine diskriminierungsfreie Bereitstellung definiert. Im selben Jahr vollzog die Bundesregierung den bereits in der Koalitionsvereinbarung 2013 verabredeten Beitritt zur internationalen *Open Government Partnership* und verabschiedete den dort zugesagten Nationalen Aktionsplan. Im Koalitionsvertrag 2018 bekennen sich die Unterzeichner zu den Verpflichtungen aus der *Open Government Partnership*. Die Bundesregierung soll international Vorreiter werden. In einem zweiten *Open Data-Gesetz* soll die Bereitstellung von mehr offenen Daten nach dem Prinzip *Open by default* geregelt werden.

Im Februar 2019 wurde auf dem Portal *govdata.de* folgende Verteilung der Datensätze nach Themengebieten und Bereitstellern angegeben (Tab. 1). Hier zeigt sich eine große Varianz, für die es keine offensichtliche Erklärung gibt. Diese Heterogenität wurde noch deutlicher bei einer früheren, vergleichenden Auszählung der Angebote mehrerer Landesportale (Abb. 2). Rheinland-Pfalz veröffentlichte damals mehr Daten aus den Bereichen Bildung und Geografie als alle anderen

**Tab. 1** Datensätze und Datenlieferanten auf dem Portal *Govdata.de* (Stand: 6. Februar 2019)

Kategorien	Daten-sätze	Datenbereitsteller	Datensätze
Bevölkerung und Gesellschaft	5788	Transparenzportal Hamburg	5860
Bildung, Kultur und Sport	2167	Open-Government-Portal Rheinland-Pfalz	3866
Energie	342	Open NRW	3443
Gesundheit	1085	Freistaat Sachsen	2201
Internationale Themen	98	Statistisches Bundesamt	1974
Justiz, Rechtssystem und öffentliche Sicherheit	3200	Berlin Open Data	1667
Landwirtschaft, Forstwirtschaft, Fischerei und Nahrungsmittel	1874	Regionalstatistik	609
Regierung und öffentlicher Sektor	5537	GDI-DE	531
Regionen und Städte	155	Bundesministerium für Bildung und Forschung	449
Umwelt	5723	Owen Data HRO	208
Verkehr	2545	Bundesministerium des Inneren	201
Wirtschaft und Finanzen	5117	Transparenzportal Bremen	150
Wissenschaft und Technologie	880	Land Brandenburg	100
		Und ca. 320 andere mit 1 bis 39 Datensätzen	



**Abb. 2** Datensätze in sechs Landesportalen (Stand 12.12.2014). (Quelle: [www.open-data-map.de](http://www.open-data-map.de))

Bundesländer, aber weniger zu Gesundheit, Infrastruktur und Umwelt. Trotz eines Umweltinformationsgesetzes in allen Bundesländern veröffentlicht nur Hamburg eine nennenswerte Anzahl von Datensätzen zu Umwelt und Klima. Andererseits liegt der Schwerpunkt der veröffentlichten Daten in Baden-Württemberg in den Bereichen Gesundheit und Soziales. An der von der *Open Data*-Bewegung vermuteten überkommenen Kultur des Amtsgeheimnisses kann dies nicht liegen, denn dann müssten die Zahlen überall gleich niedrig sein. Empirische Studien aus Nachbarländern verweisen auf vielfältige technische, organisatorische, rechtliche, wirtschaftliche und auch psychologische Gründe für diese Varianz (Breiter und Kubicek 2016).

## 4 Auswirkungen und Kritik

Ob die angestrebten Wirkungen größerer Transparenz, stärkerer Bürgerbeteiligung oder wirtschaftlichen Wachstums durch innovative *Apps* auf der Basis Offener Daten eingetreten sind, wurde bisher nicht gründlich untersucht. Bei der Evaluierung des Hamburgischen Transparenzgesetzes, die als die methodisch umfas-

sendste gelten kann, wurde nur der Abruf von Dokumenten und nicht der Abruf von Daten erfasst, die weiterverarbeitet werden können, obwohl dies die konstituierende Leistung des Transparenzportals sein soll. Die geringe und lückenhafte Umsetzung der Datenbereitstellung auf Bundesebene und bei den anderen Landesportalen lässt keine größeren gesellschaftlichen Effekte und wohl auch keine größeren Veränderungen in den Behörden erwarten. Kritiker der oben genannten Ziele und Wertversprechen haben dies aufgrund von Schwächen der referierten Argumente nicht anders erwartet.

In Bezug auf die Transparenzzielen kritisieren Breiter und Kubicek (2016) eine unreflektierte Verwendung des Transparenzbegriffs und die fehlende Beschäftigung mit den komplexen Wirkungsketten und Voraussetzungen, die für eine rezipierte Transparenz und eine tatsächliche Vertrauensbildung auf der Seite der adressierten Bürgerinnen und Bürgern gegeben sein müssen. In der Evaluation des *Hamburgerischen Transparenzgesetzes* wird ausdrücklich betont, dass eine kausale Beziehung zwischen der Veröffentlichung von Daten und einer stärkeren Bürgerbeteiligung oder einem größeren Vertrauen in Politik und Verwaltung nicht nachgewiesen werden kann (Herr et al. 2017).

Es gibt zwar *Apps*, in denen z. B. Haushaltsdaten visualisiert werden. Wie häufig diese genutzt werden, ob sie verstanden werden und welche Schlussfolgerungen Bürger\*innen daraus ziehen, ist bisher nicht untersucht worden. Es gibt auch Beispiele, in denen Daten über Umweltbelastungen veröffentlicht werden, die eine demokratische Kontrolle der Verwaltung verbessern. Es darf jedoch bezweifelt werden, dass dazu der Aufwand der Bereitstellung aller Daten erforderlich ist. Vielmehr kann davon ausgegangen werden, dass die Umweltschützer\*innen sehr gut wissen, welche Daten sie für ihr Monitoring benötigen und diese nach den geltenden Gesetzen gezielt bei den Verwaltungen anfordern können.

Die Forderung nach der unentgeltlichen Bereitstellung aller nicht personenbezogenen Daten zur beliebigen Weiterverarbeitung stellt für viele datenhaltende Stellen einen Paradigmenwechsel dar. Lange Zeit war es Konsens, dass Verwaltungen Daten, die sie für eigene Zwecke erheben und aufbereiten, nach Möglichkeit auch Dritten gegen Gebühren zur Verfügung stellen und damit zusätzliche Einnahmen generieren. Dies galt vor allem für Geodaten, Karten und verschiedene Register, für die es kommerzielle Kunden und Gebührenverordnungen gibt. Wenn Daten verkauft werden, muss man die Weiterveräußerung durch Lizenzbedingungen begrenzen. Unter dem Begriff *Public Sector Information (PSI)* erließ die EU-Kommission Richtlinien für eine einheitliche Gesetzgebung, die eine diskriminierungsfreie, aber keineswegs unentgeltliche Bereitstellung vorgeben. In Deutschland wurde die Richtlinie 2006 mit dem Gesetz über die Weitergabe von Informationen öffentlicher Stellen (*IWG*) umgesetzt. Für Geodaten gibt es spezielle Geodatenzugangsgesetze auf Bundes- und Landesebene.

Mit OGD wird nun eine Kehrtwende gefordert und teilweise auch gewährt, weil es sich angeblich wirtschaftlich lohne. Die Prognose positiver volkswirtschaftlicher Effekte mit der zitierten wohlfahrtsökonomischen Formel wird jedoch auf verschiedenen Ebenen kritisiert (Kubicek 2017b):

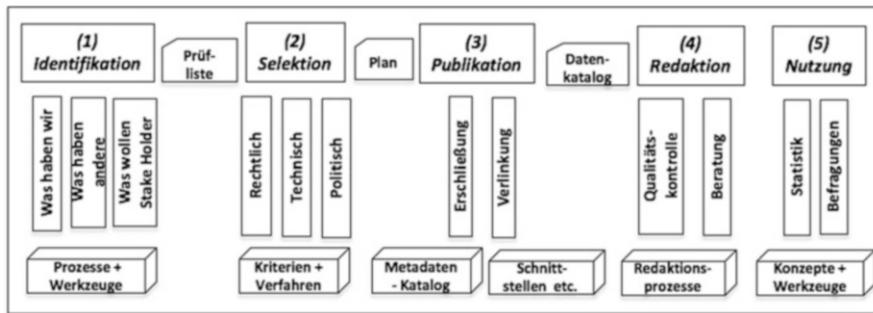
- 1) Die Formel vernachlässigt die mehrstufigen *Wertschöpfungsketten*, die erst zu einem volkswirtschaftlichen Wachstumsschub und daraus resultierenden Steuermehreinnahmen führen könnten. Dazu müssten kommerzielle Entwickler mit diesen Daten *Apps* entwickeln, die so hohe Nutzerzahlen haben, dass über Downloadentgelte und/oder Werbeeinnahmen Erlöse erzielt werden, die dann auch versteuert werden.
- 2) Dabei wird nicht zwischen inhaltlich unterschiedlichen Daten differenziert. Was für Geo- und Wetterdaten nachgewiesen werden kann, gilt nicht für Statistikdaten oder lokale Daten zu Parkplätzen oder Spielplätzen. Teilweise werden die Nutzenmultiplikatoren aus der Nutzung von Geodaten jedoch auf alle Daten übertragen.
- 3) Die Gleichsetzung von Einkommen und Kosten im Faktor F wird damit begründet, dass mangels echter Preise die Kosten als hypothetische Preise herangezogen werden müssen. Für die Schätzung der Kosten- und Nutzenmultiplikatoren liegen keine realen Daten vor.

Eine Schweizer Studie kommt aufgrund einer kritischen Auswertung vorliegender Schätzungen und eigenen Erhebungen zu dem Ergebnis, dass eine seriöse Prognose nicht möglich ist und selbst wenn Steuermehreinnahmen zu erwarten sind, diese nicht bei den Verwaltungen anfallen, bei denen die Kosten entstehen, so dass ein Finanzausgleich zwischen Behörden stattfinden müsste, damit die Kommunen entsprechend investieren (Bürgi-Schmelz 2013).

Für die dritte Begründung mit den innovativen Bürgerdiensten gelten dieselben Einwände wie gegen das Transparenz- und Vertrauensversprechen. Es gibt durchaus Beispiele für *Apps*, die auf Offenen Daten aufbauen und häufig auf *Open Data*-Portalen zu finden sind. Sie beziehen sich auf die Anzeige von freien Parkplätzen, auf Kinderspielplätze und andere Informationen, die im Alltag durchaus nützlich sind. Aber die Frage ist auch hier, ob Entwickler\*innen diese Daten nicht auch direkt bei den zuständigen Verwaltungen anfordern können und erhalten.

Nach der hier vertretenen Auffassung liegt das Hauptproblem aller drei Wertversprechen in der Unterschätzung der mit der Bereitstellung aller nicht personenbezogenen Daten verbundenen Kosten. Teilweise wird argumentiert, die Daten seien bereits intern verfügbar und es wäre kein großer Aufwand, sie auch öffentlich zugänglich zu machen. Dies ist jedoch bei weitem nicht der Fall. Vielmehr sind aufwändige rechtliche Prüfungsprozesse und technische Anpassungsprozesse erforderlich. Diese Prozesse müssen definiert und Personal muss dafür qualifiziert und zugeordnet werden. Die Freie und Hansestadt Hamburg hat beispielsweise für die Entwicklung ihres Transparenzportals für ein dreijähriges Projekt mit mehr als 20 Personen mehr als 5 Mio. Euro investiert. Die Kosten für eine einzelne Schnittstelle schwanken zwischen 2000 und 100.000 Euro. Die jährlichen Betriebskosten wurden mit rund zwei Mio. Euro angegeben.

Mittlerweile gibt es verschiedene Handlungsanleitungen für Verwaltungen mit Empfehlungen für die innerorganisatorische Gestaltung von *Open Data* (z. B. Handbuch für Offene Verwaltungsdaten des Bundesverwaltungsamts (2018)). Aus diesen kann der folgende fünfstufige Prozess als Vorbild abgeleitet werden (Abb. 3):

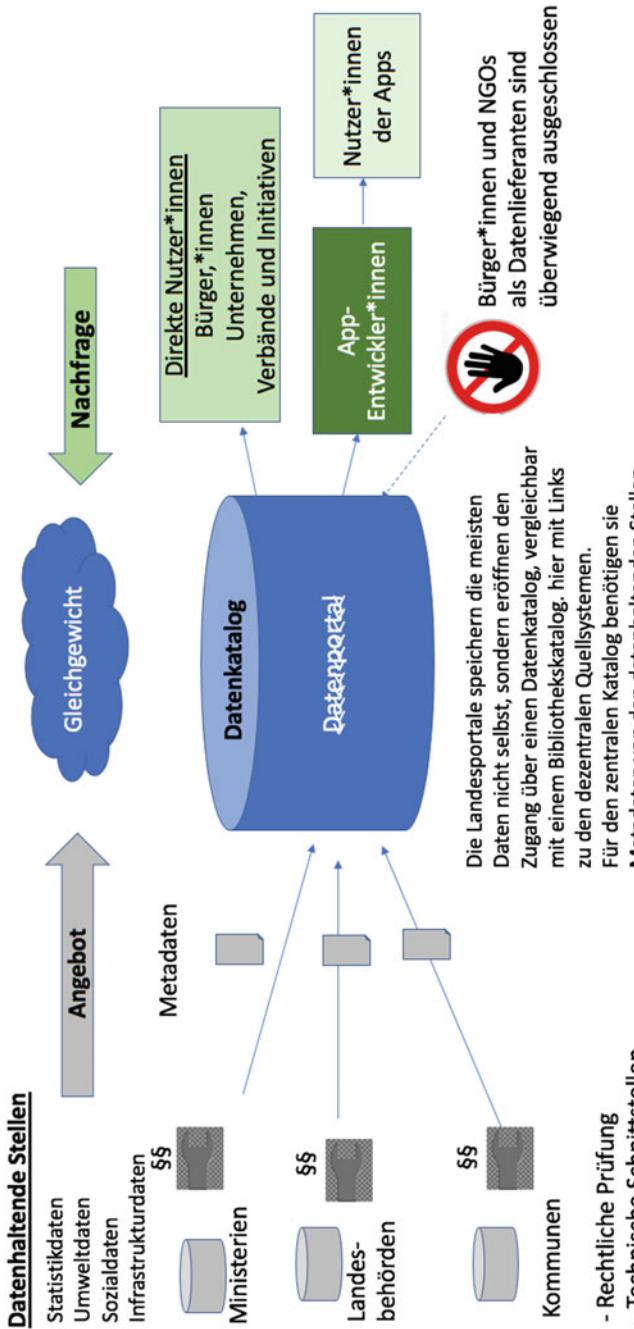


**Abb. 3** Der fünfstufige behördeneinterne Bereitstellungsprozess Offener Daten. (Quelle: eigene Darstellung)

- (1) Da nicht alle vorhandenen Daten binnen kurzer Zeit geöffnet werden können, wird empfohlen, zu Beginn die Daten zu identifizieren, die ausgewählte *Stakeholder* wünschen und/oder die bei vergleichbaren Stellen angeboten und besonders stark nachgefragt werden.
- (2) Aus diesen Kandidaten sollen dann die Daten selektiert werden, für die eine Veröffentlichung unter offenen Lizenzen rechtlich zulässig, technisch zu angemessenem Aufwand machbar und politisch konform ist.
- (3) Die ausgewählten Daten müssen dann für die Veröffentlichung vorbereitet werden, indem die erforderlichen Metadaten generiert werden und die Bereitstellung technisch durchgeführt wird (Schnittstelle, API).
- (4) Da sich Daten ändern, ist eine Aktualisierung und laufende Qualitätssicherung notwendig. Für interessierte Entwickler\*innen sollten Ansprechpersonen benannt werden, da die Metadaten nicht alle Fragen beantworten.
- (5) Um einen Eindruck von der Nachfrage nach den bereitgestellten Daten zu bekommen und für die Identifikation der nächsten bereitzustellenden Daten werden Statistiken und Nutzer\*innenbefragungen empfohlen.

Die Forderungen der *Open Data*-Bewegung gehen jedoch über die Bereitstellungsprozesse in den einzelnen Verwaltungen hinaus und beziehen sich auf ein sogenanntes *Open Data-Ökosystem*, bei dem die eingangs erwähnten *Open Data-Portale* oder *Transparenzportale* im Zentrum stehen. Die OGD-Bewegung sieht sich selbst als Hauptnutzer und weiß, wie aufwändig es ist, Daten mühsam aus den einzelnen kommunalen Internetauftritten herauszusuchen, herunterzuladen und zusammenzuführen. Ein zentraler Datenkatalog als Anlaufpunkt für alle dezentralen Datenquellen ist viel günstiger (Abb. 4).

Der Datenkatalog eines Datenportals ist komplexer als ein regionaler oder bundesweiter Bibliothekskatalog einer größeren Anzahl von Bibliotheken. Dies liegt u. a. an der Heterogenität und Eigenständigkeit der datenhaltenden Stellen und in der Heterogenität der zu katalogisierenden unterschiedlichen Arten von Daten. In einem Landesportal sollen alle in Frage kommenden Daten aller Ministerien und Landesbehörden mit ihren nachgeordneten Behörden und möglichst



**Abb. 4** Elemente einer Open Data Infrastruktur (auch „ÖkoSystem“). (Quelle: eigene Darstellung)

auch aller Kommunen (Städte, Gemeinden und Landkreise) nach einem einheitlichen Schema und einheitlichen Regeln gelistet werden. Das bedeutet u. a., dass einheitliche Metadaten verwendet werden müssten. Harmonisierungen zwischen Bundesländern mit unterschiedlichen Regierungskoalitionen und zusätzlich mit den vielen Kommunen mit ihrer verfassungsmäßigen Selbstverwaltung sind bisher nur unter besonders hohem politischen Druck zustande gekommen. Die drei Nutzenversprechen für OGD haben diesen Druck bisher nicht entfaltet. Denn kein Flächenland hat bisher eine verbindliche *Governance*-Struktur zur Umsetzung dieses Idealmodells entwickelt. Dieser Harmonisierungs- und Standardisierungsbedarf ist auch der Grund dafür, dass Bürger\*innen bei keinem Landesportal oder dem Bundesportal selbst Daten hochladen dürfen (Verbotszeichen in Abb. 4) – obwohl die Kooperation mit der Zivilgesellschaft ein explizites Ziel des *Open Government* ist.

---

## 5 Perspektiven für Politik, Staat und Verwaltung

Zusammenfassend kann man sagen, dass die Begründungen für *Open (Government) Data* eher den Status von Mythen als von wissenschaftlich begründeten Theorien und Fakten besitzen (Wewer und Wewer 2019, S. 256 f.). Politik reagiert jedoch immer wieder auf Mythen, wenn sie glaubt, dass die Wähler\*innen daran glauben und die Demoskopen sie noch befördern. Zurückblickend ist festzustellen, dass die ersten positiven Reaktionen der Politik in Deutschland nach den Erfolgen der Piratenpartei in mehreren Landtagen erfolgten. Mit deren Rückfall in die Bedeutungslosigkeit ist auch das politische Engagement der Bundes- und fast aller Landesregierungen deutlich zurückgegangen.

Manche Landesregierungen haben *Open by default* in Transparenzgesetzen für die eigenen Landesbehörden vorgeschrieben, die Kommunen jedoch überwiegend ausgenommen, um eine Inanspruchnahme nach dem *Konnexitätsprinzip* zu vermeiden. Die Bundesregierung hat ebenso wie die Mehrheit der Landesregierungen für die eigenen Behörden solche Bereitstellungspflichten durch Gesetz oder Verordnung bisher gescheut, und auch viele Kommunen halten sich zurück. Für die Ankündigung eines zweiten *Open Data*-Gesetzes mit diesem Prinzip im Koalitionsvertrag 2018 ist noch keine Umsetzung zu erkennen.

Wenn es darum geht, die geltenden Informationsfreiheitsgesetze durch *Open Data*-Regelungen zu Transparenzgesetzen zu erweitern, stellt sich angesichts der mit *Open by default* verbundenen hohen Kosten und einer schwer erreichbaren Harmonisierung die Frage nach kostengünstigeren Strategien. Im Haushaltsnotlage-land Bremen wurde nach entsprechenden Abwägungen eine gesetzliche Lösung gewählt, die man als *Open by demand* bezeichnen kann (Kubicek 2017b). Dabei wird zwischen Dokumenten und Daten unterschieden, weil die Bereitstellungskosten erheblich differieren. Während Dokumente grundsätzlich pro-aktiv bereitzustellen sind, sollen Daten, die maschinell weiterverarbeitet werden können, in erster Linie auf Antrag bereitgestellt werden. So kann vermieden werden, dass aufwändige Schnittstellen für den Abruf von Daten entwickelt werden, die möglicherweise

nie jemand abrupt. Dem Einwand, dass so *Open Innovation* verhindert werde, ist entgegenzuhalten, dass die Ideen für innovative und erfolgreiche *Apps* nicht aus einem maschinellen Durchforsten von Datenkatalogen entstehen, sondern in erster Linie aus erkannten Informationslücken oder Assoziationen, die durch andere *Apps* hervorgerufen werden. Wer eine Idee für eine *App* hat, kann sich in der Regel bei den in Frage kommenden Verwaltungen erkundigen, welche Daten im Detail vorhanden und erhältlich sind und welche nicht. Da sich vorhandene Datenbestände in Berichten und anderen Dokumenten niederschlagen, schreibt das novellierte Bremer Informationsfreiheitsgesetz die Veröffentlichung aller Dokumente vor, die nicht im einzelnen genannten Beschränkungen unterliegen. Interessenten können dann im Einzelantrag die zugrunde liegenden Daten anfordern.

Inzwischen sind in Bezug auf Transparenz und Partizipation zudem andere Themen weiter oben auf der politischen Agenda gelandet, die auch belegen, dass die Themen, die Bürgerinnen und Bürger bewegen, nicht auf Offenen Daten basieren. Dies gilt für die Dieselkrise und die Migrationspolitik ebenso wie für die Klimapolitik. Die Bürgerbewegungen für Klimaschutz, wie *Fridays for Future*, basieren nicht auf offenen Daten zu Umweltbelastungen, sondern stützen sich auf wissenschaftliche Gutachten. Die USA und das Vereinigte Königreich sind auch kein Vorbild mehr für Offenes Regierungshandeln. Nationalisten, Populisten, *Fake News* stellen einen Diskurswechsel in die entgegengesetzte Richtung dar. Dies lässt aktuell vermuten, dass der Zenit der Diskussion über *Open Data* und *Open Government* wahrscheinlich überschritten ist (Kubicek 2017a). Wewer und Wewer (2019) argumentieren noch viel grundsätzlicher: *Open Data* sei kein Selbstzweck sondern Bestandteil von *Open Government*. *Open Government* aber stärke die repräsentative Demokratie nicht, sondern schwäche sie eher, u. a. weil an den Vereinbarungen zwischen Regierung und Zivilgesellschaft im Rahmen der *Open Government Partnership* die Parlamente nicht beteiligt sind.

---

## Literatur

- Breiter, Andreas, und Herbert Kubicek. 2016. Offene Verwaltungsdaten und Verwaltungstransparenz. *Verwaltung & Management* 22(6): 283–296.
- Bundesverwaltungsamt. 2018. *Handbuch für offene Verwaltungsdaten des BVA*. Stand 08/2018. Köln: Bundesverwaltungsamt. [https://www.bva.bund.de/DE/Services/Behoerden/Beratung/Beratungszentrum/Methoden/\\_documents/stda\\_open\\_data.html](https://www.bva.bund.de/DE/Services/Behoerden/Beratung/Beratungszentrum/Methoden/_documents/stda_open_data.html). Zugegriffen am 20.12.2019.
- Bürgi-Schmelz, Adelheid. 2013. *Wirtschaftliche Auswirkungen von Open Government Data*. Verfasst im Auftrag des Bundesarchivs. Bern. [https://www.egovolution.ch/index.php/download\\_file/force/347/3337/](https://www.egovolution.ch/index.php/download_file/force/347/3337/). Zugegriffen am 20.12.2019.
- Herr, Marius, Christoph Müller, Bettina Engewald, Axel Piesker, und Jan Ziekow. 2017. *Abschlussbericht zur Evaluation des Hamburgischen Transparenzgesetzes*. Speyer: Universität Speyer. [http://www.foev-speyer.de/files/de/fbpdf/\\_vti\\_cnf/InGFA/Abschlussberichte/AB\\_Evaluationde\\_sHmbTG.pdf](http://www.foev-speyer.de/files/de/fbpdf/_vti_cnf/InGFA/Abschlussberichte/AB_Evaluationde_sHmbTG.pdf). Zugegriffen am 20.12.2019.
- Klessmann, Jens, Philipp Denker, et al. 2012. *Open Government Data Deutschland*. Eine Studie zu Open Government in Deutschland im Auftrag des Bundesministeriums des Innern. Berlin: BMI. [http://publica.fraunhofer.de/eprints/urn\\_nbn\\_de\\_0011-n-2139459.pdf](http://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-2139459.pdf). Zugegriffen am 20.12.2019.

- Kubicek, Herbert. 2017a. Open Government. Der Zenit ist überschritten. *Verwaltung & Management* 23(4): 202–212.
- Kubicek, Herbert. 2017b. *Open by default oder Open by demand? Teil I–III. Society Byte*. Bern: Berner Fachhochschule/BFH-Zentrum Digital Society. <https://www.societybyte.swiss/2017/03/01/open-by-default-oder-open-by-demand-teil-i/>. Zugegriffen am 20.12.2019.
- Kuzev, Pencho. 2016. *Open data. The benefits*. Sankt Augustin: Konrad-Adenauer-Stiftung. <http://www.kas.de/wf/de/33.44935/>. Zugegriffen am 20.12.2019.
- Presidential Documents. 2009. Transparency and open government. Memorandum of January 21, 2009. *Federal Register* 74(15): 4685–4686. <https://www.govinfo.gov/content/pkg/FR-2009-01-26/pdf/E9-1777.pdf>. Zugegriffen am 20.12.2019.
- Von Lucke, Jörn, und Christian P. Geiger. 2010. *Open Government Data. Frei verfügbare Daten des Öffentlichen Sektors*. Gutachten für die Deutsche Telekom AG. Friedrichshafen: Zeppelin Universität. <https://www.zu.de/institute/togi/assets/pdf/TICC-101203-OpenGovernmentData-V1.pdf>. Zugegriffen am 20.12.2019.
- Wewer, Göttrik, und Till Wewer. 2019. *Open Government. Stärkung oder Schwächung der Demokratie?* Wiesbaden: Springer VS.



---

# Data mining für responsive Politikgestaltung

Lena Ulbricht

## Inhalt

1 Klärung des Begriffs .....	92
2 Konzeptionelle Grundlagen .....	92
3 Praktische Anwendungsfelder .....	95
4 Umsetzungsstand und Auswirkungen in Deutschland .....	97
5 Perspektiven für Staat und Verwaltung .....	98
Literatur .....	99

---

## Zusammenfassung

*Data mining* ist ein Verfahren der Sozialforschung, das die automatisierte Extraktion von Informationen aus digitalen Spurendaten umfasst. Mit einem Einsatz in Staat und Verwaltung ist die Hoffnung verbunden, sich ein besseres Bild der Bevölkerung machen und Politik responsiver gestalten zu können. Dort, wo bereits mit solchen Verfahren gearbeitet wird, scheint Politik jedoch eher technokratischer zu werden. Anders als in den USA oder Großbritannien wird *data mining* in Deutschland nur selten durch staatliche Akteure eingesetzt und einer Ausweitung stehen zahlreiche Hindernisse entgegen.

---

## Schlüsselwörter

Sozialforschung · Computational Social Sciences · Big Data · Responsivität · Repräsentation

---

L. Ulbricht (✉)

Weizenbaum-Institut für die vernetzte Gesellschaft, Wissenschaftszentrum Berlin für Sozialforschung, Berlin, Deutschland

E-Mail: [lena.ulbricht@wzb.eu](mailto:lena.ulbricht@wzb.eu)

## 1 Klärung des Begriffs

Die Verbreitung digitaler Verfahren in allen Lebensbereichen führt dazu, dass zunehmend Daten über Populationen anfallen: eine voranschreitende „Datafizierung“ der Gesellschaft. Nicht nur Unternehmen nutzen diese Daten; auch staatliche Akteure erhoffen sich viel davon. Ein Anwendungsbereich ist etwa die Vermessung der Bevölkerung anhand digitaler Daten und Analyseverfahren, mit dem Ziel, so gewonnene Erkenntnisse in politische Prozesse einfließen zu lassen. Dazu zählen etwa *big data analytics*, *people analytics*, *web scraping*, *opinion mining*, *sentiment analysis*, *digital listening*, *predictive analytics* und *nowcasting*. Diese Verfahren gehen aus dem interdisziplinären Forschungsfeld *computational social sciences* (seltener auch *digital methods*, *social physics*, *policy analytics* und *policy informatics*) hervor, in dem neben Sozialwissenschaftler\*innen auch Informatiker\*innen, Physiker\*innen und Ingenieur\*innen tätig sind. Diese Verfahren werden hier unter dem Oberbegriff des *data mining* versammelt, der automatisierten Extraktion von Informationen aus massiven und heterogenen Datenbeständen mit dem Ziel der Wissensgenerierung (Ulbricht 2019).

Aus den Eigenschaften *online* gewonnener Daten entstehen zahlreiche Möglichkeiten und Herausforderungen. Die Größe und Vielfalt der Daten ermöglicht prinzipiell Inferenzschlüsse und Vorhersagen in neuem Ausmaß: Wo Daten über große Populationen vorhanden sind, können Rückschlüsse über Individuen gezogen werden, über die keine oder nur wenig Daten vorliegen. Bestandteil vieler *data mining*-Anwendungen sind explorative Verfahren der Musterkennung: Aus dem Verhalten von Nutzer\*innen in sozialen Netzwerken werden Vorhersagen mit Blick auf verschiedene Lebensbereiche getroffen, etwa über den Bildungsverlauf, die berufliche Entwicklung, Familiengründung, Konsum oder Wahlentscheidungen. Zusätzlich zu traditionellen statistischen Verfahren setzen Analyst\*innen zunehmend maschinelles Lernen ein, um die Validität von Vorhersagemodellen zu verbessern.

---

## 2 Konzeptionelle Grundlagen

Für Staat und Verwaltung sind die entsprechenden Verfahren aus zahlreichen Gründen interessant: Zuerst verheißen sie aufgrund der Masse und Vielfalt der Daten ein getreueres Abbild der Gesellschaft. Studien, die anhand von *data mining* Aussagen über Populationen treffen und diese als Evidenz für politische Entscheidungen propagieren, betonen die Überlegenheit entsprechender Methoden im Vergleich zu traditionellen Formen der Bevölkerungsvermessung. Zu diesen traditionellen Formen zählen etwa Daten aus der amtlichen Statistik, Prozessdaten von Behörden, Zensusdaten, Befragungen, Fokusgruppen, Interviews, Beobachtungen etc. Diese werden durch staatlich finanzierte Forschungseinrichtungen, durch Behörden und private Umfrageinstitute erhoben. Charakteristisch für diese traditionellen Daten ist, dass sie dezidiert für den Zweck der *Sozialforschung* erhoben werden. *Data mining* hingegen operiert mit Daten, die nicht in erster Linie für politische oder administrative Zwecke erhoben wurden, sondern eher Nebenprodukte anderer Funktionen sind.

So sammeln digitale Endgeräte und *Websites* mittels *Trackern* und Sensoren automatisiert vielfältige Informationen über Nutzer\*innen. Entsprechend leidet *data mining* im Gegensatz zu „klassischen“ Befragungen nicht an sinkenden Antwortraten. Für die Befragten stellt es nämlich keinen zusätzlichen Aufwand dar und auch für die Datensammlung bedeutet es weniger Kosten, da Daten analysiert werden, die ohnehin entstanden sind. Ein weiterer Vorteil des *data mining* liegt darin, dass die Beobachteten sich der Situation nicht bewusst sind und entsprechend kein strategisches Antwortverhalten entwickeln. Die gewonnenen Erkenntnisse gelten schließlich als objektiver, da sie in erster Linie Verhalten beobachten und ungefragt geäußerte Stellungnahmen auswerten. Ein weiterer Unterschied sind die Zeitabstände der Beobachtung: Während Meinungsumfragen und nationale statistische Erhebungen in Abständen von Jahren (Zensus und Mikrozensus), Monaten („Sonntagsfrage“) oder nur zu bestimmten Stichtagen durchgeführt werden, ist *data mining* prinzipiell immer möglich. Es erlaubt Analyst\*innen, sich häufiger ein Bild der Lage zu machen sowie (vermutete) Einstellungen zu ganz bestimmten Zeitpunkten zu messen, auch retrospektiv, im Zeitvergleich sowie über eine frei wählbare Dauer. Auf diese Weise sind „Echtzeit-Analysen“ der Bevölkerung möglich, so das Versprechen. Darüber hinaus wird *data mining* als ein Verfahren dargestellt, das fragmentierten und komplexen Gesellschaften besser gerecht wird, da über einzelne Individuen mehr Daten vorhanden seien als je zuvor. Zudem könnten Bevölkerungen in allen Weltregionen beobachtet werden, selbst in entlegenen Gebieten, die für traditionelle Erhebungen schwer zugänglich sind.

Die entsprechenden Verfahren werden durch zahlreiche staatliche Akteure genutzt, aber primär von Forscher\*innen und Beratungsunternehmen ausgeführt. Nur selten führen Behörden, Parteien und Interessengruppen sie auch *in-house* durch. Manche Länder wie die USA und die Niederlande bemühen sich um die Koordination von *data mining*-Analysen als Teil der nationalen Sozialberichterstattung: Statistische Ämter nehmen *data mining*-basierte Indikatoren mit auf bzw. erproben diese (Grommé 2018). Die American National Science Foundation zum Beispiel hat sich zum Ziel gesetzt, *social observatories* zu errichten, um traditionelle mit neuen Daten und Analysen zu kombinieren und sich dadurch ein umfassendes und tagesaktuelles Bild der Bevölkerung machen zu können (American National Science Foundation 2012).

Auf dieser Grundlage erhoffen sich staatliche Akteure von *data mining* neue Möglichkeiten, die *Responsivität* staatlichen Handelns zu steigern. *Responsivität* gilt als ein zentraler Kennwert der Qualität moderner Demokratien. Hanna Pitkin zufolge ist *Responsivität* eines der zwei Elemente, die *Repräsentation* ausmachen. Das zweite Element ist die politische Führung, die im Sinne des Gemeinwohls urteilt und handelt (Pitkin 1967, S. 169, 193). Der Kern des Versprechens, dass *data mining* Politik responsiver machen könne, lautet, dass eine bessere Kenntnis der Bevölkerung es erlaube, deren Eigenschaften, Bedürfnisse und Präferenzen in größerem Ausmaß in Politikgestaltung einfließen zu lassen. In dieser Lesart können politische Eliten auf der Grundlage von *data mining* mehr Stimmen „hören“, sich häufiger ein Stimmungsbild verschaffen und politische Interventionen beständig darauf überprüfen, ob sie noch dem Volkswillen entsprechen und sie ggf. zeitnah anpassen.

Regierungen in Australien und Großbritannien haben auf Grundlage von *data mining* politische Strategien wie etwa *open policy making* oder *agile policy making* (*Government Digital Service 2017*) sowie eine *public service big data strategy* (*Australian Government 2013*) entwickelt. Diese Konzepte sollen experimentell und schnell anpassungsfähig sein und dabei die Bedürfnisse der Bürger\*innen ins Zentrum zu stellen. Nicht nur Regierungen und Verwaltungen, auch politische Parteien und Interessengruppen nutzen *data mining*, um sich ein detaillierteres Bild der Bevölkerung und gesellschaftlicher Gruppen zu machen und in ihre politischen Strategien zu integrieren.

Es gibt allerdings auch Befürchtungen, dass *data mining* ein verzerrtes Bild der Gesellschaft und somit wenig valide Befunde liefern könnte. Ein zentrales Problem ist der *digital divide*, also der Umstand, dass Populationen unterschiedlich gut Zugang zu digitalen Medien haben. Entsprechend sind englischsprachige, junge und urbane Populationen in digitalen Datensätzen überrepräsentiert. Zudem verändert sich das Internet im Zeitverlauf, so dass die Validität von Längsschnittanalysen begrenzt ist: Nutzerverhalten auf *Facebook* aus dem Jahre 2008 ist mit jenem von 2018 in vielen Dimensionen nicht vergleichbar. Eine weitere Herausforderung von Analysen auf Grundlage von *data mining* ist der Umstand, dass Analyst\*innen meist sehr wenig über den Kontext der Datengenerierung wissen. Dies schränkt die Validität der Analysen massiv ein und führt zu Unsicherheiten bei der Interpretation der Befunde: In welchem Verhältnis stehen zum Beispiel *Online*-Verhalten und politische Orientierung? Analyst\*innen stehen zudem vor der Aufgabe, *Bots* zu identifizieren, Ironie und Sarkasmus zu erkennen und Affekte bzw. Einstellungen nicht nur dichotom zu erfassen (positiv-negativ), wie es bislang häufig praktiziert wird. Darüber hinaus ist das Bürger\*innenbild der gegenwärtigen Verfahren häufig sehr verhaltenszentriert. Idealtypisch gesprochen beobachten *data mining*-Analyst\*innen Bürger\*innen aus der Ferne, treten aber nicht an diese heran, um ihr Wissen und ihre Sinnzuschreibungen zu erfahren. Doch wenn Befürworter solcher Verfahren *Online*-Verhalten als Äußerung politischer Präferenzen und Absichten verstehen, verlieren sie aus dem Blick, dass das beobachtete Verhalten in vielen Fällen nicht dezidiert *politisch* intendiert war. So widerspricht die Beobachtung von Nutzer\*innen ohne deren Wissen mitunter ethischen Forschungsstandards.

Eine weitere Befürchtung ist, dass Regieren auf der Grundlage von *data mining* technokratischer werden könnte. So skizziert etwa der Rechtsprofessor Richard T. Ford eine Dystopie, in der Datenanalyse politische Partizipation ersetzt: „In fact, why not dispense with cumbersome voting altogether? A computer simulation of the preferences of all citizens could compile the Pareto Superior outcome for any given collective decision (...). Think of the benefits – no money in politics problems, no deceptive ads, no graft and corruption. Best of all, no time wasted studying the issues, and yet we still get better substantive representation than any possible system of actual representation“ (*Ford 2000*, S. 1579). Eine entsprechend technokratische Deutung des *data mining* kommt gänzlich ohne politische Partizipation aus. Trotz Initiativen, die sich darum bemühen, Bürgerinnen und Bürger in die Entwicklung

digitaler staatlicher Dienstleistungen und Verfahren zur Bürgerbeteiligung zu integrieren (*civic tech*), bleibt deren Rolle hier meist begrenzt: Sie sollen auf Probleme hinweisen und Daten spenden, werden aber an der Analyse und Interpretation eben jener Daten nicht beteiligt. Die Möglichkeiten der Bevölkerung und des politischen Systems, über digitale Verfahren politische Repräsentation herzustellen, werden zudem häufig überschätzt (Kelty 2017). Das Problem, eine heterogene Bevölkerung angemessen in Politikgestaltung einzubeziehen, lässt sich nicht lösen, indem mehr Menschen an digitale Dienste angeschlossen werden oder indem traditionelle Datensätze mit neuartigen ergänzt werden.

Eine weitere Befürchtung gegenüber *data mining* für politische Zwecke ist, dass es hyper-responsive Politik zeitigen könnte (Ulbricht 2019). Anders als bei Wahlprogrammen und Regierungserklärungen, durch die Parteien und Regierungen sich für die Dauer einer Legislaturperiode festlegen, verspricht *data mining* häufigere Anpassungen der Programmatik an Bürger\*innenpräferenzen. Sollte die Bedeutung von *data mining*-basierten Echtzeit-Analysen der Bevölkerung zunehmen, bergen sie das Risiko, beständig neue programmatische Änderungen zu begründen, die allerdings nicht beidseitig, sondern allein durch Eliten festgelegt werden. *Agile policy making kann so leicht in hyper-reactive policy making umschlagen*. Eine radikal an Meinungsschwankungen orientierte Politik könnte sich stark an Mehrheitsmeinungen orientieren und bestimmte Gruppen, etwa Nicht-Wähler\*innen oder künftige Generationen, außer Acht lassen (Ulbricht 2019).

---

### 3 Praktische Anwendungsfelder

Politisches *data mining* hat verschiedene Ausprägungen: Eine Variante sind Verfahren, in denen digitale Spurendaten mit relativ einfachen quantitativen Analyseverfahren (Regressionen, Netzwerkanalysen, Clusteranalysen) ausgewertet werden. Einfaches *data mining* mit Spurendaten nutzen Ermittlungsbehörden, um Aufschluss über kriminelle und terroristische Netzwerke zu erlangen, indem sie Netzwerkanalysen mit Daten über das *dark net* sowie Konsum- und Mobilitätsdaten durchführen. Häufig werden digitale Spurendaten mit anderen Verwaltungsdaten kombiniert, wie etwa im Hessischen Polizeiinformationsportal „*hessenDATA*“. Polizeieinheiten analysieren Daten aus sozialen Medien, um die Gewaltbereitschaft von Demonstranten oder bestimmte Delikte vorherzusagen (*predictive policing*). *Data mining* wird auch eingesetzt, um die Ausbreitung von Krankheiten, von Wohlbefinden und Konsum zu verfolgen und vorherzusagen. In Regionen, deren Populationen wegen politischer Instabilität schwer abzubilden sind, wird *data mining* genutzt, um Hilfsleistungen zuzuweisen (*The Carter Center* 2017). Ein weiteres Beispiel ist die Analyse von *Online*-Verhalten und Aussagen in sozialen Netzwerken oder auf Webseiten mithilfe von *webtracking*, *NLP* (*natural language processing*) und *A/B-Testing*, um Stimmungsbilder zu erfassen, Wahlergebnisse vorherzusagen oder Wähler\*innen anzusprechen, das sogenannte *political micro-targeting* (Karpf 2016; Kreiss 2016). Parteien und

Regierungsstellen in zahlreichen Ländern nutzen diese Verfahren in Wahlkämpfen und zum Teil auch außerhalb von Wahlkämpfen (*Tactical Tech* 2019, S. 40 f., 56 f., 60 f.).

Eine zweite Variante von *data mining* ist, Spurendaten mit komplexen Analyseverfahren wie etwa *machine learning* auszuwerten. Dieses komplexe *data mining* mit Spurendaten ist im staatlichen Kontext noch selten. Ein Beispiel ist etwa die Auswertung der sogenannten Fluggastdaten in vielen Industrienationen. Hier werden komplexe Mobilitäts-, Konsum- und Netzwerksdaten mithilfe von *machine learning* ausgewertet, um risikobehaftete Individuen zu identifizieren, etwa mutmaßliche Kriminelle oder Terroristen. Auch Verfahren der Gesichts-, Stimm- und Bewegungserkennung zählen dazu; sie finden überwiegend im Bereich der Sicherheitspolitik Anwendung, etwa zur Beobachtung von Großereignissen, der Prävention und Verfolgung von Kriminalität und für militärische Zwecke. Die EU setzt an Grenzen in Ungarn, Griechenland und Lettland stimmbasierte, automatisierte Lügendetektoren in Asylverfahren ein und die Polizei in Spanien verwendet Stimmanalysen, um die Validität telefonischer Meldungen zu prüfen (*Algorithm Watch* und Bertelsmann Stiftung 2019, S. 37, 121).

Eine dritte Variante ist schließlich komplexes *data mining* mit traditionellen Daten. Hier werden Verwaltungsdaten verschiedener Provenienz und Art kombiniert und mit komplexen Verfahren ausgewertet, um neue Erkenntnisse zu gewinnen. Typisch sind etwa Risikoscores und Vorhersagen, wie sie beispielsweise durch Arbeitsämter in Österreich, Belgien und Polen durchgeführt wurden, um die Arbeitsmarktchancen von Arbeitslosen zu bewerten (*Algorithm Watch* und Bertelsmann Stiftung 2019, S. 108). In Großbritannien (Kent County) werden Gesundheitsdaten verschiedener Quellen explorativ ausgewertet, um bestimmte Populationen zu präventiven Untersuchungen zu bewegen (Dencik et al. 2018, S. 42). Darüber hinaus werden im Londoner Viertel Camden mithilfe vielfältiger Verwaltungsinformationen und Inferenzverfahren Bürger\*innenprofile geschaffen, um Sozialbetrug und illegale Unter Vermietungen zu bekämpfen (Dencik et al. 2018, S. 48). In verschiedenen britischen Städten werden vielfältige Sozialdaten mithilfe von maschinellem Lernen ausgewertet, um die Gefährdung von Kindern und Jugendlichen vorherzusagen (Dencik et al. 2018, S. 27).

Dennoch sind viele der Eigenschaften von *data mining*-Verfahren für den staatlichen Kontext wenig geeignet. Ein Problem ist die weiter oben dargelegte mangelnde Validität der Befunde. Mögliche Verzerrungen oder Fehler sind im Marketing oder in der Grundlagenforschung unbedenklich, im staatlichen Bereich jedoch illegitim. Ein weiteres Problem sind *machine learning*-Analyseverfahren, die die Nachvollziehbarkeit und die Transparenz gefährden. Bei *deep learning* oder sehr komplexen *decision trees* ist nicht nachvollziehbar, wie eine bestimmte Vorhersage entstanden ist. Wenn entsprechende Verfahren jedoch für die Allokation von Sozialleistungen, in der Strafverfolgung oder in der Kinder- und Jugendhilfe eingesetzt werden, ist ein hohes Maß an Intransparenz äußerst problematisch. Es gibt Fälle, in denen Regionalregierungen in den USA und in Neuseeland den Einsatz von prädiktiven Verfahren im staatlichen Bereich wegen mangelnder Transparenz wieder eingestellt haben.

## 4 Umsetzungsstand und Auswirkungen in Deutschland

Verglichen mit anderen Ländern nutzen staatliche Akteure in Deutschland *data mining* nur wenig. Allerdings beobachten sie die Erfahrungen im Ausland aufmerksam und erproben Machbarkeit und Mehrwert im Rahmen erster Anwendungen, Pilot- und Forschungsprojekte.

Das einfache *data mining* mit Spurendaten ist in Deutschland noch die Ausnahme: Ein Beispiel ist das BMBF-Forschungsprojekt PANDORA, das anhand von *Social Media*-Daten Radikalisierung beobachten will und an dem neben öffentlichen Forschungseinrichtungen auch das BKA und zwei LKAs beteiligt sind. PANDORA steht für „Propaganda, Mobilisierung und Radikalisierung zur Gewalt in der virtuellen und realen Welt“. Zu nennen ist zudem die Risikobewertungs-*Software* RADAR-iTE des BKA („Regelbasierte Analyse potenziell destruktiver Täter zur Einschätzung des akuten Risikos – islamistischer Terrorismus“), die auf der Grundlage von vielfältigen Informationen über Zielpersonen, die unter anderem aus den sozialen Medien stammen, einen Gefährdungsscore erzeugt. Ein anderes Beispiel sind die Versuche von Regierungsstellen und Parteien, anhand von *Twitter*- und *Facebook*-Daten die öffentliche Meinung zu beobachten. Entsprechende Projekte werden allerdings selten offen kommuniziert – aus Furcht vor kritischer Berichterstattung und aufgrund einer zurückhaltenden Einschätzung bezüglich des zu erwartenden Nutzens.

Auch das komplexe *data mining* mit Spurendaten ist in Deutschland sehr selten. Eine Anwendung ist die Sammlung und Analyse von Fluggastdaten durch das BKA, um mithilfe von *machine learning* verdächtige Muster und Risikopersonen zu identifizieren, die des Terrorismus oder der schweren Kriminalität verdächtigt werden können. Darüber hinaus gibt es Projekte, in denen automatisierte Bild- und Videoerkennung für die Sicherung des öffentlichen Raums erprobt werden. Digital erhobene Daten werden hierfür mithilfe von maschinellem Lernen ausgewertet, allerding geht es bislang um die Erkennung gesuchter Personen und bestimmter Bewegungen und (noch) nicht um die Generierung von Vorhersagen über kriminelles Verhalten aus Bildern und Videos. Entsprechende Projekte führen die Bundespolizei (Projekt Videoüberwachung am Bahnhof Berlin Südkreuz) und die Polizei Mannheim durch. Darüber hinaus verwendet das BAMF automatisierte Sprachanalysen, um Berichte in Asylverfahren zu validieren.

Komplexes *data mining* mit traditionellen Daten findet man in deutschen Behörden nur in Ansätzen. Meist werden Daten aus verschiedenen staatlichen Quellen kombiniert, um daraus automatisiert neue Erkenntnisse zu gewinnen. Die Bundesagentur für Arbeit nutzt etwa Analysen der Nutzung ihres Vermittlungsportals durch Arbeitsvermittler, Arbeitssuchende und Arbeitgeber, um das *matching* zu verbessern (Hartl et al. 2018). Und die Polizei in sechs Bundesländern wertet Informationen über Einbruchsdiebstahl mithilfe von *machine learning* aus, um Einbrüche vorherzusagen und zu verhindern.

Ob und in welcher Form *data mining* staatliche Steuerung verändert, ist bisher nicht erforscht. Hier wären Studien notwendig, die *data mining* mit traditionellen Formen der Sozialforschung vergleichen. Mit Blick auf die Möglichkeiten, auf der

Grundlage solcher Analysen das Verhalten von Bürger\*innen zu beeinflussen, kreist die öffentliche Debatte um zwei Thesen: Die eine geht davon aus, dass Verhaltensbeeinflussung durch staatliche Akteure stärker individualisiert und machtvoll wird, zudem kaum wahrnehmbar ist und sich deshalb für unethische Zwecke anbietet, wie beispielsweise Manipulation oder Diskriminierung. Dies wurde im Kontext der Kontroverse über das Unternehmen *Cambridge Analytica* diskutiert, das *Facebook*-Daten und psychometrische Profile für Wahlkampagnen in den USA und Großbritannien eingesetzt hat. Die entgegengesetzte These besagt hingegen, dass *data mining* aufgrund der ungenauen Datenbasis und methodischer Mängel die adressierten Populationen schlecht trifft und Interventionen auf dieser Grundlage wenig wirksam sind. Gesicherte Erkenntnisse über die Effektivität von Verhaltensbeeinflussung auf der Grundlage von *data mining* liegen bislang nicht vor, da ein entsprechender Nachweis methodisch sehr anspruchsvoll ist und Forscher\*innen häufig nicht über die notwendigen Informationen verfügen. Meist werden Datenbasis, Algorithmen und Verwendungszweck von den beteiligten Organisationen geheim gehalten.

---

## 5 Perspektiven für Staat und Verwaltung

In welchem Ausmaß sich *data mining* in westlichen Demokratien ausbreitet, hängt von zahlreichen institutionellen, rechtlichen, finanziellen und normativen Faktoren ab. In Deutschland sind Staat und Verwaltung gegenüber solchen Verfahren vorsichtig und versuchen sich in ersten Pilot-Projekten. In den USA, wo ein anderes Verständnis von Datenschutz herrscht, ist *data mining* durch politische Parteien und Interessengruppen fester Teil des Repertoires in Wahlkämpfen geworden und in verschiedenen Bereichen der öffentlichen Verwaltung üblich – bei großen Schwankungen zwischen Bundesstaaten und Politikbereichen. Das weltweit umfassendste Projekt der staatlichen Bevölkerungsbeobachtung und -beeinflussung mithilfe digitaler Spurendaten ist das chinesische *social credit system*, das sich im Aufbau befindet.

Dass *data mining* zwar im Marketing boomt, jedoch nicht im staatlichen Bereich, liegt unter anderem daran, dass es voraussetzungsvoll ist, große, heterogene Datensammlungen unterschiedlicher Provenienz und Qualität auszuwerten. Um Daten beschaffen, sichern und aufbereiten zu können, bedarf es zahlreicher Ressourcen. Dazu gehören unter anderem die rechtliche Kompetenz zur Datenerhebung, Expertise in Datenbankverwaltung, Interoperabilität und Datenaufbereitung, technische Schnittstellen zur *Software*, die die Daten erhebt, und *Server*- und Rechnerkapazität. Nur wenige staatliche Akteure verfügen über die entsprechenden Infrastrukturen und Kompetenzen, sie können etwa nur unter bestimmten Bedingungen und zum Teil gegen Geld auf Daten aus sozialen Netzwerken zugreifen und Angebote von Datenhändlern (*data brokers*) nicht nutzen, da sie sonst Datenschutzrecht verletzen würden. Für weitere Anwendungen, die in deutschen Behörden diskutiert werden, etwa die automatisierte Auswertung der Performanz sozialer Träger oder der Wirksamkeit bestimmter Sozialleistungen, müssten erst gemeinsame Datenspeicher (*data ware-*

*houses)* geschaffen werden. Dies ist wegen des deutschen Datenschutzrechts und der hohen Kosten für die Herstellung von Interoperabilität sehr voraussetzungsvoll. Ob eine entsprechende Dateninfrastruktur geschaffen wird, ist für die Ausbreitung von *data mining* durch staatliche Behörden in Deutschland entscheidend.

Die Beispiele aus dem Ausland zeigen zudem, dass *data mining* in staatlichen Behörden Widerstände erzeugt. So gibt es zum Beispiel Kritik daran, in der Sozialpolitik und der Strafverfolgung Informationen einzubeziehen, die entweder nicht offensichtlich für den Sachverhalt relevant sind (etwa Mobilität als Indikator für Kriminalität) oder die zwar relevant sind, aber nicht direkt von den betroffenen Personen stammen (aus einer Befragung), sondern externer Natur sind (durch Beobachtung entstehen). Ein zweiter wichtiger Konfliktpunkt ist die Bedeutung beruflicher Erfahrung und Intuition von Behördenmitarbeiter\*innen im Vergleich zur computergenerierten Empfehlung. Beide können in Widerspruch geraten und die Priorisierung ist nicht immer klar. Auch mit Blick auf die Nutzung digitaler Verhaltensdaten für zielgerichtete Bürger\*innenansprache durch Parteien und Regierungen hat in Deutschland, wie auch in anderen Ländern, eine rege Kontroverse über illegitime politische Manipulation und über eine mögliche Fragmentierung der politischen Öffentlichkeit provoziert. Vor diesem Hintergrund erscheint es im Moment unwahrscheinlich, dass staatliche Akteure *data mining* stark ausweiten werden.

Anders als durch Technologiekonzerne und Politikberatungsunternehmen propagiert, betrachten deutsche Akteure aus Politik und Verwaltung *data mining* nicht als geeignet, Prozesse zu entpolitisieren und scheinbar objektive Entscheidungen auf der Grundlage moderner Datenanalyse zu treffen. Hier besteht vielmehr die Ansicht, dass der „Volkswille“, auf den politische Eliten reagieren sollen, uneindeutig und nur bedingt objektivierbar ist. Entsprechend ergänzt *data mining* andere Verfahren der Sozialforschung und ist in Entscheidungsprozessen ein Faktor von vielen – und vermutlich nicht der wichtigste.

---

## Literatur

- Algorithm Watch und Bertelsmann Stiftung. 2019. *Automating society. Taking stock of automated decision-making in the EU*. [https://algorithmwatch.org/wp-content/uploads/2019/02/Automating\\_Society\\_Report\\_2019.pdf](https://algorithmwatch.org/wp-content/uploads/2019/02/Automating_Society_Report_2019.pdf). Zugegriffen am 01.06.2019.
- American National Science Foundation. 2012. *Vision statement for a national network of social observatories*. <https://socialobservatories.org/vision>. Zugegriffen am 01.06.2019.
- Australian Government. 2013. *The Australian public service big data strategy. Improved understanding through enhanced data-analytics capability*. <https://www.finance.gov.au/sites/default/files/Big-Data-Strategy.pdf>. Zugegriffen am 01.06.2019.
- Dencik, Lina, Arne Hintz, Joanna Redden, und Harry Warne. 2018. *Data scores as governance. Investigating uses of citizen scoring in public services*. Project report. <https://datajustice.files.wordpress.com/2018/12/data-scores-as-governance-project-report2.pdf>. Zugegriffen am 01.06.2019.
- Ford, Richard T. 2000. Save the robots. Cyber profiling and your so-called life. *Stanford Law Review* 52(5): 1573–1584.
- Government Digital Service. 2017. *Open policy making toolkit*. <https://www.gov.uk/guidance/open-policy-making-toolkit/getting-started-with-open-policy-making>. Zugegriffen am 01.06.2019.

- Gromm , Francisca. 2018. Is facebook the future of the national census? *The Conversation*, 11.07.2018. <https://theconversation.com/is-facebook-the-future-of-the-national-census-97018>. Zugegriffen am 01.06.2019.
- Hartl, Tobias, Christian Hutter, und Enzo Weber. 2018. Big Data bei der BA. Neue Erkenntnisse zum Suchverhalten am Arbeitsmarkt. *IAB-Forum*, 29.05.2018. <https://www.iab-forum.de/big-data-bei-der-ba-neue-erkenntnisse-zum-suchverhalten-am-arbeitsmarkt>. Zugegriffen am 01.06.2019.
- Karpf, David. 2016. *Analytic activism. Digital listening and the new political strategy*. New York: Oxford University Press.
- Kelty, Christopher M. 2017. Too much democracy in all the wrong places. Toward a grammar of participation. *Current Anthropology* 58(15): 77–90. <https://doi.org/10.1086/688705>.
- Kreiss, Daniel. 2016. *Prototype politics. Technology-intensive campaigning and the data of democracy*. New York: Oxford University Press.
- Pitkin, Hanna F. 1967. *The concept of representation*. Berkeley: University of California Press.
- Tactical Tech. 2019. *Personal data. Political persuasion. Inside the influence industry. How it works*. [https://ourdataourselves.tacticaltech.org/media/Personal-Data-Political-Persuasion-How-it-works\\_print-friendly.pdf](https://ourdataourselves.tacticaltech.org/media/Personal-Data-Political-Persuasion-How-it-works_print-friendly.pdf). Zugegriffen am 01.06.2019.
- The Carter Center. 2017. *Syria conflict resolution*. [https://www.cartercenter.org/peace/conflict\\_resolution/syria-conflict-resolution.html](https://www.cartercenter.org/peace/conflict_resolution/syria-conflict-resolution.html). Zugegriffen am 01.06.2019.
- Ulbricht, Lena. 2019. Scraping the demos. Digitalization, opinion mining and the democratic project. In *Democratization* 26 [Special Issue: Democratization beyond the Post-Democratic Turn], i. E.



---

# Digitale Geodaten

Lars Bernard und Stephan Mäs

## Inhalt

1 Klärung des Begriffs .....	102
2 Theoretische Grundlagen .....	102
3 Praktische Anwendung .....	103
4 Umsetzungsstand und Auswirkungen .....	105
5 Perspektiven für Staat und Verwaltung .....	109
Literatur .....	110

---

## Zusammenfassung

Geodaten sind Grundlage vieler Verwaltungsanwendungen. Standardisierungen und Regelungen zielen auf eine einfache Nutzung von digitalen Geodaten aus unterschiedlichen Quellen. Über Geodateninfrastrukturen werden digitale Geodaten publiziert, ausgetauscht und in Form von *web*-basierten Informationsdiensten zur direkten Nutzung durch Dritte bereitgestellt. Heute sind in dieser Form viele Geodaten verfügbar und werden beispielsweise im Rahmen von behördlichen Informationssystemen und Planungsverfahren für elektronisches Regieren und Verwalten genutzt. Aktuelle Entwicklungen zur Bereitstellung und Nutzung hochaktueller Beobachtungsdaten aus *online*-Sensorsystemen, zum Aufbau digitaler Stadtmodelle und der automatisierten Datenintegration und -analyse zeigen das Potenzial für die verbesserte Inwertsetzung dieser Daten etwa für das urbane Ressourcenmanagement.

---

L. Bernard (✉)

Professur für Geoinformationssysteme, TU Dresden, Dresden, Deutschland

E-Mail: [Lars.Bernard@tu-dresden.de](mailto:Lars.Bernard@tu-dresden.de)

S. Mäs

TU Dresden, Dresden, Deutschland

E-Mail: [stephan.maes@tu-dresden.de](mailto:stephan.maes@tu-dresden.de)

**Schlüsselwörter**

Geodateninfrastrukturen · Geoinformation · Geoinformationssysteme ·  
INSPIRE · GDI-DE

---

**1 Klärung des Begriffs**

*Digitale Geodaten* beschreiben *Geoobjekte* mit ihrem Raum- und Zeitbezug sowie in ihren thematischen Eigenschaften und ihrer Dynamik. *Geoobjekte* dienen als Abstraktionen von in der Welt beobachtbaren Phänomenen oder Objekten. So können Geoobjekte diskret und recht exakt geometrisch erfassbar sein, z. B. ein Flurstück, ein Gebäude oder auch ein Baum. Sie können bezüglich ihrer Eigenschaften dynamisch oder statisch sein: Ein Geoobjekt Fahrzeug ist bezüglich seiner Geometrie – die die aktuelle Fahrzeugposition abbildet – dynamisch; ein Gebäude in der Regel statisch. Geoobjekte können auch räumlich kontinuierlich verlaufende Umweltpfänomene präsentieren, etwa ein Temperaturfeld oder den Geländeverlauf. Diese Felder können dann im Sinne einer Funktion von Raum – und bei Betrachtung der Dynamik auch der Zeit – für jeden beliebigen Orts- und ggf. Zeitpunkt ausgewertet werden, also etwa zur Ermittlung der jeweiligen Temperatur bzw. Geländehöhe. Geoobjekte können zusammengefasst werden und bilden als Aggregat wiederum ein Geoobjekt: Viele Geoobjekte der Objektklasse Straße bilden beispielsweise ein Geoobjekt Straßennetz. Die Geometrien von Geoobjekten können im zwei- oder dreidimensionalen Raum durch Geokoordinaten beschrieben werden. Etablierte internationale Regelungen zu einheitlichen Raumbezugssystemen stellen dabei sicher, dass die Geokoordinaten eindeutig verortet werden können und sich Geodaten aus unterschiedlichen Quellen geometrisch zusammenführen lassen.

**2 Theoretische Grundlagen**

Geodaten sind traditionell eine wesentliche Grundlage für viele Bereiche des Verwaltungshandelns. Prominentes Beispiel ist hier das seit Beginn des 19. Jahrhunderts in der preußischen bzw. deutschen Verwaltung etablierte Kataster mit der Flur- oder Liegenschaftskarte, die in Verbindung mit dem Liegenschaftsbuch Auskunft zu Grenzverläufen und Eigentumsverhältnissen von Grundstücken liefert. Die klassischerweise für Verwaltungsprozesse eingesetzte analoge *Karte* wird seit Mitte des vorigen Jahrhunderts zunehmend durch die Verwendung digitaler Karten und heute auch immer mehr durch die direkte Verwendung digitaler Geodaten in Verwaltungsanwendungen und der Einbindung einzelner Werte dieser Geodaten (z. B. Flächengrößen, Nutzungsart, Schutzstatus etc.) ersetzt. Die Erfassung, Verwaltung und Analyse von Geodaten erfolgt heute in der Regel vollständig digital. Die Verwaltung und Bearbeitung von Geodaten erfolgt unter Einsatz von *Geoinformationssystemen (GIS)*. Diese Systeme bieten spezielle Funktionalitäten zur Einbindung und Verknüpfung von (Geo-)Daten unterschiedlicher Quellen, zum Geodatenmanagement,

zur Analyse der geometrischen und thematischen Eigenschaften der abgebildeten Geoobjekte sowie zur kartografischen Darstellung oder auch zur Publikation von Datensätzen im Internet. Genutzt werden in der Praxis sowohl kommerzielle als auch frei verfügbare und *Open Source*-Systeme, die als Systeme mit offenen Programmcode zur Verfügung stehen und weiterentwickelt werden können (Bill 2016).

Bei den Datenstrukturen zur Abbildung von Geoobjekten werden heute üblicherweise *Vektordaten* und *Rasterdaten* unterschieden. In Vektordaten werden die Geometrien der Geoobjekte durch Koordinaten als Punkte, Linienzüge oder Polygone im 2D- oder 3D-Raum bzw. als Solide oder Grenzflächenkörper im 3D-Raum repräsentiert. Derzeit überwiegen dabei die Repräsentationen im 2D-Raum. Diese Geometrien werden dann als Vektordaten mit den thematischen Beschreibungen als Sachdaten der Geoobjekte (etwa Flurstücknummer und Eigentümer für das Polygon eines Grundstücks) verknüpft. Die Vektorgeometrien können so auch mit Zeitstempeln verknüpft sein, etwa um die Gültigkeitsdauer einer Grenzlinie zu beschreiben.

In Rasterdaten wird der 2D-Raum typischerweise in einem regelmäßigen Gitter aus rechteckigen oder quadratischen Zellen abgebildet. Den einzelnen Zellen werden die thematischen Eigenschaften für die betrachteten Geoobjekte zugeordnet: Etwa die Niederschlagsmenge oder die mittlere bodennahe Lufttemperatur in einer Gitterzelle für die Darstellung eines Niederschlags- oder Temperaturfeldes. Analog kann einer Zelle auch ein nominaler Wert „Wald“ zur Darstellung der für diese Zelle vorherrschenden Landbedeckung zugewiesen werden.

Diskrete Geoobjekte eignen sich gut für die Darstellung im Vektormodell: Die Geometrien dieser Objekte können so möglichst exakt beschrieben werden. Kontinuierliche, feldhafte Phänomene werden meist in Rasterdaten repräsentiert. Numerische Berechnungen und Analysen lassen sich einfacher auf Grundlage von Rasterdaten durchführen. Auch die Art der Geodatenerfassung bestimmt über die Geodatenstruktur: Globale Positionierungssysteme und geodätische Messverfahren liefern Punktkoordinaten, die am Besten in Vektordaten abgebildet werden. Für Katasteranwendungen werden so geometrische Genauigkeiten im Zentimeterbereich erreicht. Die Erfassung von Geodaten mit der flugzeug- oder satellitengestützten Fernerkundung liefert die Beobachtungen als digitale Bilder direkt in einer Rasterdatenstruktur. Wie für digitale Bilder bestimmt sich die geometrische Genauigkeit von Rasterdaten durch die Auflösung der Erdoberfläche in Rasterzellen, wobei eine höhere geometrische Auflösung auch immer einen größeren Bedarf an Speicherplatz bedeutet. Heutige *Geoinformationssysteme (GIS)* erlauben den Wechsel von der Vektor- in die Rasterdarstellung und umgekehrt zur Unterstützung der unterschiedlichen Analyseverfahren.

---

### 3 Praktische Anwendung

Heute führen unterschiedliche Stellen in der Verwaltung (amtliche) Geodaten. Zu den Kataster- und Vermessungsämtern – die traditionell Geodaten als Grundlagen der Kataster und der topografischen Karten führen – sind zahlreiche Ämter und Behörden etwa aus den Bereichen Bau und Planung, Naturschutz und Umwelt,

Verkehr, Gewässer und amtliche Statistik getreten, die ebenfalls mit solchen Daten arbeiten. Seit jeher sind Nutzer von amtlichen Geodaten nicht nur die Verwaltungen selbst, sondern auch vielfältige andere öffentliche und wirtschaftliche Einrichtungen in ganz unterschiedlichen Bereichen (z. B. Militär, Raum- und Umweltplanung, Telekommunikation, Ver- und Entsorgung, Logistik und Verkehr, Versicherung, Immobilienwirtschaft). Die Geodaten in der Verwaltung erfüllen daher zum einen häufig eine Querschnittsfunktion und bilden eine wichtige Referenz (*Geobasisdaten*) zur Zusammenführung unterschiedlicher fachlicher Aufgaben bzw. Aspekte. Zum anderen besteht eine große Nachfrage nach amtlichen Geodaten für ganz unterschiedliche Anwendungszwecke. Das *Bundesamt für Kartografie und Geodäsie (BKG)* integriert die in den Landesvermessungsämtern geführten Geobasisdaten der Länder als gemeinsame deutschlandweite Datenbasis und koordiniert die Arbeiten zur Entwicklung und zum Betrieb der *Geodateninfrastruktur Deutschland (GDI-DE)*. Diese internet-basierte Infrastruktur erlaubt Behörden, Wirtschaft, Wissenschaft und Bürgern die gemeinsame Nutzung von Geodaten und Geoinformationsanwendungen.

Im Bereich der Bürgerinformation gibt es zahlreiche von Kommunen oder Landesbehörden betriebene Onlineangebote: Diese stellen etwa digitale Stadtpläne, Luftbilder, historische Karten oder spezifische Pläne zu verschiedenen Themen wie Bodenrichtwerte, Hochwasser, Schadstoffbelastung oder Verkehr bereit. Typische Beispiele sind die *web*-basierten Stadtpläne Dresden oder Berlin. Diese *Browser*-Anwendungen bieten typischerweise interaktive Visualisierungen mit einer Hintergrundkarte über die die jeweils ausgewählten Themen als Kartenebene (oft über *Web Map Service [WMS]* bereitgestellt) gelegt werden. Zu den in der Karte gezeigten Objekten können meist auch zusätzliche, textbasierte Informationen abgefragt werden. Teilweise finden sich hier auch bereits Integrationsansätze mit anderen Behördenanwendungen im Sinne eines *E-Government*: Bei Auswahl des Themas Erdwärmesonden im Themenstadtplan Dresden erfolgt beispielsweise eine auf die Anforderungen des ausgewählten Standorts bezogene Weiterleitung zu den für eine Erdwärmebohrung notwendigen Beantragungen (siehe <https://stadtplan.dresden.de/>).

Auf Bundesebene bietet *Geoportal.de* einen zentralen Einstieg für die verteilt vorliegenden Angebote der GDI-DE. Dort können von Bund, Ländern und Kommunen bereitgestellte Geodaten exploriert und die angebotenen Geoinformationsdienste genutzt werden. Auch in Ländern und Kommunen finden sich zahlreiche *Geoportale*, die ebenfalls einen Zugriff auf die jeweiligen Informationsangebote erlauben.

Ein Beispiel behördlicher Geodaten, die in Echtzeit bereitgestellt werden, liefert *PEGELONLINE* – das Gewässerkundliche Informationssystem der Wasserstraßen- und Schifffahrtsverwaltung des Bundes. Hier werden über verschiedene Webdienste aktuelle Messdaten als Zeitreihen unterschiedlicher Gewässerparameter und speziell der Pegelmessungen bereitgestellt. Genutzt werden diese Daten beispielsweise im Länderübergreifenden Hochwasserportal, das die aktuellen Wasserstände im Bundesgebiet und einiger Nachbarstaaten aus den jeweiligen behördlichen Portalen zur Darstellung der aktuellen Hochwasserlage zusammenführt. Die Daten werden zusätzlich auch über die mobile Anwendung „Meine Pegel“ angeboten und die Nutzer können auf den eigenen Bedarf ausgerichtete Benachrichtigungen konfigurieren

(Siehe <https://www.hochwasserzentralen.de/> und <https://www.pegelonline.wsv.de/>). So sind nicht nur Warnungen vor lokalen Hochwässern möglich, sondern es erschließen sich auch andere Anwendungen: Kanuten nutzen diese App zum Beispiel, indem sie Schwellwerte für die Wasserstände der kleineren Flüsse festlegen, so dass sie automatisch benachrichtigt werden, wenn die aktuellen Pegelstände eine Befahrung dieser Flüsse zulassen.

---

## 4 Umsetzungsstand und Auswirkungen

Bisherige Aktivitäten zur Digitalisierung im Kontext von behördlichen Geodaten können chronologisch grob durch folgende, sich überlappende Phasen charakterisiert werden:

- (1) *Von analogen Karten zu digitalen Geodaten:* In den 1970er-Jahren finden sich erste Ansätze zur Erstellung von digitalen Karten als Vorstufe zur Erzeugung und Verwaltung digitaler Geodaten, die dann zunehmend in vollständig digitalen Arbeitsflüssen erhoben und verarbeitet werden. Neben der traditionell visuellen Analyse und Berechnung in der Karte tritt verstärkt die automatisierte, numerische Analyse der geometrischen und thematischen Attributwerte der digitalen Geodaten (*Spatial Analysis*) in GIS.
- (2) *Entwicklung gemeinsamer einheitlicher Geodatenmodelle und interoperabler GIS:* Seit den 1980er-Jahren befasst sich die *Arbeitsgemeinschaft Vermessungsverwaltung der Länder der Bundesrepublik Deutschland (AdV)* mit der Entwicklung gemeinsamer Datenmodelle, um bundesweit harmonisierte und integrierbare Geobasisdatenbestände aufzubauen. Heute bildet das sogenannte *AAA®-Modell* die Grundlage für das Amtliche Topographisch-Kartographische Informationssystem (*ATKIS®*), das Amtliche Liegenschaftskatasterinformationssystem (*ALKIS®*) und das Amtliche Festpunktinformationssystem (*AFIS®*) in Deutschland. Es basiert auf internationalen Standards (Tab. 1) und dient den Bundesländern als einheitliches Datenmodell zur Beschreibung der Geoobjekte der amtlichen Liegenschafts- und Topografieinformationen als Grundlage für den Datenaustausch zwischen unterschiedlichen Systemen (Kummer et al. 2014). 1994 wurde das *Open Geospatial Consortium (OGC)* als gemeinnütziges Konsortium zur Entwicklung von offenen, internationalen Industriestandards gegründet. Hauptziel des OGC ist es, *Interoperabilität* für Geodaten und zwischen GIS zu schaffen. Inzwischen wurden durch das OGC zahlreiche Standards (sog. *Spezifikationen*) für Geodatenformate und Geoinformationsdienste entworfen. Die Kooperation zwischen dem OGC und der internationalen Standardisierungsorganisation ISO stellt sicher, dass OGC-Spezifikationen auch in die entsprechende ISO 19100er Normenserie übernommen werden, die heute auch Grundlage des *AAA®-Modells* sind.

Speziell die OGC-Spezifikationen für interoperable, web-basierte Geoinformationsdienste haben sich heute international etabliert. Prominentestes Beispiel sind hier die Schnittstellenbeschreibungen des OGC *Web Map Services (WMS)*. Eine WMS-Implementierung erlaubt es mittels einfach zu realisierender *Web-*

**Tab. 1** Einige Standards für Geodaten und Geoinformationsdienste

<b>Geo-Metadaten</b>		
<b>ISO 19115</b>	Metadata – Fundamentals	Beschreibung geografischen Informationsressourcen (Geodaten, Geoinformationsdienste und -anwendungen)
<b>ISO 19139</b>	Metadata – XML schema implementation	XML Schema für Metadaten abgeleitet aus ISO 19115
<b>Geodaten</b>		
<b>GML/ISO 19136</b>	Geography Markup Language	XML-basierte Auszeichnungssprache für räumliche Objektdaten, definiert u. a. die Beschreibung Objekten mit deren Geometrien und Attributen sowie Maßeinheiten und räumlichen Referenzsystemen und bildet damit die Grundlage für die Definition von Anwendungsschemata
<b>CityGML</b>	GML Anwendungsschema	XML-basierte Auszeichnungssprache für den Austausch und die Speicherung von virtuellen 3D Stadtmodellen
<b>INSPIRE Data Specifications</b>	Überwiegend GML basierte Anwendungsschemata	Harmonisierte Geodatenmodelle für 34 Datenthemen der Umweltberichterstattung als Teil der INSPIRE Gesetzgebung
<b>KML</b>	Keyhole Markup Language	XML basiertes Format für Geodaten in Raster- und Vektorform
<b>GeoTIFF</b>	Georeferenziertes TIFF	TIFF basiertes, georeferenziertes Rasterdatenformat
<b>Shape</b>	ESRI Shapefile	Von der Firma ESRI entwickelter <i>de facto</i> Standard für vektorbasierte Geodaten
<b>XPlanung</b>	GML Anwendungsschema	GML basiertes Austauschformat für Bauleit- und Raumordnungspläne
<b>Webbasierte Geoinformationsdienste</b>		
<b>OpenGIS CSW</b>	Catalog Service for the Web	Katalogdienst zur Suche auf Metadaten
<b>OpenGIS WCS</b>	Web Coverage Service	Dienst zum Bereitstellen und Abfrage von rasterbasierten Geodaten (z. B. Fernerkundungsdaten, Höhenmodelle, zeitvarianten 3D Klimadaten)
<b>OpenGIS WFS /ISO 19142</b>	Web Feature Service,	Dienst zum Bereitstellen und Abfrage von vektorbasierten Geoobjekt-Daten
<b>OpenGIS WMS /ISO 19128</b>	Web Map Service	Dienst zur Bereitstellung und Zusammenführung von Kartensvisualisierungen
<b>OpenGIS WPS</b>	Web Processing Service	Dienst zum Bereitstellen von (Geo-) Prozessierungsfunktionalität (z. B. räumliche Analysen, Interpolationen, Simulationen)

*browser*-Anwendungen, thematische Karten aus unterschiedlichen Quellen – die durch unterschiedliche, verteilte *Server* bereitgestellt werden – zu kombinieren und interaktiv zu nutzen.

Weitere Standards beschreiben die Schnittstellen von *Katalogdiensten* für die Suche nach Geodaten und Geoinformationsdiensten, *Zugriffsdiensten* für die verteilte Abfrage von Vektor- und Rasterdaten, *Sensordiensten* für den Zugriff auf Zeitreihendaten aus Umweltsensoren (z. B. Fernerkundungssatelliten, Flusspegel, Wetterstationen etc.) sowie für die interoperable Bereitstellung von *Geoprozessierungsdiensten* für die räumliche Analyse.

Im Vergleich zu GIS mit dem Fokus der Analyse von in Geodaten erfassten Beobachtungen und Messungen dienen die technisch verwandten Systeme für CAD (*Computer Aided Design*) überwiegend zur Erzeugung von Entwurfs- und Planungsunterlagen. Der Schwerpunkt von CAD liegt also auf Konstruktion und Entwurf von 2D- und oft auch 3D-Objekten, die als 3D-Vektordaten repräsentiert werden. Die Weiterentwicklung der Funktionalitäten in beiden Systemwelten macht die Unterscheidung jedoch heute schwieriger und gemeinsame, standardisierte Austauschformate erleichtern den Wechsel zwischen den Systemen: CityGML ist die unter Nutzung des aus der GIS-Welt stammenden Standards GML (*Geographic Markup Language*) und der im CAD-Bereich verwendeten *Industry Foundation Classes* (IFC) entwickelte Datenauszeichnungssprache, die heute als Standard für den Austausch von virtuellen 3D-Stadt- und Gebäudemodellen genutzt wird. XPlanung ist ein auf der GML basierendes Datenaustauschformat für raumbezogene Planungsdaten, wie beispielsweise Bauleitpläne oder Raumordnungspläne. Es wurde im Oktober 2017 durch den IT-Planungsrat als verbindlicher nationaler IT-Standard festgelegt. Damit sollen der Datenaustausch zwischen den verschiedenen Planungsakteuren und Planungsebenen vereinheitlicht, Planungsvorgänge effektiver gestaltet und Kosten gespart werden.

- (3) *Geodateninfrastrukturen für den (einfacheren) breiten Datenaustausch und -zugriff:* Parallel zu den skizzierten Entwicklungen interoperabler GIS wurde seit den 1990er-Jahren international und von Beginn auch national in zahlreichen Kooperationen der deutschen Verwaltungen mit der Geoinformatik-Wissenschaft und -Wirtschaft mit dem Aufbau von Geodateninfrastrukturen (*GDI*) begonnen. Grundsätzliche Ziele des Aufbaus von GDI sind die bessere Inwertsetzung der erfassten und verwalteten Geodaten, ihr verbesserter Austausch und die gleichzeitige Vermeidung von unnötigen Dopplungen in beispielsweise der Geodatenerfassung und -management. Eine GDI sollte sowohl ihren aus unterschiedlichen Bereichen stammenden Nutzern transparente, verlässliche, gut recherchierbare sowie problemlos kombinier- und nutzbare Geoinformationsinhalte anbieten als auch den Anbietern von Geodaten einfache Wege zur Bereitstellung dieser Daten und darauf aufsetzender Geoinformationsdienste ermöglichen. Aufbau und Betrieb einer GDI sind typischerweise eine Querschnittsaufgabe und die erfolgreiche Etablierung einer GDI stellt mit ihren

komplexen Zielstellungen und Anforderungen eine erhebliche Herausforderung für die Verwaltung dar (Bernard et al. 2019).

Die 2007 verabschiedete EU-Richtlinie Initiative *Infrastructure for Spatial Information in Europe* (INSPIRE) und deren Umsetzung in die deutschen Geodatenzugangsgesetze auf Bundes- und Länderebene bildet heute den gesetzlichen Auftrag zum Aufbau behördlicher GDI in Europa. Die INSPIRE-Gesetzgebung adressiert die in einer GDI bereitzustellenden Komponenten, die Interoperabilitäts- und Leistungsfähigkeitsforderungen sowie die Zeitpläne für eine konsolidierte GDI-Entwicklung. Die Direktive benennt 34 Themen, die sich an den Anforderungen der Umweltberichterstattung orientieren und für die – europaweit – harmonisierte Geodatenmodelle entwickelt wurden. Diese sollen die Grundlage für die Publikation von leicht zu kombinierenden amtlichen Geodaten sein. Sie werden über internetbasierte Dienste zur Recherche, zur Darstellung als interaktive Karte und zum Datenzugriff für Dritte bereitgestellt. Die Beschreibung der Geodaten und Geoinformationsdienste mittels standardisierter Metadaten soll GDI-Nutzern nicht nur die Datensuche in Portalanwendungen ermöglichen, sondern auch Hilfestellung zur Bewertung der Nutzbarkeit der gefundenen Daten und Dienste geben.

2003 wurde durch die Chefs des Bundeskanzleramts und der Staats- und Senatskanzleien der Länder der Aufbau der GDI-DE als ein Bestandteil der Entwicklungen für ein deutsches *E-Government* initiiert und 2005 wurde für den Aufbau der GDI-DE das mit Bund- und Ländervertretern besetzte Lenkungsgremium eingerichtet. Die am BKG eingerichtete Koordinierungsstelle ist seit 2007 auch die nationale Anlaufstelle für die INSPIRE-Umsetzung in Deutschland. Ebenfalls am BKG werden die zentralen Komponenten der GDI-DE betrieben, beispielsweise Geoportal.de als Einstiegspunkt für Recherchen. Mit der Umsetzung des 2009 in Kraft getretenen Artikels 91c des Grundgesetzes zur Bund-Länder-Zusammenarbeit in der Informationstechnologie wird die GDI-DE seit 2010 vom IT-Planungsrat gesteuert. 2016 hat das Lenkungsgremium GDI-DE die Umsetzung der Nationalen Geoinformations-Strategie (NGIS) beschlossen, die im Kern auf die Bereitstellung von für alle Nutzer leicht zugänglichen Geoinformationen und die Entwicklung von durch Nutzerinteressen getriebene (amtliche) Geoinformationsangebote zielt.

- (4) *Verstärkte Bereitstellung von offenen und frei verfügbaren Geodaten:* Die Umsetzung von INSPIRE hat wesentliche Impulse für die umfassende Bereitstellung amtlicher Geodaten gesetzt. Immer häufiger werden behördliche Geodaten in Europa dabei als *Open Data* veröffentlicht – mit dem Ziel, die Inwertsetzung dieser Daten etwa zur Umweltinformation, in der Umwelt- und Raumplanung, aber auch für Anwendungen in der Wirtschaft zu fördern. Auch das 2012 reformierte Geodatenzugangsgesetz (GeoZG) des Bundes fordert, Geodaten und aufsetzende Informationsdienste des Bundes grundsätzlich kostenfrei bereit zu stellen. So stehen beispielsweise die Daten des Deutschen Wetterdienstes (DWD) als offene Daten zur Verfügung. Solche Regelungen etablieren verstärkt auch die Länder und es finden sich immer mehr amtliche

Geodaten, die kostenfrei zur Verfügung stehen. Im deutschen GOVDATA-Portal machen Geodaten bereits einen sehr großen Anteil des Angebots aus. Es fehlt derzeit jedoch an einer vollständigen, idealerweise lizenzrechtlich harmonisierten Durchsetzung von *Open Data* für die Geodaten aller Länder und aller Kommunen. Aktuell ist daher der Zugriff auf kommunale Geodaten oder die Zusammenführung von Geodaten der Länder auf der Bundesebene als freie Angebote noch vielfach schwierig oder gar nicht möglich.

---

## 5 Perspektiven für Staat und Verwaltung

Auch wenn die Digitalisierung amtlicher Geodaten weit vorangeschritten ist und ihre Verfügbarkeit in der vergangenen Dekade erheblich gesteigert werden konnte, bleiben zahlreiche Herausforderungen für künftige Entwicklungen. So finden sich bis dato immer noch wenige (durchgängige) *E-Government*-Anwendungen, die Geodaten oder Geoinformationsdienste nahtlos in administrative Prozesse integrieren. Hier gilt es, diese Möglichkeiten weiter zu verbessern und dabei Aspekte wie gemeinsame Lizenzierteilsregeln, Sicherheitsstandards für kritische Informationen und insbesondere auf die Anwendungsbedarfe angepasste, aber nicht zu komplexe Geodatenangebote weiter zu entwickeln. Diese Bedarfe sind an verschiedenen Stellen erkannt. So hat eine EU-Analyse zur Umsetzung der INSPIRE-Direktive (Europäische Kommission 2016) als wesentliche Probleme die uneinheitlichen Zugriffsregelungen und den Mangel an Anwendungen ausgemacht, die INSPIRE nutzen (können). Als eine Konsequenz soll die weitere Umsetzung stärker auf die Harmonisierung und EU-weite Zusammenführung von Geodaten für das Umwelt-*Reporting* der EU-Mitgliedsstaaten fokussiert werden.

Mit dem Erdbeobachtungsprogramm Copernicus der Europäischen Union und weiteren neuen Erfassungsmethoden und Sensortechniken stehen Datenquellen bereit, die das Potenzial haben, sowohl kürzere Datenaktualisierungszyklen für amtliche Geodaten zu realisieren als auch Umweltänderungen in Form von zeitvarianten Geodaten abzubilden und etwa für unterschiedliche Monitoring- und Planungsanwendungen zur Verfügung zu stellen. Hier gilt es, sowohl geeignete Konzepte für die Modellierung und idealerweise voll automatisierten Erfassung solcher Veränderungen in zeitvarianten Geodaten unter Nutzung der neu verfügbaren Sensortechnologien zu entwickeln als auch Ansätze zur Versionierung und Archivierung von (historischen) Geodaten weiterzuentwickeln und diese für operationelle Anwendungen zu ertüchtigen. Gerade im Kontext von *Smart Cities* haben diese Entwicklungen erhebliche Bedeutung als Datengrundlage für das Monitoring einer Stadt und als Entscheidungsbasis, um *smart*e Infrastrukturen für Energie, Wasser, Verkehr etc. zu realisieren.

Zukünftige Entwicklungen müssen auch Lösungen dazu bereitstellen, wie die Verwaltung eigene, amtliche Geodaten mit den durch kommerzielle Anbieter (*Google* etc.) oder im Rahmen freiwilliger Initiativen (*Open Street Map* etc.) erfassten Geodaten und bereitgestellten Geoinformationsdienste sinnvoll kombiniert.

## Literatur

- Bernard, Lars, Johannes Brauner, Stephan Mäs, und Stefan Wiemann. 2019. Geodateninfrastrukturen. In *Geoinformatik*, Hrsg. Monika Sester, 91–122. Berlin: Springer.
- Bill, Ralf. 2016. *Grundlagen der Geoinformationssysteme*, 6. Aufl. Berlin: Wichmann.
- Europäische Kommission. 2016. *Bericht der Kommission an den Rat und das Europäische Parlament über die Durchführung der Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14.03.2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE)*. [https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52016DC0478R\(01\)](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52016DC0478R(01)).
- Kummer, Klaus, Theo Kötter, und Andreas Eichhorn, Hrsg. 2014. *Das deutsche Vermessungs- und Geoinformationswesen 2015*. Berlin: Wichmann.



---

# Agent-based Modeling und Politikberatung

Florian Eyert

## Inhalt

1 Klärung des Begriffs .....	112
2 Theoretische Grundlagen .....	113
3 Praktische Anwendung .....	115
4 Umsetzungsstand und Auswirkungen .....	118
5 Perspektiven für Staat und Verwaltung .....	119
Literatur .....	121

---

## Zusammenfassung

Die Computersimulationsmethode der agentenbasierten Modellierung ist ein neuartiges Analyseinstrument, das vermehrt auch in der Beratung politischen Handelns eingesetzt wird und sich durch seinen Umgang mit Komplexität, seine Experimentalität und seinen Formalitätsgrad auszeichnet. In der praktischen Anwendung, etwa in der Gestaltung von Infrastruktur-, Gesundheits- oder Wirtschaftssystemen, befindet es sich in einem Spannungsfeld zwischen wissenschaftlicher Problemlösung und politischer Legitimierung. Trotz Risiken und Begrenzungen kann in Zukunft mit einem vermehrten Einsatz gerechnet werden.

---

## Schlüsselwörter

Policy Modeling · Computational Social Science · Simulation · Evidenzbasierte Politik · Repräsentation

---

F. Eyert (✉)

Weizenbaum-Institut für die vernetzte Gesellschaft/Wissenschaftszentrum Berlin für Sozialforschung, Berlin, Deutschland

E-Mail: [florian.eyert@wzb.eu](mailto:florian.eyert@wzb.eu)

## 1 Klärung des Begriffs

Die computerbasierte Simulation sozialer Prozesse und ihre Verwendung als Instrument der Politikberatung ist ein noch junger, aber zunehmend bedeutender Ansatz. In seinem Zentrum steht das Paradigma der agentenbasierten Modellierung, oft mit dem englischen „agent-based modeling“ oder der Abkürzung „ABM“ bezeichnet. Hierbei handelt es sich im Kern um Computerprogramme, in denen die Akteure eines relevanten Gesellschaftsbereiches sowie ihre institutionelle Umgebung als Softwareelemente modelliert und anschließend in ihrer Interaktion dynamisch simuliert werden. Im Mittelpunkt stehen also nicht mathematische Gleichungen, sondern wechselwirkende Softwareelemente. Auf diese Weise soll versucht werden, schwer vorhersehbare gesellschaftliche Dynamiken zwischen einer Vielzahl heterogener Akteure nachzuverfolgen, auf ihre Tendenzen hin zu prüfen und im Idealfall besser zu verstehen.

Auf ein besseres Verständnis ist auch staatliches Handeln angewiesen, denn erst ein adäquates Bild gesellschaftlicher Prozesse erlaubt angemessene Regierungs- und Regulierungsstrategien. Derartige Bilder lassen sich als Modellierungen realer Phänomene fassen, also als spezifische Versuche, die Komplexität der Welt unter gewissen Gesichtspunkten zu reduzieren. Modellbildung – ob implizit oder explizit, formal oder informal – gestattet es politischen Akteuren, Handlungsfähigkeit und -orientierung zu entwickeln. Für die Beratung politischen Handelns bietet agentenbasierte Modellierung daher die Möglichkeit, kausal kohärente Weltbeschreibungen innerhalb eines informatisch-formalen Rahmens vorzunehmen, anhand derer potenzielle Auswirkungen von *Policy*-Entscheidungen untersucht und virtuelle Experimente mit variierenden Parametern durchgeführt werden können. So kann etwa dasselbe Problemfeld einmal mit und einmal ohne ein spezifisches Gesetz oder unter Verwendung verschiedener Regulierungsinstrumente simuliert und in seinem Verhalten verglichen werden. Insbesondere in Situationen, in denen riskante Reformen als Formen politisch-experimentellen Handelns aus finanziellen, zeitlichen oder ethischen Gründen nicht sinnvoll sind, ergibt sich so ein besonderer Vorzug. In diesem Sinne kann ABM als Teil eines evidenzbasierten Politikansatzes begriffen werden, mithilfe dessen Problemlagen reproduzierbar analysiert und anschließend begründet gestaltet werden können. Die dabei produzierte Evidenz beruht zwar nicht notwendigerweise auf empirischer Messung, allerdings aber auf kausaler Plausibilisierung. Aus politikwissenschaftlicher Sicht können derartige Modelle zudem als Legitimationsinstrumente politischen Handelns betrachtet werden, was die kritische Aufmerksamkeit sowohl auf die Stringenz und Transparenz der Modellierung als auch auf die Beratungskontexte lenkt. In den letzten Jahren kam es nicht zuletzt aufgrund verstärkter öffentlicher Förderung zu einer Zunahme explizit auf die Unterstützung politischer Entscheidungsfindung ausgerichteter Simulationsprojekte. Obgleich momentan noch stark in der wissenschaftlichen Forschung verankert, ist denkbar, dass ABM in Zukunft auch über die im engeren Sinne wissenschaftliche Politikberatung hinaus wirksam werden könnte. Die *Policy*-Modellierung durch agentenbasierte Computersimulation als Basis und Legitimation politischer Gestal-

tung bietet wertvolle Möglichkeiten für Staat und Verwaltung im digitalen Zeitalter, weist aber auch sachliche und normative Grenzen auf.

---

## 2 Theoretische Grundlagen

Simulationen spielen in der Geschichte der Politikberatung schon seit längerem eine Rolle, wie das klassische Beispiel der „Grenzen des Wachstums“ des *Club of Rome* von 1972 zeigt. Ziel des darin verwendeten *World3*-Modells war es, mithilfe der Simulation von Interdependenzen des Wirtschaftssystems und der Umwelt die Konsequenzen des Umgangs mit den begrenzten Ressourcen der Natur aufzuzeigen. Als Alternative zu derartigen, in den 1970er-Jahren typischen „System Dynamics“-Modellen, die soziale Systeme üblicherweise durch Aggregatvariablen wie Bevölkerungs- oder Produktionsraten und mithilfe von Differenz- oder Differenzialgleichungen modellieren, entwickelte sich in den 1990er-Jahren aus den informatischen Ansätzen der verteilten künstlichen Intelligenz und der Multiagentensysteme das Paradigma der agentenbasierten Modellierung.

In diesem Ansatz werden Akteure des relevanten Gesellschaftsbereiches als autonome, soziale, reaktive und pro-aktive Softwareagenten (Wooldridge und Jennings 1995) modelliert: Sie verhalten sich nach eigenen Maßstäben, in Interaktion mit anderen Agenten, in Reaktion auf ihre Umwelt und mit eigenem Antrieb. Realisiert werden Agenten dabei als Softwareobjekte mit internen Zustandsvariablen und durch Softwareprozeduren formalisierten Handlungsschemata. Zentral ist also zunächst die Mikrofundierung, durch die eine je kontextspezifisch angemessene Repräsentation von Akteuren und ihren Werten, Meinungen und Handlungsstrategien möglich ist und deren Wechselwirkung mit anderen Agenten, wie Organisationen und Staaten, und ihren Umwelten mittels Simulation begreifbar werden. In diesem Sinne zeichnen sich agentenbasierte Modelle durch ihre Sensitivität für *Bottom-Up*-Dynamiken aus und folgen häufig einem „generativen“ Paradigma (Epstein 2007), das die Frage in den Mittelpunkt stellt, wie gesellschaftliche Makrostrukturen aus den Interaktionen zwischen Agenten auf der Mikroebene erwachsen. Individuell und divers modellierbar, gehen letztere dabei bewusst über die in der Ökonomie verbreiteten, aber auch in der Politikwissenschaft oft implizierten „repräsentativen Agenten“ (Hartley 1997) hinaus. Simuliert werden können weiterhin sowohl abstrakt-hypothetische Prozesse als auch konkrete empirische Anwendungsfälle. In beiden Fällen lassen sich die im Laufe der Simulation entstehenden Daten anschließend mit statistischen Verfahren untersuchen.

Auf theoretischer Ebene können weiterhin drei Merkmale agentenbasierter Modellierung herausgegriffen werden, die für die Politikberatung besonders relevant sind.

a) *Komplexitätsbewältigung*: In der Debatte um die Rolle von Politikberatung wird oft die zunehmende Komplexität der durch die Politik zu treffenden Entscheidungen hervorgehoben. Allzu oft zeigen sich die Grenzen politischer Steuerbarkeit an unüberschaubaren gesellschaftlichen Dynamiken, Rückkopplungseffekten und

historischen Pfadabhängigkeiten. Parallel dazu haben in den letzten Jahren zahlreiche Beobachter\*innen den Zusammenhang zwischen Komplexität, *Governance* und *Public Policy* hervorgehoben und dabei politische Zusammenhänge als „komplexe adaptive Systeme“ (Duit und Galaz 2008) beschrieben, deren Dynamik durch lokale Interaktionen heterogener Akteure, emergente Prozesse, Selbstorganisation und nicht-lineare Entwicklungen geprägt ist. Wenn solche aus nicht-trivialen Interaktionen resultierenden Veränderungen der Elemente wiederum auf den Zustand des Systems zurückwirken, lassen sich Entwicklungen kaum mehr ohne die Hilfe von Computern erfassen. ABM gilt als elementares Analyseinstrument derartiger komplexer, zwischen Ordnung und Chaos verorteter Systeme (Bonabeau 2002).

*b) Experimentalität:* Experimente, insbesondere solche mit größeren Populationen, sind oftmals aus ethischen oder auch schlicht praktischen, wie etwa zeitlichen oder finanziellen, Gründen nicht oder allenfalls in der Form natürlicher Quasi-Experimente denkbar. Hier versprechen virtuelle Experimente mithilfe von Computersimulationen einen Lösungsansatz durch die Beobachtung „künstlicher Gesellschaften“. Was in der heutigen Digitalwirtschaft oft das A/B-Testing leisten soll, erlaubt hier die Variation von Parametern innerhalb der Simulationsmodelle, die sowohl ein ergebnisoffenes Erkunden als auch das Prüfen spezifischer *Treatment*-Effekte ermöglicht. Vertreter\*innen des Ansatzes der agentenbasierten Modellierung verweisen dabei oft auf den experimentellen Charakter einer jeden *Policy*-Entscheidung, deren Angemessenheit sich stets erst an den Folgen in der realen Welt und oft erst nach langer Zeit zeigt. Simulationen bieten zumindest einen teilweisen Ersatz, indem sich kausale Prozesse *ex ante* betrachten lassen. Dieser Zugang markiert insbesondere den Vorzug gegenüber anderen Formen quantitativer Evidenz: Statt kausale Effekte von Entscheidungen *ex post* und inferentiell zu suchen, werden angenommene soziale Mechanismen nachvollziehbar implementiert und in begrenztem Maße einer vorausschauenden Evaluierung zugänglich gemacht. Vor allem das strukturelle Problem der divergenten zeitlichen Orientierung von Wissenschaft und Politik erfährt eine Verschiebung dadurch, dass sozialwissenschaftliche Diagnosen sich nicht erst am realhistorischen Verlauf herausbilden müssen, sondern vielmehr dem kurzfristigeren Entscheidungsbedarf der Politik entgegenkommen können.

*c) Formalität:* Um im Rahmen eines Computermodells repräsentiert werden zu können, müssen soziale Prozesse hinreichend formal modelliert werden. Erst auf computerlesbare Weise abstrahiert lassen sie sich automatisiert simulieren und so in ihrer Dynamik analysieren. Die Formalisierung über Softwareagenten eröffnet dabei gleichzeitig wesentlich höhere Gestaltungsspielräume als dies bei analytisch oder auch numerisch lösbarren mathematischen Gleichungen der Fall ist. Agentenbasierte Modelle ermöglichen so einen Kompromiss zwischen der Eindeutigkeit mathematischer Modelle und der Ausdrucksvielfalt natürlicher Sprache. Während der Einsatz von ABM im privatwirtschaftlichen Bereich hauptsächlich auf effiziente Ergebnisse abzielt, tritt im öffentlichen Sektor und auch in der Politikberatung Legitimität als zentrale Kategorie hinzu. Ein angemessenes Abstraktionsniveau, Klarheit und Eindeutigkeit der Modelle erhalten daher eine besondere Bedeutung.

Politisches Handeln beruht mindestens implizit auf einem Modell, einem vereinfachten Bild des jeweils von Politik betroffenen Wirklichkeitsbereiches. Solche

„mentalen Modelle“ (Johnson-Laird 1983) von Regierungsakteuren können in diesem Sinne als Zielfläche der Bestrebungen von Beratungstätigkeiten seit Machiavelli bis hin zu den heutigen *Think Tanks* verstanden werden. Der Bezugspunkt von Politikberatung ist immer auch die Lesbarmachung der Gesellschaft. Agentenbasierte Modelle und Simulationen können daher als eine spezifische, durch Computertechnologien ermöglichte Form derartiger Welterschließung verstanden werden, denen stets ein konstruktivistisches Moment innewohnt. Indem sie gewisse Aspekte der Realität zugunsten anderer vernachlässigen, kommt ihnen selbst ein politischer Charakter und damit eine Doppelfunktion zu: als Strategien der sozialwissenschaftlichen Forschung und als Methoden der Legitimation politischen Handelns. Im Verhältnis zwischen Wissenschaft und Politik, zwischen technokratischen und dezisionistischen Formen der Politikberatung (Habermas 1969) befinden sich agentenbasierte Modelle als wissenschaftliche Analyse- und politische Legitimationsinstrumente an einer Grenzstelle, die deutlich macht, dass Fragen der wissenschaftlich-technischen Repräsentation eng verknüpft sind mit Fragen der politischen Repräsentation.

Auch hinsichtlich der Transparenz ergeben sich Ambivalenzen. Insbesondere für die Politikberatung befindet sich agentenbasierte Modellierung in einem Spannungsfeld zwischen dem Öffnen kausaler *Black Boxes* – im Sinne eines Explizitmachens von jedem Handeln ohnehin unterliegenden Modellen – und dem erneuten *Black-boxing* durch das Modell selbst. Denn die einzelnen Mechanismen, die sich im Laufe der Simulation vollziehen, können mitunter ein hohes Maß an faktischer Intransparenz aufweisen und so für den Einsatz in der gesellschaftlichen Praxis und die Legitimation politischen Handelns auf ähnliche Weise problematisch werden wie gewisse Methoden der künstlichen Intelligenz. Zudem bestehen politisch relevante methodische Probleme, wie etwa der als Äquifinalität bekannte Umstand, dass unterschiedliche Mechanismen dieselben Strukturen produzieren können. ABM kann daher immer nur Erklärungskandidaten liefern, deren Tragfähigkeit eine verantwortungsvolle Politikberatung sowie die Politik selbst bestimmen müssen. Die Gefahr der bewussten oder unbewussten Verschleierung derartiger Begrenzungen von Simulationsmodellen hat Bruce Edmonds jüngst als „post-truth drift“ (2017) herausgestellt. Die beschriebenen, dem Einsatz von ABM in der Politikberatung inhärenten Spannungen müssen – gemäß Habermas' drittem, dem pragmatischen Modell – in der Praxis verhandelt werden.

---

### 3 Praktische Anwendung

Unter dem Gesichtspunkt der praktischen Anwendung agentenbasierter Modelle ist zunächst klarzustellen, dass bei der Simulation gesellschaftlicher Prozesse, im Gegensatz etwa zur Wetteranalyse oder zum Maschinenentwurf, präzise Vorhersagen über zukünftige Systemzustände bis auf Extremfälle illusorisch bleiben. Praktische Anwendungen sind stattdessen vornehmlich durch die Abschätzung von generellen Tendenzen und ein verbessertes Verständnis für erklärende Mechanismen und komplexe Dynamiken motiviert. Mitunter wird auch das Aufzeigen von *Trade-Offs* und die „Disziplinierung“ von Debatten über Politikgestaltung durch rigorosere

Evidenzstandards zu den Zielen gezählt (Epstein 2008). In diesem Sinne kann agentenbasierte Modellierung in kritischen Entscheidungsszenarien zwar eine nachvollziehbare Basis für Handlungsempfehlungen bilden, ist aber zugleich nur in Kombination mit anderen Ansätzen und vor allem dem Sachverstand von Expert\*innen des Sachgebietes sinnvoll.

Politikberatung stellt sich heute als diverses Feld mit verschiedenen relevanten Akteuren dar, das sowohl durch privatwirtschaftlich verfasste professionelle Politikberatung als auch durch Lobbyismus und wissenschaftliche Beratung gekennzeichnet ist und unter anderem aus Universitäten, Forschungsinstituten, *Think Tanks*, Unternehmensberatungen, Expertenkommissionen, Stiftungen und Lobbyorganisationen besteht. Demgegenüber setzen sich die Akteure im Bereich agentenbasierter Modellierung in erster Linie aus Wissenschaftler\*innen in universitären und außeruniversitären Forschungseinrichtungen zusammen, die Expertise für politisches Handeln entweder angebotsorientiert über die Veröffentlichung eigenständiger Forschung oder auftragsorientiert entlang gezielt geförderter Projekte bereitstellen. Insbesondere im englischsprachigen Raum finden Sozialsimulationen Einsatz, wichtige Orte hierfür sind das *Centre for Research in Social Simulation* in Surrey (UK), das *Centre for Policy Modelling* in Manchester (UK) oder die zahlreichen Komplexitätsforschungszentren der USA, darunter das *Center for Social Complexity*, das *New England Complex Systems Institute* oder das berühmte *Santa Fe Institute*. Auch im kontinentaleuropäischen Kontext finden sich entsprechende Einrichtungen, etwa das niederländische *Groningen Center for Social Complexity Studies*. Darüber hinaus sind Institutionen wie die *European Social Simulation Association (ESSA)* oder das *Network for Computational Modeling in Social and Ecological Sciences (CoMSES)* an der Etablierung agentenbasierter Modellierung, auch als Bestandteil der Politikberatung, beteiligt.

Zu den politiknahen Anwendungsfeldern von ABM zählen unter anderem die folgenden Bereiche:

a) *Infrastruktur*: Zu den häufigen Einsatzgebieten agentenbasierter Modellierung gehören Infrastruktursysteme wie Energie oder Verkehr. Ziel ist es hier, die Auswirkungen politisch-gestalterischen Handelns in komplexen Entscheidungs- und Akteurszusammenhängen besser zu verstehen. Exemplarisch für den deutschsprachigen Raum lässt sich das *AMIRIS*-Projekt nennen, das das Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit zur Abwägung von Fördermechanismen bei der Marktintegration von Strom aus erneuerbaren Energien beriet. Das unter anderem durch das Deutsche Zentrum für Luft- und Raumfahrt umgesetzte agentenbasierte Modell wurde hier als „Tool zur Politikberatung“ (Reeg et al. 2013, S. 2) eingesetzt, um die Wirkung von Instrumenten wie der gleitenden Marktprämie zu eruieren. Zu den Resultaten der Simulation zählen eine Abschätzung der entstehenden Anreizstrukturen für verschiedene Markakteure durch die Marktprämie, die Identifikation der zentralen Profiteure ihrer Einführung sowie eine Einschätzung der Einsparungspotenziale beim Fördervolumen. Im BMBF-geförderten Projekt *SW-Agent* wurde ebenfalls ein Aspekt der Energiewende simuliert, in diesem Fall, um geeignete Strategien für Stadtwerke zu entwickeln. Auch im Bereich Verkehrspolitik werden agentenbasierte Modelle eingesetzt, um komplexe Dynamiken zwi-

schen heterogenen Verkehrsteilnehmer\*innen besser zu verstehen und Infrastrukturen geeignet zu gestalten.

b) *Gesundheit*: Ein weiterer prominenter Anwendungsbereich agentenbasierter Modellierung besteht in der Politikgestaltung im Bereich *Public Health*. Hierzu zählt etwa die Forschung zu Krankheitsepidemien, die die Verbreitung von Erregern in komplexen, teils globalen Netzwerken modelliert, um erfolgreiche Präventions- sowie Eindämmungsstrategien zu entwickeln. Im durch die EU-Kommission geförderten Projekt *TELL ME* wurde agentenbasierte Modellierung verwendet, um die Interaktionen zwischen Individuen während des Ausbruchs einer Epidemie zu beleuchten und geeignete öffentliche Kommunikationsstrategien zur Motivierung präventiven Handelns in der Bevölkerung und Vermeidung von Paniken zu entwickeln. Auch Modelle zu Nahrungsmittelsicherheit oder den Dynamiken exzessiven sozialen Alkoholkonsums betreffen die *Policy*-Gestaltung in diesem Bereich.

c) *Wirtschaft*: Insbesondere im Nachgang der globalen Finanz- und Wirtschaftskrise haben sich viele Expert\*innen für den Einsatz agentenbasierter Modelle als einer realistischeren Alternative zu den mathematisierten Modellen des ökonomischen Mainstreams ausgesprochen (beispielhaft Bookstaber 2017). Phänomene wie *Bottom-Up*-Dynamiken oder die „bounded rationality“ von Akteuren ließen sich auf diese Weise wirklichkeitsgetreuer formalisieren. In dieser Hinsicht sind Parallelen zu verhaltensökonomischen Ansätzen sichtbar und auch volkswirtschaftliche Annahmen wie die einer Tendenz zum Marktgleichgewicht lassen sich modelltechnisch kontingenzt halten, statt sie a priori vorauszusetzen. Zu den Beispielen im deutschsprachigen Raum zählt das *Eurace@Unibi*-Modell, das eine Makroökonomie modelliert, um einen einheitlichen Rahmen für wirtschaftspolitische Analysen zu ermöglichen und etwa Dynamiken des technologischen Wandels oder Effekte von Währungspolitik abzuschätzen.

Weiterhin sind konkrete Versuche zu erwähnen, den Einsatz von Computersimulationen für *Policy*-Modellierung und Politikberatung zu einem übergreifenden Ansatz zu entwickeln, von denen hier zwei im Rahmen des EU-Forschungsrahmenprogramms finanzierte Projekte exemplarisch genannt werden sollen. *Future Policy Modeling (FUPOL)* konzipierte ein neues *E-Government*-Modell des *Policy*-Gestaltungs- und Implementationszyklus und verband dabei automatisierte, webbasierte Themenanalyse, kommunikative Einbindung von Bürger\*innen und Computersimulationen. *Open Collaboration for Policy Modeling (OCOPOMO)* entwickelte eine *Software-Toolbox* für den Prozess der *Policy*-Gestaltung, in der agentenbasierte Modellierung mit anderen digitalen Methoden verbunden wurde. Zentral war hier die Erhöhung der Transparenz des Modellierungsprozesses sowie das Einbeziehen verschiedener *Stakeholder* und Expert\*innen. Gemeinsam ist beiden Projekten der Versuch, ABM als Teil eines auf *E-Government* basierenden *Policy*-Prozesses zu etablieren.

Der Erfolg des Einsatzes agentenbasierter Modelle im staatlichen Handeln hängt dabei auch von der Beschaffenheit des relevanten Problembereiches ab. Ihre Stärke liegt in Fällen, in denen die Entscheidungsmodelle der Akteure einem relativ gut verstandenen oder zumindest annäherungsweise formalisierbaren Schema folgen und sich die Komplexität der Situation primär aus den Interaktionen dieser Akteure

ergeben. In Fällen, in denen die Handlungsmuster der Akteure selbst schlecht verstanden sind oder etwa aufgrund der Bedeutung latenter Faktoren wie Kultur schwer modellierbar sind, können agentenbasierte Modellierungen weniger gut geeignet sein.

Schließlich seien einige grundlegende Anmerkungen zur technischen Umsetzung gemacht. Während sich im Prinzip jedes agentenbasierte Modell mit allen gängigen Programmiersprachen von Grund auf erstellen lässt, wird die Anwendung in der Praxis oft durch die zunehmende Verfügbarkeit von Entwicklungsumgebungen und Softwarebibliotheken wie *NetLogo*, *Repast*, *MASON*, *Ascape* und *Mesa* erleichtert. Oftmals sind diese dabei auf objektorientierte Programmiersprachen wie *Java* oder *C++* ausgelegt, deren Ontologie der aus Zuständen und Prozeduren bestehenden Entitäten für die agentenbasierte Modellierung einen besonders natürlichen Zugang darstellt. Zudem fördern erste Standardisierungsversuche die Interoperabilität und Reproduzierbarkeit. Der gegenwärtig verbreitete *ODD*-Standard (Grimm et al. 2006) etwa strebt ein einheitliches Protokoll für die Beschreibung von Simulationsmodellen an, in dem ein Überblick (Zweck, Statusvariablen und Skalen sowie Prozessüberblick und *Scheduling*), Informationen zu Design-Konzepten und weitere Details (Initialisierung des Modells, *Input* und Submodelle) enthalten sind. Derartige Protokolle könnten in der Zukunft zu einer stärkeren Vergleichbarkeit und Nachvollziehbarkeit von agentenbasierten Modellen auch in der Politikberatung beitragen.

---

## 4 Umsetzungsstand und Auswirkungen

Bei der agentenbasierten Modellierung handelt es sich weniger um eine Technologie zur Digitalisierung konkreter Verwaltungsprozesse, sondern vielmehr um eine neue, computergestützte Form der Analyse und Anleitung staatlichen Handelns. Als Teil meist wissenschaftlicher Politikberatung wird sie in der Regel außerhalb staatlicher Behörden eingesetzt und kann diesen wiederum als eine Entscheidungsgrundlage dienen. Insofern lässt sich also ein Umsetzungsstand im engeren Sinne nur schwer bemessen. Da sich der Einsatz von ABM in der Politikberatung zudem noch in einem experimentellen Zustand befindet, ist eine systematische Evaluation der Auswirkungen zum jetzigen Zeitpunkt noch verfrüht.

Interessant ist dennoch eine Zustandsbestimmung der Verbreitung agentenbasierter Modellierung in der Beratung von Politik. Wie bereits angedeutet, zeigt zunächst der internationale Vergleich, dass agentenbasierte Modellierung in Deutschland noch weniger häufig Verwendung findet als etwa im englischsprachigen Bereich. Dieses Verhältnis deckt sich mit der geografischen Verbreitung evidenzbasierter Politikansätze im Allgemeinen, hängt zugleich aber auch mit konkreten Institutionen und Netzwerken zusammen. Wie jede Form politischer Expertise unterliegen auch Sozialsimulationen einem langfristigen Prozess der Etablierung, Legitimierung und Normalisierung, dem zunächst Unvertrautheit, Skepsis und institutionelle Trägheit gegenüberstehen. Für den deutschen Kontext hervorzuhebende Pionierprojekte sind die bereits erwähnten *AMIRIS*, *SW-Agent* und *Eurace@Unibi*, darüber hinaus aber auch etwa die vom Bundesministerium für Bildung und Forschung geförderten

Projekte *KUBUS* und *SPREAD*, wobei *KUBUS* staatliches Handeln durch die Optimierung von Interventionsszenarien bei Hitzewellen in Nordhessen unterstützen sollte und *SPREAD* die Dynamiken privater Stromanbieterwechsel für eine bessere Gestaltung der Energiewende untersuchte. Diese Beispiele zeigen, dass ABM derzeit nicht direkt in Ministerien oder Verwaltungen verankert ist, sondern in Form konkret problembezogener Projekte vonseiten der Wissenschaft angewandt und von der Politik punktuell nachgefragt und gefördert wird. Des Weiteren führt der relativ hohe zeitliche und finanzielle Entwicklungsaufwand agentenbasierter Modelle dazu, dass sie in der Tendenz eher in langfristigeren und auf höheren staatlichen Ebenen angesiedelten Problemfeldern zum Einsatz kommen und derzeit für einzelne Verwaltungsprozesse eine geringere Rolle spielen. Obgleich ein *Impact Assessment* agentenbasierter Modellierung zum jetzigen Zeitpunkt verfrüh und zudem aufgrund der Heterogenität des Ansatzes wenig sinnvoll erscheint, lässt sich eine generelle Auswirkung doch vermerken. So führt der Einsatz von ABM zu einer verstärkt informatisch geprägten Perspektive auf gesellschaftliche Herausforderungen, in der staatliches Handeln vermehrt auf naturwissenschaftlich inspirierte Erkenntnismethoden zurückgreift. Damit einher geht, und darin ähneln ABM anderen Phänomenen der Digitalisierung, eine Verschiebung innerhalb der Verteilung von Deutungsmacht und Expertise in Staat und Verwaltung hin zu technisch ausgebildetem Personal. Eine zentrale Rolle wird also spielen, welche Gruppen sich agentenbasierte Modellierung aneignen, das heißt ob sie zur Domäne von IT-Expert\*innen und „Social Physicists“ wird oder auch durch politik- und sozialwissenschaftlich ausgebildete Akteure mitgestaltet wird. In jedem Fall deutet der Einsatz agentenbasierter Modellierung in Richtung neuer Sichtweisen auf Gesellschaft, veränderter staatlicher Umgangsweisen mit Zukunft und potenziell neuer Austauschverhältnisse zwischen Wissenschaft auf der einen und Staat und Verwaltung auf der anderen Seite.

---

## 5 Perspektiven für Staat und Verwaltung

Aus sozialwissenschaftlicher Perspektive lässt sich agentenbasierte Modellierung als Teil eines umfangreicheren Trends gesamtgesellschaftlicher Quantifizierung und der wachsenden Bedeutung computerbasierter Welterschließung, auch in Staat und Verwaltung, betrachten. Die zunehmende Übersetzung und Modellierung sozialer Phänomene in Zahlen bietet eine Grundlage für das Vertrauen in die Objektivität agentenbasierter Modelle. Zudem ermöglichen Entwicklungen in der Leistungsfähigkeit von *Computerhardware* immer umfangreichere Simulationen. Als Teilbereich der sich etablierenden Disziplin der *Computational Social Science* erfährt ABM so seit einiger Zeit zunehmende Aufmerksamkeit und die Zahl praktischer Anwendungsfälle befindet sich nicht zuletzt aufgrund vermehrter Förderung im Wachstum. Als Anzeichen dafür kann etwa die Tatsache dienen, dass die Europäische Kommission bei der Gestaltung des Forschungsförderungsprogramms „Horizon 2020“ ihrerseits die Ergebnisse eines agentenbasierten Modells – *INFSO-SKIN* – einbezog (Gilbert et al. 2018). Auch wenn ABM gegenwärtig nur in wenigen Bereichen von Staat und Verwaltung zum Standard gehört und in Deutschland oft

höchstens mittelbar Eingang in die Regierungspraxis findet, kann für die Zukunft mit einer stärkeren Etablierung gerechnet werden.

Für Staat und Verwaltung bedeuten Simulationsmethoden wie die agentenbasierte Modellierung vor allem die Möglichkeit erhöhter Planungsfähigkeit und Kompetenz im Umgang mit komplexen sozialen Dynamiken. Welche Stellung sie als Evidenz für Politikgestaltung auf Dauer tatsächlich einnehmen wird, hängt dabei zunächst vom Erfolg gegenwärtiger Projekte und der wahrgenommenen Legitimität des daraus resultierenden Wissens ab. Wichtig ist weiterhin vor allem, in welchem Ausmaß eine empirische Fundierung sowohl durch *Big Data* als auch durch qualitative Ansätze gewährleistet werden kann, sei es durch die Kalibrierung der Modellparameter oder durch die Validierung anhand empirischer Daten. ABM und der Trend zu *Big Data* bilden hier eine wertvolle Konvergenz und auch Methoden der künstlichen Intelligenz werden in den kommenden Jahren voraussichtlich an Bedeutung gewinnen, etwa durch die häufigere Integration von *Machine Learning* in die Entscheidungsprozesse von Agenten. Für Staat und Verwaltung zeichnet sich somit eine neuartige Verwendungsweise der ihnen zur Verfügung stehenden Daten ab. Eine weitere Neuerung besteht in den Ansätzen zur Einbindung empirischen Wissens auch aus weniger quantitativen Ansätzen, das in der Modellierung von Agenten berücksichtigt werden kann. Einfließen können hier etwa qualitative Interviews mit involvierten Akteuren, aber auch verhaltenspsychologische Experimente und die Erkenntnisse zu psychologischen Mechanismen wie der kognitiven Dissonanz oder zu Heuristiken und kognitiven Verzerrungen. Zu den nennenswerten Perspektiven gehören weiterhin partizipative Ansätze der Modellierung, bei denen versucht wird, möglichst viele *Stakeholder*, also etwa Bürger\*innen oder Unternehmen, in den Prozess der Modellbildung einzubeziehen. Dabei geht es nicht lediglich darum, die beteiligten Akteure mittels Interviews und Fragebögen innerhalb des Modells adäquat abzubilden, sondern vor allem auch darum, dass diese ihre Sichtweisen auf das modellierte System beisteuern und so aktiv an der Modellierung teilhaben können. Sollten sich derartige Ansätze durchsetzen, könnte dies auch in Richtung einer Demokratisierung von Expertise in Staat und Verwaltung wirken.

Ein weiterer Bestandteil der Normalisierung von agentenbasierter Modellierung in der Politikberatung und in Staat und Verwaltung liegt in ihrer Standardisierung. In Großbritannien hat das Finanz- und Wirtschaftsministerium 2015 das *Aqua Book* zur „Guidance on producing quality analysis for government“ veröffentlicht (HM Treasury 2015), in dem Qualitätskriterien für *Policy-Simulationen* und andere Analyseverfahren benannt werden, darunter Verifizierung und Validierung, aber auch Wiederholbarkeit und Unabhängigkeit. Allgemeiner und ohne Bezug zu Computersimulationen hat die Berlin-Brandenburgische Akademie der Wissenschaften 2008 eine Reihe von Leitlinien der Politikberatung publiziert und dabei unter anderem die Notwendigkeit betont, Unsicherheiten, Wissenslücken und implizite Wertannahmen zu kommunizieren und explizit zu machen (Berlin-Brandenburgische Akademie der Wissenschaften 2008). Eine elementare ethische Herausforderung des Einsatzes von ABM in der Politikberatung ist daher dieselbe wie in der Politikberatung im Allgemeinen: Die Gesellschaft sollte möglichst unvoreingenommen beschrieben und Grenzen der Analyse herausgestellt werden. Agentenbasierte

Modelle erweisen sich in dieser Hinsicht, wie beschrieben, als zweischneidiges Schwert. Zum einen besteht die Gefahr, dass Simulationsmodelle implizite Annahmen verstecken, die das Ergebnis in eine schon vorher erwünschte Richtung bewegen, und sich somit den Eindruck von Objektivität und Präzision, den Simulationen und ihre Visualisierungen vermitteln können, für bestimmte politische Ziele zunutze machen. Zum anderen bieten sich allerdings auch zahlreiche Chancen der Transparenzzunahme, da sämtliche Eigenschaften des Modells expliziert und im *Code* festgelegt werden müssen. *Bias* und Diskriminierung sowie Vernachlässigung von Anliegen Betroffener können so aufgezeigt und korrigiert werden.

Von Bedeutung ist es folglich, innerhalb der Politik ein angemessenes Bewusstsein der Chancen, aber auch der Grenzen agentenbasierter Modellierung im administrativen Handeln zu schaffen. Die stets vorhandene Kontingenz und Interpretationsoffenheit von Modellierung sollte kritisch behandelt und die Vielzahl möglicher Zwecke von Simulationen jenseits präziser Vorhersage thematisiert werden. Unter Anerkennung der Tatsache, dass epistemische Konflikte immer auch politische Konflikte bedeuten, sollten möglichst viele Betroffene in den Modellierungsprozess einbezogen werden. Transparenz und Modelldokumentation sowie Verifizierung und Validierung von Modellen können zudem verhindern, dass agentenbasierte Modelle als Feigenblätter der Wissenschaftlichkeit für zuvor dezisionistisch getroffene politische Entscheidungen gebraucht werden. ABM kann dabei niemals alleine Policy-Entscheidungen informieren, zusammen mit anderen Methoden der Politikberatung jedoch einen wertvollen Beitrag zu einer vorausschauenderen und ausgewogeneren Politikgestaltung leisten. Wenn es gelingt, den diskutierten ethischen Herausforderungen zu begegnen, Standards zu schaffen und so die Verankerung agentenbasierter Modelle im Alltag politischer Beratung zu erhöhen, könnten Simulationsansätze zukünftig zum gängigen Repertoire in Staat und Verwaltung zählen.

---

## Literatur

- Berlin-Brandenburgische Akademie der Wissenschaften. 2008. *Leitlinien Politikberatung*. [http://www.bbaw.de/service/publikationen-bestellen/manifeste-und-leitlinien/BBAW\\_PolitischeLeitlinien.pdf](http://www.bbaw.de/service/publikationen-bestellen/manifeste-und-leitlinien/BBAW_PolitischeLeitlinien.pdf). Zugegriffen am 27.11.2019.
- Bonabeau, Eric. 2002. Agent-based modeling: Methods and techniques for simulating human systems. *Proceedings of the National Academy of Sciences* 99(Supplement 3): 7280–7287.
- Bookstaber, Richard. 2017. *The End of Theory. Financial Crises, the Failure of Economics, and the Sweep of Human Interaction*. Princeton: Princeton University Press.
- Duit, Andreas, und Victor Galaz. 2008. Governance and Complexity – Emerging Issues for Governance Theory. *Governance* 21(3): 311–335.
- Edmonds, Bruce. 2017. *The Post-Truth Drift in Social Simulation*. [http://cfpm.org/file\\_download/179/SSC\\_Edmunds\\_SSC2017-309.pdf](http://cfpm.org/file_download/179/SSC_Edmunds_SSC2017-309.pdf). Zugegriffen am 27.11.2019.
- Epstein, Joshua M. 2007. *Generative Social Science. Studies in Agent-Based Computational Modeling*. Princeton: Princeton University Press.
- Epstein, Joshua M. 2008. Why Model? *Journal of Artificial Societies and Social Simulation* 11(4): 1–12.
- Gilbert, Nigel, Petra Ahrweiler, Pete Barbrook-Johnson, Kavin Preethi Narasimhan, und Helen Wilkinson. 2018. Computational Modelling of Public Policy: Reflections on Practice. *Journal of Artificial Societies and Social Simulation* 21(1): 1–14.

- Grimm, Volker, et al. 2006. A standard protocol for describing individual-based and agent-based models. *Ecological Modelling* 198(1–2): 115–126.
- Habermas, Jürgen. 1969. Verwissenschaftlichte Politik und öffentliche Meinung. In *Technik und Wissenschaft als ‚Ideologie‘*, Hrsg. Jürgen Habermas, 120–145. Frankfurt a. M.: Suhrkamp.
- Hartley, James E. 1997. *The Representative Agent in Macroeconomics*. London: Routledge.
- HM Treasury. 2015. *The Aqua Book. Guidance on producing quality analysis for government*. <https://www.gov.uk/government/publications/the-aqua-book-guidance-on-producing-quality-analysis-for-government>. Zugegriffen am 27.11.2019.
- Johnson-Laird, Philip N. 1983. *Mental Models. Towards a cognitive science of language, inference, and consciousness*. Cambridge: Harvard University Press.
- Reeg, Matthias, et al. 2013. *Weiterentwicklung eines agentenbasierten Simulationsmodells (AMIRIS) zur Untersuchung des Akteursverhaltens bei der Marktintegration von Strom aus erneuerbaren Energien unter verschiedenen Fördermechanismen. Abschlussbericht*. Stuttgart: Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR). [https://www.dlr.de/tt/Portaldata/41/Resources/dokumente/institut/system/publications/AMIRIS\\_Weiterentwicklung\\_Abschlussbericht.pdf](https://www.dlr.de/tt/Portaldata/41/Resources/dokumente/institut/system/publications/AMIRIS_Weiterentwicklung_Abschlussbericht.pdf). Zugegriffen am 27.11.2019.
- Wooldridge, Michael, und Nicholas R. Jennings. 1995. Intelligent agents. Theory and practice. *The Knowledge Engineering Review* 10(2): 115–152.



---

# Digitale Verhaltenspolitik

Holger Straßheim

## Inhalt

1 Begriff und Grundlagen .....	124
2 Theoretische Grundlagen .....	124
3 Praktische Anwendungen .....	126
4 Künftige Entwicklungen .....	131
Literatur .....	133

---

## Zusammenfassung

Verhaltenspolitik bezeichnet alle politischen Maßnahmen, die auf Verhaltensänderungen zielen und zu diesem Zweck auf Erkenntnisse der Verhaltenswissenschaften und Psychologie zurückgreifen. In digitalisierter Form basiert Verhaltenspolitik auf der automatisierten Generierung und Auswertungen großer Mengen unterschiedlicher Verhaltensdaten. In Staat und Verwaltung kann sie Tendenzen einer Mikrofokussierung von Politik verstärken. Ihre inter- und transnationale Verbreitung hängt von den jeweiligen Verwaltungs-, Politikberatungs- und Regulierungskulturen ab. Mehr denn je wirft die Debatte um die Verhaltenspolitik die Frage nach den legitimen Formen von Regulierung und Repräsentation unter den Bedingungen der Digitalisierung auf.

---

## Schlüsselwörter

Nudging · Verhaltensökonomik · Maschinenlernen · Scoring · Evidenzbasierte Politik

---

H. Straßheim (✉)

Fakultät für Soziologie, Universität Bielefeld, Bielefeld, Deutschland  
E-Mail: [holger.strassheim@uni-bielefeld.de](mailto:holger.strassheim@uni-bielefeld.de)

## 1 Begriff und Grundlagen

*Verhaltenspolitik* („*behavioural public policy*“) bezeichnet die Gesamtheit aller politischen Maßnahmen und Koordinationsmodi, die auf Verhaltensänderungen zielen und zu diesem Zweck auf Erkenntnisse der *Verhaltensökonomik*, Psychologie, Neurowissenschaften oder der Verhaltenswissenschaften zurückgreifen (Straßheim und Beck 2019). Um digitale Verhaltenspolitik handelt es sich dann, wenn dies auf der Grundlage digitaler Daten geschieht. *Big-Data*-gestützte Verhaltenspolitik basiert auf der mindestens teilautomatisierten Generierung und Auswertungen möglichst großer Datenmengen aus möglichst unterschiedlichen Quellen (Grafenstein et al. 2018).

Verhaltenspolitik ist nicht neu, hat aber seit der Jahrtausendwende inter- und transnational eine erhebliche Verbreitung erfahren. Das Spektrum ist breit und reicht von Vereinfachungen in der Verwaltungskommunikation („*simplification*“), der Schulung im Umgang mit Risiken („*boosts*“) bis hin zur Regulierung manipulativer Marketingstrategien („*budges*“). Bei dem vielfach diskutierten „*Nudging*“ – einem weiteren Subtypus der Verhaltenspolitik – handelt es sich um verhaltenspolitische Maßnahmen, die ohne Zwang und ohne signifikante Anreize Verhaltensänderungen auslösen sollen, indem sie auf den nicht-reflexiven Teil des kognitiven Systems („*system 1*“) zielen und sich dazu wissenschaftlicher Erkenntnisse über Entscheidungsheuristiken und fehlerhafte Verzerrungen von Entscheidungsrationalitäten („*biases*“) bedienen (John 2018).

---

## 2 Theoretische Grundlagen

Bereits in den 1970ern hatten Psychologen wie Amos Tversky, Daniel Kahneman, Baruch Fischoff, Paul Slovic und andere gezeigt, dass unter Bedingungen von Entscheidungsunsicherheit im Verhalten von Individuen mentale Kurzschlüsse und Vereinfachungen zu beobachten sind, die durch Modelle rationalen Handelns nicht erklärt werden können (Kahneman et al. 1982). Zudem werden Verhaltensweisen durch die Art der Präsentation von Optionen beeinflusst – die Anordnung von Produkten in einer Cafeteria oder der Aufbau einer Webseite können die Auswahlentscheidung beeinflussen. Nicht immer lösen zusätzliche Informationen das Problem, da sie tendenziell zu einer Steigerung von Unsicherheit und damit zu einer höheren Fehlerwahrscheinlichkeit führen. *Nudging* verändert systematisch solche Entscheidungsarchitekturen („*choice architectures*“), um durch die gezielte Aktivierung bestimmter Heuristiken die Verzerrungen im Verhalten auszugleichen (Thaler und Sunstein 2008). Wenn Einflüsse durch Entscheidungsarchitekturen ohnehin unvermeidbar und ubiquitär sind, so ein zentrales Argument, dann sollten politische Akteure mit der Hilfe von Verhaltensexperiten selbst zu Entscheidungsarchitekten werden. Die Fliege im Urinal, abstoßende Bilder auf Zigarettenpackungen, Treppeinstufen mit Pianoklang – wir beobachten mittlerweile die Verbreitung und Veralltäglichung von *Nudging*. Dabei ist *Nudging* sowohl in der wissenschaftlichen als auch in der politischen Diskussion umstritten. Manche Kritiker plädieren eher für eine erzieherische Unterstützung des reflexiven Teils des kognitiven Systems

(„system 2“), um das Wissen über Heuristiken zu erhöhen, Anpassungs- und Entscheidungspotenziale anzuregen und Individuen zu einem bewußten Umgang mit Risiken und Unsicherheiten zu befähigen (John 2018). Verhaltenspolitik darf also nicht auf *Nudges* reduziert werden, sondern nimmt je nach Umsetzung sehr unterschiedliche Formen an.

Den gemeinsamen Fluchtpunkt aller Formen der Verhaltenspolitik bilden zwei eng miteinander zusammenhängende Annahmen, durch die sie sich von anderen Politiken unterscheidet (Straßheim und Beck 2019; Straßheim 2018): Erstens setzt sie auf der Ebene individuellen Verhaltens an – also auf der Mikroebene und nicht etwa bei Organisationen, Strukturen oder Aggregaten auf der Meso- und Makroebene. Verhaltenspolitik ist mikrofokussiert, auch wenn es um übergreifende Normen, Werte oder Interessen geht. Kleinschrittige Veränderungen des Verhaltens können, so die Idee des „*radikalen Inkrementalismus*“, potenziell große Auswirkungen auf den Erfolg oder Misserfolg von Politiken haben (Halpern und Mason 2015). *Radikaler Inkrementalismus* fordert zugleich die radikale und den gesamten Politikprozess umfassende Evaluation dieser Politiken im Hinblick auf Effektivität und Effizienz. Dabei wird solchen Verfahren der Politikevaluation der Vorzug gegeben, die politisch wie wissenschaftlich als „Goldstandards“ gelten, insbesondere *randomisierten Kontrollstudien* („randomized controlled trials“, RCTs) und zunehmend digitalen Verhaltensanalysen. Zweitens bedient sich Verhaltenspolitik empirischer und theoretischer Erkenntnisse der Kognitions- und Verhaltensforschung. Sie verknüpft also politische Gestaltungs- mit verhaltenswissenschaftlichen Geltungssprüchen. Dahinter steht die Annahme, dass ein systematischer Zusammenhang zwischen den Mechanismen individuellen Verhaltens und den Wirkungsbedingungen von Politik besteht, der durch wissenschaftliche Erkenntnisse und Evidenzen erhellt und in politische Interventionen übersetzt werden kann. Diese Annahme bezieht sich nicht auf einzelne Instrumente oder Politikfelder, sondern umfasst potenziell alle politischen Maßnahmen und Koordinationsmodi. Verhaltenspolitik versteht und legitimiert sich in diesem Sinne immer auch als „*evidenzbasierte Politik*“. Zur Verhaltenspolitik gehört daher auch der Aufbau, die Verbreitung und Institutionalisierung von Verhaltensexpertise an den Schnittstellen von Wissenschaft und Politik. Auf diese Weise gewinnt sie politische wie epistemische Autorität.

Die Digitalisierung und *Big Data*-Unterstützung von Verhaltenspolitik gilt vor dem Hintergrund dieser Annahmen als konsequenter, nächster Schritt. Sie basiert auf vier analytisch unterscheidbaren, wenn auch empirisch miteinander verbundenen Typen von Praktiken und Verfahren (Grafenstein et al. 2018): Erstens zielt sie auf die *Generierung von Verhaltens- und Kontextdaten*. Durch Sensoren, die Selbsteingabe von Nutzerdaten, *Online*-Verhaltensanalysen, Text- und Bildanalysen, aber auch die Verknüpfung („*Kommensurabilisierung*“) mit bereits Bestehendem werden Daten aus unterschiedlichen Quellen zusammengefügt. Dies ermöglichen die ubiquitäre, kontinuierliche, simultane und (teil-)automatisierte Erhebung von Daten über Verhalten und Entscheidungsarchitekturen zugleich. Verhaltenspolitik kann damit potenziell über den gesamten Politikprozess hinweg in Echtzeit auf der Mikroebene beobachtet und evaluiert werden. Diese zeitliche Synchronisation von Evidenzen und Entscheidungen entspricht einer zentralen Forderung des *radikalen Inkrementalismus*.

Zweitens öffnen *Big Data*-gestützte Verfahren den Weg für vielfältige Verfahren der *Verhaltensanalyse* und der Identifikation von *Prognosen*, Mustern und Profilen. Die Erstellung von Lageberichten und Trends, individualisierten Verhaltensprofilen, das Erkennen von Regelmäßigkeiten und Anomalien basiert auf Verfahren des *Text-Mining*, der Mustererkennung, Netzwerkanalyse oder des algorithmischen Maschinenlernens („*machine learning*“). Digitale Verhaltenspolitik nutzt diese Verfahren, um Verhaltensmuster und Vorhersagen zu erstellen, zu visualisieren und damit für den Entscheidungsprozess verfügbar zu machen.

Drittens erfolgt die zunehmend automatisierte *Verhaltensbewertung* in Form von kardinal oder ordinal skalierbaren Punktesystemen („*scoring*“) oder Rangordnungen („*ranking*“), die dann in nominale Klassifikations- oder Kategoriensysteme übersetzt und damit der eigentlichen Bewertung von Verhalten zugänglich gemacht werden können. Das Ergebnis sind komplexe und auch für Programmierer nicht mehr ohne weiteres rekonstruierbare Klassifikationen von Verhalten. Das liegt daran, dass Verfahren des Maschinenlernens im Gegensatz zu traditionellen Methoden der künstlichen Intelligenz ihre Klassifikationen kontinuierlich und eigenständig optimieren.

Schließlich und viertens bildet die Generierung, Analyse und Bewertung von Verhaltens- und Kontextdaten die Voraussetzung für *Verhaltensregulierungen*. Verhaltenspolitik wird personalisiert, indem aufgrund der Verhaltensbewertung jeweils für Gruppen von Verhaltensmustern oder sogar Einzelpersonen maßgeschneiderte Interventionen entwickelt, angewandt und (in Echtzeit) evaluiert werden („*targeted interventions*“). Die Logik der Mikrofokussierung von Politik, die auf das jeweilige Individuum in seiner je spezifischen Entscheidungsarchitektur zielt – und dies bei einer möglichst großen Zahl von Adressaten – findet hier ihre Vollendung (Straßheim 2018).

---

### 3 Praktische Anwendungen

Verhaltenspolitik ist – auch in digitalisierter Form – inter- wie transnational weit verbreitet und kommt in nahezu allen Politikfeldern zum Einsatz (Straßheim 2017). Das früheste Beispiel einer verhaltenspolitischen Expertiseeinheit findet sich in Singapur: Am *Home Team* (HT), einem Zusammenschluss der dem Innenministerium nachgeordneten Polizei-, Sicherheits- und Strafbehörden wurde bereits 2006 das *Home Team Behavioural Sciences Center* (HTBSC) gegründet. Weitere Vorreiter sind vor allem die angelsächsischen Länder und hier insbesondere die USA, Großbritannien, Australien und Neuseeland. Die von Obama 2015 erlassene Executive Order 13707 „Using Behavioural Science Insights to Better Serve the American People“ weist alle Ministerien und Agenturen der amerikanischen Regierung an, Politiken und Programme auf die Anwendbarkeit verhaltenspolitischer Erkenntnisse zu überprüfen, Verhaltensexpertise einzuholen und durch Maßnahmen der Verwaltungsvereinfachung, der Gestaltung von Entscheidungsarchitekturen und entsprechende Verhaltensinterventionen umzusetzen. Das *Office of Evaluation Sciences* (OES) in der *General Services Administration* (GSA) verfolgt entsprechende Strategien.

In Großbritannien ist die Verbreitung von Verhaltenspolitik eng verbunden mit dem *Behavioural Insights Team* (BIT), einer seit 2014 teilprivatisierten Einheit, die sich mit ihren mehr als 120 Mitarbeiter\*innen in der Londoner Zentrale sowie in den Büros in Manchester, Sidney, Wellington, Singapur und New York zum Vorbild weltweit entwickelt hat. Die BIT-Abteilung *BI Ventures* entwickelt *Online*-Plattformen, um Methoden und Techniken der digitalen Verhaltenspolitik zu verbreiten. Kooperationspartner sind neben vielen anderen die *Behavioural Insights Unit* des *New South Wales' Department of Premier and Cabinet* (NSW BIU), das *Behavioural Economics Team of the Australian Government* (BETA) wie auch das Finanzministerium in Neuseeland.

Skandinavische Länder folgen in doppelter Hinsicht einem abweichenden Ansatz: In Norwegen und Dänemark sind es neben Expertenteams vor allem Multiakteursnetzwerke, in denen Instrumente der Verhaltenspolitik entwickelt und erprobt werden. Das *Danish Nudging Network* (DNN), ein Zusammenschluss von zivilgesellschaftlichen, politisch-administrativen, wirtschaftlichen und verhaltenswissenschaftlichen Akteuren ist eng mit *iNudgeyou*, der „Danish Nudge Unit“ (so die Selbstauskunft) verbunden. In ähnlicher Weise agiert auch das norwegische *Green Nudge*.

In kontinentaleuropäischen Ländern wie Deutschland, Frankreich, Italien, Österreich oder den Niederlanden wird Verhaltenspolitik in einer eher dezentralen, teilweise durch interministerielle oder interadministrative Abstimmungseinheiten sehr lose gekoppelten Form organisiert (z. B. durch das Referat „Wirksam Regieren“ im Kanzleramt). Das liegt zu einem erheblichen Teil an den Verwaltungskulturen in diesen Ländern, die dem Ressortprinzip eine wichtige Rolle einräumen. In Deutschland etwa ist auch in Zukunft eine Umsetzung digitaler Verhaltenspolitiken eher in einzelnen Ministerien bzw. nachgeordneten Behörden und in einzelnen Politikfeldern zu erwarten. So hat man sich in den vergangenen Jahren insbesondere im Bundesamt für Sicherheit in der Informationstechnik (BSI) intensiv mit Möglichkeiten auseinandergesetzt, durch digitales *Nudging* und andere Formen der Verhaltenspolitik die Verbraucher\*innen vor Manipulationen auf *Online*-Märkten zu schützen. Intelligente und individualisierte Voreinstellungen („smart defaults“) können die Verweildauer im Netz oder am Telefon limitieren; *Plug-Ins* bieten für ausgewählte Webseiten oder zu festgelegten Tageszeiten digitale Selbstbeschränkungen gegen suchtähnliches und selbstschädigendes Konsumverhalten an („shopper stopper“); Textnachrichten erinnern an die Kündigung von *Online*-Abonnements. Weitere Anwendungen finden sich in der Energiepolitik (z. B. bei der Energieabrechnung), der Gesundheitspolitik (z. B. durch intelligente und vernetzte Fitnessstracker) oder der Mobilitätspolitik (z. B. durch digitale Feedbacksysteme).

Lateinamerikanische Staaten wie Mexiko, Kolumbien, Costa Rica, Peru oder Guatemala kooperieren bei der Entwicklung verhaltenspolitischer Interventionen häufig mit dem BIT, der Weltbank und den Vereinten Nationen. Mexiko ist mit dem 1997 etablierten *Conditional Cash Transfer Programme* (CCT) „Prospera“ ein besonders prominenter und auch einflussreicher Fall. In Zusammenarbeit mit dem Präsidialamt Mexikos, der zivilgesellschaftlichen Organisation *Qué Funciona para el Desarrollo* (QFD), UNICEF und dem BIT entstand ein interaktives System von

Textnachrichten, das schwangere Mütter zur Wahrnehmung von Untersuchungs- und Vorsoreterminen anregen soll („Prospera Digital“). In weiteren Ländern ist die Einrichtung von verhaltenspolitischen Expertenteams geplant oder bereits umgesetzt worden: Beispiele sind Indiens *Think Tank NITI Aayog* in Kooperation mit der *Bill & Melinda Gates Foundation*, die *Qatar Behavioural Insights Unit* (QBIU), die *Nudge Unit Japan* im japanische Umweltministerium und *NudgeLebanon*.

Verhaltenspolitik hat längst auch die transnationale Ebene erreicht: Ein Protagonist ist die Weltbank mit der *Mind, Behavior and Development Unit* (eMBeD); die Vereinten Nationen haben die *UN Behavioural Initiative* (UNBI) etabliert und testen im Rahmen des Agenda 2030 Prozesses Verhaltensinterventionen; die OECD bearbeitet die Thematik durch eine Serie von *Surveys* und Konferenzen. Die EU-Kommission entwickelt seit mehr als zehn Jahren Interventionen in einem zunehmend größeren Spektrum von Politikbereichen. Im Jahr 2014 gründete das *Joint Research Centre* (JRC) die *Foresight, Policy Design and Behavioural Insights Unit* (FBIU), die nun unter dem Dach des *EU Policy Labs* Verhaltenspolitiken entwickeln und koordinieren soll.

Anhand der oben genannten vier Typen von Praktiken und Verfahren (Datenerhebung, Datenanalyse, Datenbewertung und Verhaltensregulierung) lassen sich zumindest beispielhaft solche Anwendungen digitaler Verhaltenspolitik identifizieren, die in den genannten Organisationen und Netzwerken entwickelt werden:

- Die Generierung und Kommensurabilisierung möglichst großer und verschiedener Mengen von Verhaltensdaten bildet ein zentrales Element von Verhaltenspolitik. Ihre Bedeutung ist in den vergangenen Jahren erheblich gestiegen, unter anderem weil randomisierte Kontrollstudien (RCTs) – die bislang als Goldstandard etikettierte und in Evidenzhierarchien am höchsten bewertete Datenquelle – wegen des Aufwandes, der Kosten, Problemen der Replizierbarkeit und der Übertragbarkeit auf andere Kontexte in die Kritik geraten sind. Verhaltenspolitische Expertenorganisationen wie das BIT oder das am *Massachusetts Institute of Technology* (MIT) ansässige *Abdul Jameel Poverty Action Lab* (J-PAL) kombinieren daher die Daten aus hunderten von weltweit umgesetzten RCTs mit anderen Daten auf der Mikroebene, etwa strukturierte Daten amtlicher Statistiken, aber auch unstrukturierte Daten aus digitalisierbaren Aktennotizen oder von Internetseiten („scraping“). Potentiell können diese Datenquellen noch vervielfältigt werden, etwa durch automatisch erhobene Bewegungs-, Positions- und Körperdaten aus *Wearables* oder *Smartphones*, Kommunikationsdaten, Energieverbrauchs- und Mobilitätsdaten wie auch Daten über das Internetverhalten (Mausbewegungen etc.); hinzu kommen Daten aus Monitoringsystemen im öffentlichen Nahverkehr, aus Überwachungs- und Mautkameras oder „smartten“ Gegenständen wie etwa anwesenheitssensiblen Gebäuden; schließlich Daten durch die Selbsteingabe von Informationen über die Gesundheit, das Ernährungsverhalten oder politische Präferenzen. Verhaltenspolitisch relevant ist oft schon die Visualisierung der Daten selbst, beispielsweise über die Langzeitentwicklung des eigenen Körpergewichts, die Zahl der Jogger in der Umgebung, den laufenden Energieverbrauch, das Verhalten anderer Verkehrsteilnehmer, das Verhalten

von Wählern oder die Entscheidungsbegründungen anderer Kollegen in Behörden (z. B. in der Sozialarbeit). Es geht also bereits bei der Generierung verhaltenspolitischer Daten um die auch öffentlich demonstrierbare Steigerung der politischen und wissenschaftlichen Aussagekraft („data maturity“); zugleich werden durch Visualisierungen und andere Datenrepräsentationen informationelle Entscheidungsarchitekturen errichtet, die selbst bereits verhaltenspolitisch eingesetzt werden können.

- Die Generierung von Verhaltensdaten ist eng verwoben mit deren Bewertung. Gemeint ist damit ein Prozess, bei dem die Relevanz bestimmter Daten, ihre Hierarchisierung und Gruppierung letztlich in *Klassifikationen* und Kategorien mündet, die wiederum für Prognosen, Lagebilder und Trends oder für die Erkennung von Anomalien genutzt werden können. Dabei beruht die maschinengestützte Analyse von Verhaltensweisen nicht auf vorgegebenen Bewertungsschemata, sondern ist das Ergebnis eines in Echtzeit ablaufenden Prozesses der algorithmischen Reduktion von Komplexität durch Schwellenwerte und Clusterbildungen. Die sich daraus ergebenden Ordnungs- und Bewertungsmodelle beruhen auf komplexen, für Programmierer wie Nutzer nicht ohne weiteres rekonstruierbaren Rechenschritten (Passoth und Straßheim 2018). *Big Data*-Verfahren werden in Organisationen wie dem BIT oder J-PAL auch genutzt, um Daten aus früheren RCTs noch einmal zu analysieren. Das BIT (2018) unterzog die Aktennotizen, die Sozialarbeiter bei der Entscheidung über Kinderbetreuungen anfertigen, Methoden des „structural topic modelling“, also der statistischen Analyse von Wortclustern. In der Kombination mit amtlichen Statistiken und auf der Grundlage von Informationen über frühere Fallgeschichten wurde ein Risikomodell erstellt, das Prognosen über zunächst unauffällige Eskalations- und Härtefälle ermöglicht. Das Ergebnis ist ein digitales Verhaltenstool, das den Sozialarbeitern bzw. ihren Vorgesetzten praktisch in Echtzeit anhand der angefertigten Notizen die Risiken einer Fehlentscheidung visuell und statistisch anzeigt. Ähnliche Methoden sind auch für die Gesundheitspolitik relevant: Gesundheitsdaten aus Therapieverläufen, Verhaltensdaten und genetischen Informationen lassen sich für gesundheitspolitische Entscheidungen so kombinieren, dass Dispositionen für Erkrankungen oder die Erfolgswahrscheinlichkeiten für misslingende Operationen im Einzelfall abgeschätzt werden können. In den Krankenhäusern des *Department of Veterans Affairs* der US-Regierung lösen bedenkliche Befunde, etwa ein auffälliges Blutbild, eine Nachricht an die behandelnden Ärzte aus. Die britische *Care Quality Commission* (CQC) konnte in Kooperation mit dem BIT auf der Basis nationaler Gesundheitsstatistiken, Verschreibungsdaten und Online-kommentare 95 % der zuvor in Inspektionen aufgefallenen problematischen Kliniken identifizieren und so ein Modell für medizinische „underperformer“ entwickeln. In der Sicherheitspolitik („predictive policing“) werden Verfahren des Maschinenlernens entwickelt, um auf der Grundlage von Passagierverhaltensdaten potenzielle Drogenkuriere, Terroristen und illegale Einwanderer zu erkennen – oder solche, die es zukünftig werden könnten. Die Bewertung von Verhaltensdaten ist insofern in ihren Anwendungsbereichen kaum begrenzt. Sie

beruht auf der komplexen Verknüpfung automatisierter und dynamischer Mustererkennungen, Datenhierarchisierungen, Datenklassifizierungen und nachträglichen Interpretationen durch Nutzer, Entscheider, Experten oder die Öffentlichkeit.

- Das Ziel der Generierung und Bewertung von Verhaltensdaten sind letztlich auf Einzelpersonen zugeschnittene *Verhaltensregulierungen*. So arbeiten Wahlkampfteams schon seit Jahren mit Verhaltensexpererten zusammen, um politische Botschaften auf Individuen zuzuschneiden und so eine personalisierte Kommunikationsumwelt zu errichten. In *East Sussex* ermittelte das BIT (2018) auf der Grundlage von Verkehrsunfallstatistiken, Aktennotizen zu Unfällen und anderen Verkehrs- und Infrastrukturstatistiken algorithmisch die Risikogruppen und erprobte dann für diese Gruppen maßgeschneiderte Briefe und Textnachrichten mit direktem Bezug zu deren eigenen Verkehrsvergehen. Das *Center for Data Science and Public Policy* der Universität Chicago hat „targeted interventions“ in verschiedenen Politikbereichen – Gesundheit, öffentliche Sicherheit, Erziehung, Arbeitsmarktpolitik, Stadtentwicklung Umwelt und Energie – erprobt und umgesetzt: *Early Interventions Systems* (EIS) identifizieren solche Polizeibeamte, die sich möglicherweise nicht regelgemäß verhalten oder sogar unberechtigt Gewalt anwenden und weist sie präventiv entsprechenden Beratungen und Fortbildungen zu. In Zusammenarbeit mit der *White House's Workforce Data Initiative* und dem *Department of Labor* werden Daten aus Bundes-, Landes- und Städtestatistiken kombiniert und zeigen in der *Open Source*-Anwendung *DataAtWork* in Echtzeit die Entstehung von Problemquartieren und städtischen Brennpunkten an, um dann Mikrointerventionen vorzuschlagen. Personen, die in den USA ihre Steuererklärung digital ausgefüllt haben, wurden über die Form ihrer eventuellen Steuerrückzahlungen befragt und bekamen automatisch eine Option angezeigt, das Geld direkt in ein steuerlich begünstigtes Altersvorsorgeprogramm einzuzahlen. Das Programm wurde unter der Regierung Trump eingestellt. Einen weiteren Anwendungsbereich bilden vielfältige Formen der *App*-gestützen Selbstregulierung und Selbstvermessung (Grafenstein et al. 2018). Die *App Nudgy* lädt dazu ein, sich Ziele zu setzen, *To-Do*-Listen zu erstellen und Bekannte als persönlicher „Nudge Pal“ mit der Kontrolle der Zielerreichung zu beauftragen; *Apps* wie *UbiGreen* zeigen den Nutzern die Umweltfreundlichkeit ihres Mobilitätsverhaltens an; *FoodSwitch* ermittelt beim *Scannen* eines Lebensmittelstrichodes die Nährwerte zeigt durch Visualisierungen, ob das Produkt mit den gesundheitlichen Präferenzen der Nutzer übereinstimmt. In allen diesen Fällen werden Erkenntnisse der Verhaltensökonomik und Psychologie über kognitive Heuristiken gezielt genutzt, um individuelle Verhaltensänderungen auszulösen. Chinas viel zitiertes *Sozialkredit-System*, ein komplexes und eigentlich aus vielen verschiedenen Teilsystemen des *Scorings* und *Ratings* zusammengesetztes System, verbindet dagegen *Nudging*-Techniken mit Überwachung, Anreizen und Strafen – und verzahnt auf diese Weise digitalisierte Verhaltenspolitik mit dem Regulierungsarsenal des autokratischen Staates.

## 4 Künftige Entwicklungen

Überblickt man die gegenwärtige Forschung, so können eine Reihe von Erklärungsansätzen und Thesen identifiziert werden, die Ermöglichungsbedingungen und Einflussfaktoren der Verbreitung digitaler Verhaltenspolitik identifizieren, daraus Vermutungen über künftige Entwicklungen ableiten und sich dabei auch normativ positionieren. Digitale Verhaltenspolitik erscheint als das Ergebnis des Aufstiegs der digitalen Ökonomie und der Technologisierung aller Lebensbereiche, als radikale Konsequenz der Psychologisierung und Therapeutisierung der Gesellschaft, als Medium der Erschließung neuer Interventionsräume für den Staat oder als Ausdruck globaler Verwissenschaftlichung, Technokratisierung, Ökonomisierung, Neoliberalisierung und Deregulierung (Straßheim und Beck 2019; John 2018). Digitale Verhaltenspolitik entsteht dann als das Produkt einer multiplen Gelegenheitskonstellation: „an idea whose time has come“ (Kingdon 1995). Damit sind allerdings primär generelle Kontextbedingungen benannt, die zudem teilweise im Widerspruch zueinanderstehen und keine spezifischen Aussagen über die Entstehungszusammenhänge und Mechanismen digitaler Verhaltenspolitik erlauben. Dies jedoch wäre die Voraussetzung, um das Phänomen in seinen Varianten, Dimensionierungen und Konsequenzen erfassen zu können. Drei Erklärungsansätze lassen sich unterscheiden (Selbstbindungstheorien, Gouvernementalitätstheorien, politische Epistemologien):

- (1) In einer Variante des Selbstbindungstheorems bei Jon Elster und anderen wird von den Protagonisten der Verhaltenspolitik wie Cass Sunstein argumentiert, dass sich mit der weltweiten Ausdehnung von Kommunikationshorizonten und der Verbreitung digitaler Technologien die Entscheidungsfreiheiten, aber auch -zwänge vervielfacht haben (Sunstein 2015; Elster 2000). Immer komplexere Informationsumwelten, aber auch die Möglichkeiten privatwirtschaftlicher Manipulation erhöhen das Risiko von Fehlentscheidungen und Kontrollverlust. Kognitive Überlastung führt zu Inkonsistenzen in der Präferenzbildung und damit zur Selbstschädigung. Das schiere Übermaß von Optionen aktiviert jene Heuristiken, die unter Druck zwar die Entscheidungsfähigkeit sichern, aber zugleich Rationalitätsverzerrungen und Zielabweichungen verursachen. Digitale Verhaltenspolitik entsteht als Reaktion darauf und ermöglicht die Rückgewinnung von Autonomie und Authentizität durch *personalisierte Selbstbindungs-technologien*. Die Vereinfachung komplexer Informationen und *Tools* der Selbst- und Fremdfestlegung entlasten Individuen in vielen Bereichen, schützen Konsumenten und Konsumentinnen vor Fehlentscheidungen und ermöglichen die Konzentration auf das wirklich Relevante. Freiheit wird durch Selbstbindung zurückgewonnen. Die Option, sich durch individuell zugeschnittene Vorentscheidungen („*personalized default rules*“) bei komplexen Fragen in der Renten-, Gesundheits-, oder Umweltpolitik einem öffentlichen Drittentscheider zu übereignen, wird aus gutem Grund vielfach gewählt. Aus dieser Sicht muss es

unter diesen Bedingungen in Zukunft die Aufgabe des Staates sein, personalisierte Selbst- und Fremdbindungstechnologien anzubieten und durch das aktive Design von Entscheidungsarchitekturen die Selbstbestimmungsfähigkeit der Bürger sicherzustellen („libertärer Paternalismus“).

- (2) Demgegenüber sehen Theoretiker in der Tradition Foucaults in dem Aufstieg der digitalen Verhaltenspolitik die seit langem absehbare Ausprägung von *Gouvernementalität* in Zeiten des globalisierten *Neoliberalismus* (Whitehead et al. 2017; Bröckling 2017). Gegenüber dem klassischen Liberalismus sucht der Neoliberalismus nach Wegen, die Markttauglichkeit der Gesellschaft durch eine prominente Rolle des Staates zu sichern. Unter diesen Bedingungen entstehen Technologien des Regierens, die auf paradoxe Weise Formen der unternehmerischen Selbstentfaltung mit den Normalisierungsstrategien von Regulierern, Experten und Therapeuten verbinden. Digitale Verhaltenspolitik ist die letzte Konsequenz dieser Entwicklung und eine Antwort auf die selbsterzeugten Probleme kapitalistischer Gesellschaften wie Klimawandel, Verschuldung und ungesunden Lebenswandel. Sie zeigt neue Möglichkeiten auf, durch Regierungsformen der verhaltensbasierten und neuronalen Manipulation („Neoliberalismus“) die Selbstdestruktionstendenzen im fortgeschrittenen Kapitalismus zu bändigen, die Verwissenschaftlichung des Sozialen voranzutreiben und Sozial- und Selbsttechnologien auf der Mikroebene in Einklang zu bringen.
- (3) *Politische Epistemologien* basieren auf Erkenntnissen der Wissenssoziologie und Wissenschaftsforschung, der *Science, Technology and Society Studies* (STS) und des Neoinstitutionalismus. Entsprechende Forschungen gehen nicht von einheitlichen Entwicklungsdynamiken aus, sondern von multiplen, durchaus widersprüchlichen Verknüpfungen zwischen Erkenntnis- und Ordnungsbildung unter den Bedingungen der postnationalen Konstellation (Straßheim 2017). Beobachtet wird seit geraumer Zeit eine Pluralisierung von Akteuren und Akteursgruppen, die über Grenzen und Ebenen hinweg Geltungs- und Gestaltungsansprüche erheben. Durch intermediäre und grenzüberschreitende Expertenorganisationen, die Mobilisierung wissenschaftlich anerkannter und politisch hochgradig relevanter Evidenzen aus randomisierten und digital bearbeiteten Kontrollstudien und durch die Neustrukturierung politischer Zeithorizonte in Echtzeitprozessen wird politische und epistemische Autorität mobilitiert. Digitale Verhaltenspolitik wird aus dieser Sicht dann epistemisch und politisch besonders wirksam, wenn es ihr gelingt, durch Musterbildung und Kategorisierung das Wissen von Gesellschaft über sich selbst zu prägen und damit zugleich auch zur Repräsentation und Legitimierung kollektiven Handelns beizutragen. So verändern *Big Data*-basierte Verhaltensanalysen das Bild, das sich Parteien von Wählern machen und dies verändert wiederum die Selbstwahrnehmung der Wähler. Digitale Verhaltenspolitik ist insofern performativ, transformiert die Erkenntnis- und Entscheidungsmöglichkeiten von Politik und verändert, z. B. durch die Delegation von Bewertungs- und Entscheidungskompetenzen an Algorithmen (etwa im Zuge von „Scoring“), sogar politisches Handeln selbst.

Digitale Verhaltenspolitik ist keinesfalls ein Selbstläufer, sondern muss sich in spezifischen institutionellen und soziotechnischen Kontexten bewähren. Die Reichweite von Verhaltenspolitiken hängt vor allem von den jeweiligen *Verwaltungs- und Rechtskulturen*, den dominierenden Formen der *Expertise* und den *Innovations- und Regulierungssystemen* ab (Straßheim et al. 2015). Diese Faktoren erklären die weltweit zu beobachtende Vielfalt und unterschiedliche Durchsetzungsstärke digitaler Verhaltenspolitiken. Angesichts der massiven Verwertung personalisierter Verhaltensdaten durch global agierende Konzerne werden allerdings zukünftig die Forderungen zunehmen, der Staat möge selbst im Namen der Konsumenten Verhaltenssteuerung betreiben (Yeung 2018). Längst sind digitale Nudges im Bereich der „Cyber-Security“ Gegenstand intensiver Diskussionen (Dold und Krieger 2017). Mehr denn je wirft die Debatte um die Verhaltenspolitik daher die Frage nach den legitimen Formen von Regulierung und Repräsentation unter den Bedingungen der Digitalisierung auf.

---

## Literatur

- BIT. 2018. *Using data science in policy. A report by The Behavioural Insights Team*. London: The Behavioural Insights Team.
- Bröckling, Ulrich. 2017. *Gute Hirten führen sanft. Über Menschenregierungskünste*. Frankfurt a. M.: Suhrkamp.
- Dold, Malte, und Tim Krieger. 2017. Cyber-Security aus ordnungspolitischer Sicht. Verfügungsrechte, Wettbewerb und Nudges. *Wirtschaftsdienst* 97(8): 559–565.
- Elster, Jon. 2000. *Ulysees unbound. Studies in rationality, precommitment, and constraint*. Cambridge: Cambridge University Press.
- Grafenstein, Max von, Max, Julia Hözl, Florian Irgmaier, und Jörg Pohle. 2018. *Nudging. Regulierung durch Big Data und Verhaltenswissenschaften. Gutachten im Rahmen des Projekts Assessing Big Data (ABIDA)*. Berlin: Alexander von Humboldt Institut für Internet und Gesellschaft.
- Halpern, Michael, und Danielle Mason. 2015. Radical incrementalism. *Evaluation* 21(2): 143–149.
- John, Peter. 2018. *How far to nudge? Assessing behavioural public policy*. Cheltenham/Northampton: Edward Elgar.
- Kahneman, Daniel, Paul Slovic, und Amos Tversky, Hrsg. 1982. *Judgement under Uncertainty. Heuristics and Biases*. Cambridge: Cambridge University Press.
- Kingdon, John W. 1995. *Agendas, alternatives, and public policies*, 2. Aufl. New York: Harper Collins.
- Passoth, Jan, und Holger Straßheim. 2018. Normativ hergestellte Erwartungen durch Big Data. Normierung, Normalisierung und Nudging. In *Big Data und Gesellschaft. Eine multidisziplinäre Annäherung*, Hrsg. Barara Kolany-Raiser, Reinhard Heil, Carsten Orwat und Thomas Hoeren, 169–178. Wiesbaden: VS Verlag für Sozialwissenschaften.
- Straßheim, Holger. 2017. Die Globalisierung der Verhaltenspolitik. In *Kapitalismus, Globalisierung, Demokratie. Jahrbuch Normative und institutionelle Grundfragen der Ökonomik Band 16*, Hrsg. Katharina Hirschbrunn, Gisela Kubon-Gilke und Richard Sturm, 211–242. Marburg: Metropolis.
- Straßheim, Holger. 2018. Verhaltenspolitik im Wohlfahrtsstaat. Zur Mikrofokussierung in der Sozialpolitik(forschung). *Sozialer Fortschritt* 67(8–9): 759–782.
- Straßheim, Holger, und Silke Beck, Hrsg. 2019. *Handbook of behavioural change and public policy*. Cheltenham/Northampton: Edward Elgar.

- Straßheim, Holger, Arlena Jung, und Rebecca-Lea Korinek. 2015. Reframing expertise. The rise of behavioural insights and interventions in public policy. In *Moments of valuation. Exploring sites of dissonance*, Hrsg. Ariane Berthoin Antal, Michael Hutter und David Stark, 249–268. Oxford: Oxford University Press.
- Sunstein, Cass R. 2015. *Choosing not to choose. Understanding the value of choice*. Oxford/New York: Oxford University Press.
- Thaler, Richard H., und Cass R. Sunstein. 2008. *Nudge. Improving decisions about health, wealth and happiness*. New Haven: Yale University Press.
- Whitehead, Mark, Rhys Jones, Rachel Lilley, Jessica Pykett, und Rachel Howell. 2017. *Neuroliberalism. Behavioural government in the twenty first century*. London/New York: Routledge/Taylor & Francis Group.
- Yeung, Karen. 2018. Five fears about mass predictive personalization in an age of surveillance capitalism. *International Data Privacy Law* 8(3): 258–269.

---

## **Teil III**

### **Leitbilder und normative Grundfragen**



---

# Agile Verwaltung

Daniel Rölle

## Inhalt

1 Klärung des Begriffs .....	138
2 Konzeptionelle Grundlagen .....	139
3 Praktische Anwendung .....	142
4 Hürden für die agile Verwaltung .....	144
5 Perspektiven für Staat und Verwaltung .....	145
Literatur .....	146

---

## Zusammenfassung

Ereignisse wie die Flüchtlingskrise, terroristische Bedrohungen oder Umweltprobleme stellen die öffentliche Verwaltung vor neue Herausforderungen, die wegen der Komplexität der Ereignisse kaum mehr nach dem klassischen Zuständigkeitsprinzip innerhalb der Verwaltung gelöst werden können. Diesen Herausforderungen kann die Verwaltung, so das Konzept der „agilen Verwaltung“, nur vernetzt begegnen. Was aber ist wirklich neu an der agilen Verwaltung? Welche Rolle spielt dabei die Digitalisierung? Der Beitrag setzt sich kritisch mit der Funktionalität, der Umsetzbarkeit und der Zukunft einer agilen Verwaltung auseinander.

---

## Schlüsselwörter

Vernetzung · Prozesse · Kommunikation · Verwaltungskultur · Arenen

---

D. Rölle (✉)

Lehrstuhl für Verwaltungswissenschaft, Universität Konstanz, Konstanz, Deutschland  
E-Mail: [daniel.roelle@uni-konstanz.de](mailto:daniel.roelle@uni-konstanz.de)

## 1 Klärung des Begriffs

Die Verknüpfung von administrativem Handeln mit dem Begriff der „Agilität“ wird in der öffentlichen Verwaltung seit dem Beginn der 2000er-Jahre diskutiert. Verbunden ist damit die Vorstellung, dass sich Verwaltungshandeln generell an sich schnell und unerwartet ändernde Umwelten besser anpassen kann. Entsprechend ist ein Kennzeichen von agilen Verwaltungen, dass sie mit agilen (Management-)Methoden geführt bzw. nach betriebswirtschaftlichen Maßstäben organisiert werden. Dies umfasst z.B., verschiedene Problemlösungsansätze auszuprobieren und schnell zu eruieren, was funktioniert und was nicht, sowie gute Lösungen weiterzuverfolgen und schlechte zu erkennen und zu eliminieren.

Anders als im Neuen Steuerungsmodell, beansprucht die agile Verwaltung jedoch keine vollständige Ausrichtung der Verwaltung nach betriebswirtschaftlichen Maßstäben. Die Herausforderung für eine agile Verwaltung liegt vielmehr in der Neubetrachtung von meist standardisierten Prozessabläufen, insbesondere in schwachstrukturierten *Prozessen* im Verwaltungshandeln. Zentraler Aspekt ist dabei eine Neuausrichtung der *Kommunikation*: weg von einer hierarchischen, einseitigen *top-down*-Kommunikation hin zu einer horizontalen, problemorientierten Kommunikation.

Der Begriff der *Agilität* stammt aus der IT-Branche und beschreibt die Beweglichkeit oder Wendigkeit von Personen oder Organisationen. Semantisch ist Agilität nahe am Begriff der Flexibilität angesiedelt, beide Begriffe werden häufig synonym verwendet. Tatsächlich erscheint eine Abgrenzung relativ schwierig. Beide Begriffe bedeuten grundsätzlich „Anpassungsfähigkeit“. Bezieht man sich aber auf die Art der Anpassung des Handelns in der Organisation, wird der Unterschied deutlich. Flexibel wäre demnach eine rein reaktive Anpassung, während agil darüber hinaus bedeutet, proaktiv und initiativ zu agieren, um notwendige Veränderungen durchzuführen. Bezogen auf Organisationen ist Agilität also die Fähigkeit, in Zeiten des Wandels und Unsicherheit flexibel, aktiv, anpassungsfähig und initiativ zu handeln.

Als Organisationsprinzip wurde Agilität zuerst systematisch in der Informations-technologie eingesetzt. Das sogenannte „Agile Manifest in der Softwareentwicklung“ (2001) ist eine Art Handlungsorientierung, nach welchen Prinzipien die Softwareentwicklung gestaltet sein sollte, damit sie als agil zu bezeichnen ist und deren Vorteile tatsächlich zum Tragen kommen. Dieses Manifest umfasst vier zentrale Forderungen: „Individuen und Interaktionen sind mehr als Prozesse und Werkzeuge“, „Funktionierende Software ist mehr als umfassende Dokumentation“, „Zusammenarbeit mit dem Kunden ist mehr als Vertragsverhandlung“ und „Reagieren auf Veränderung ist mehr als das Befolgen eines Plans“ (Agiles Manifest 2001). Anlass für dieses Manifest war die Erfahrung der Software-Industrie in den 1990er-Jahren, dass die Entwicklung von Software, die nach den spezifischen Vorstellungen der Kund\*innen entwickelt wurde, teilweise sehr viel Zeit in Anspruch nahmen. Gleichzeitig gab es aber Abteilungen, die deutlich schneller bei der Software-Entwicklung waren. Die verschiedenen Fachprogrammierer arbeiteten dort in Teams zusammen.

Im Folgenden werden die konzeptionellen Grundlagen der agilen Verwaltung dargestellt und Beispiele vorgestellt, wo es agile Verwaltungen bereits gibt. Darüber

hinaus soll diskutiert werden, welche Hürden die agile Verwaltung zu überwinden hat und welche Rolle die Digitalisierung bei der zukünftigen Entwicklung der agilen öffentlichen Verwaltung spielen könnte.

---

## 2 Konzeptionelle Grundlagen

Die Literatur, die sich mit der agilen Verwaltung beschäftigt, arbeitet in der Regel nicht theoriegeleitet. Allerdings gäbe es zumindest zwei organisationssoziologische Ansätze, die dem Konzept der agilen Verwaltung als theoretische Grundlage dienen könnten. Zum einen die Systemtheorie nach Talcott Parsons (1951), zum anderen das Konzept der lernenden Organisation von Argyris und Schön (1999). Der amerikanische Soziologe Talcott Parsons identifizierte vier Funktionen, die jedes System erfüllen muss, um in der Systemumwelt zu überleben. Er beschreibt dabei die Fähigkeit eines Systems, auf die sich verändernden äußeren Bedingungen zu reagieren (*Adaptation*), Ziele zu definieren und zu verfolgen (*Goal Attainment*), Kohäsion und Inklusion herzustellen und abzusichern (*Integration*) und grundlegende Strukturen und Wertmuster aufrechtzuerhalten (*Latency*). Aus den Anfangsbuchstaben dieser vier Funktionen *Adaption*, *Goal-Attainment*, *Integration* und *Latency* ergibt sich das sogenannte „AGIL-Schema“. Parsons hat dieses strukturfunktionalistische Schema auf soziale Systeme angewandt.

Das AGIL-Schema Parsons ist ein komplexes Modell, das sich auf die gesamte Lebenswelt bezieht. Diese Universalität erlaubt es, das AGIL-Schema auf beliebige Anwendungsbereiche zu übertragen und diese entsprechend zu strukturieren. Tatsächlich gibt es jedoch wenige Beispiele, wo das auch erfolgt ist. Hilfreich bei der theoretischen Fundierung der agilen Verwaltung könnte Parsons AGIL-Schema dennoch sein, weil es sich jeweils um eine grundsätzliche Beschreibung der Flexibilität einer Organisationseinheit hinsichtlich äußerer Veränderungen handelt.

Ein weiterer Ansatz zur theoretischen Einordnung agilen Verwaltungshandelns ist das Konzept der lernenden Organisation nach Argyris und Schön (1999). Lernen bedeutet hier die Veränderung von Handlungsroutinen, deren Grundlagen (Ziele/ Präferenzwandel) und von *Prozessen*, in denen Individuen oder Organisationen Ziele und Routinen bestimmen, überprüfen und bewerten. Ausgehend vom theoretischen Ansatz der lernenden Organisation, der auch in verschiedenen Kontexten der öffentlichen Verwaltung, etwa bei Fragen der Führung und der Personalrekrutierung schon Grundlage von Organisationsveränderungen war, gehören Teamarbeit auf Augenhöhe, Experimentierfreude und Bereitschaft zu Fehlern, sowie frühzeitiges und regelmäßiges *Feedback* zu den wesentlichen Merkmalen agiler Verwaltungen. Teil der lernenden Organisation ist auch, dass sich Organisationshandeln schnell ändern kann, etwa durch *Vernetzung von Teams* und Austausch *in Teams*, sowie die Einbeziehung aller Beteiligten. Weitere Verknüpfungsversuche von Agilität und Organisationstheorien lassen sich bei Förster und Wendler (2013) finden.

Agilität basiert aber meist viel stärker auf bestimmten Managementmethoden. Nach Bartonitz et al. (2018, S. 6 ff.) lassen sich zwölf agile Prinzipien ableiten. Diese sind:

1. Unsere höchste Priorität ist es, den Kunden durch frühe und kontinuierliche Auslieferung unseres Produkts/unserer Dienstleistung zufrieden zu stellen.
2. Heiße Anforderungsänderungen selbst spät in der Entwicklung willkommen. Agile Prozesse nutzen Veränderungen zum Wettbewerbsvorteil des Kunden.
3. Liefere funktionierende Produkte/Dienstleistungen regelmäßig innerhalb weniger Wochen oder Monate und bevorzuge dabei die kürzere Zeitspanne.
4. Lasse Fachleute aus verschiedenen Bereichen während des Projekts täglich zusammenarbeiten.
5. Errichte Projekte rund um motivierte Individuen. Gib Ihnen das Umfeld und die Unterstützung, die sie benötigen, und vertraue darauf, dass sie die Aufgabe erledigen.
6. Die effizienteste und effektivste Methode, Informationen an und innerhalb eines Teams zu übermitteln, ist im Gespräch von Angesicht zu Angesicht gegeben.
7. Funktionierende Dienstleistungen/Produkte sind das wichtigste Fortschrittsmaß.
8. Agile Prozesse fördern nachhaltige Entwicklung. Die Auftraggeber, das Team und die Nutzer der Dienstleistung sollten ein gleichmäßiges Tempo auf unbegrenzte Zeit halten können.
9. Ständiges Augenmerk auf fachliche Exzellenz und gute Gestaltung der Arbeitsabläufe fördert Agilität.
10. Einfachheit – die Kunst, die Menge nicht getaner Arbeit zu maximieren – ist essenziell.
11. Die besten Arbeitsrahmen, Anforderungen und Entwürfe entstehen durch selbst organisierte Teams.
12. In regelmäßigen Abständen reflektiert das Team, wie es effektiver werden kann, und passt sein Verhalten entsprechend an.

Viele Ideen zur Umsetzung agiler Methoden in der Verwaltung beruhen auf der Arbeit von Wernham (2012), einer Ansammlung von Fallbeispielen aus der britischen und US-amerikanischen Verwaltung. Nach Wernham gehören zu den Grundsätzen einer agilen Verwaltung u. a. Aspekte wie Kundenzufriedenheit, Vertrauen zu gewinnen, eine *Face-to-Face*-Arbeitsweise, Raum, im Sinne von Möglichkeiten zur Teamarbeit. Ein *Whitepaper* von Bearing Point (2013) beschäftigte sich ebenfalls mit der agilen Verwaltung. Danach führen einzelne Bausteine allein in der Regel nicht unbedingt zu einer höheren Agilität. Erst das Zusammenwirken vieler unterschiedlicher Bausteine bewirkt den gewünschten positiven Effekt. Bearing Point identifizierte fünf Hebel, an denen anzusetzen ist, um die Verwaltung agiler zu machen. Diese sind:

- strategische Steuerung und Ressourcenmanagement,
- flexible und adaptive Organisationsstrukturen,
- strategisches Personalmanagement,
- anpassungsfähige und kundenorientierte IT,
- Kultur und Wandlungsfähigkeit.

Kernelement der agilen Verwaltung ist das Anliegen, ein Denken in Zuständigkeiten oder Sachgebieten aufzugeben; stattdessen sollen behördenübergreifende Vorgangsteams (*Arenen*) gebildet werden, die regelmäßig miteinander kommunizieren und die entsprechend für die fristgerechte Durchführung des Vorhabens verant-

wortlich sind. Arenen entstehen auf Antrag eines Mitarbeiters bzw. einer Mitarbeiterin. Dafür gibt es drei Voraussetzungen. Die Arena wird nur dann gebildet, wenn ein explizites Bürgerbedürfnis besteht; d. h. sie werden nicht für interne Organisationsaufgaben gebildet, sondern nur im Rahmen der Kernprozesse. Bedingung ist, dass die Organisation ein Problem gemeldet hat („Signal“), das die einzelne Abteilung nicht allein lösen kann. Als zweite Bedingung ist Kooperation notwendig, die über Sachgebiete oder Abteilungen hinausgeht. Dritte und letzte Bedingung ist der überschaubare Zeitraum der Lösungsfindung für ein Problem. Dieses Problem sollte in drei bis fünf Arenasitzungen gelöst werden. Sind diese Bedingungen erfüllt, bildet sich ein Arena-Team mit Mitarbeiter\*innen der Verwaltung und Expert\*innen außerhalb der Verwaltung. Moderiert und geleitet werden diese Arenen von zwei Prozessmoderator\*innen. Entscheidungen werden in den Arenen durch Konsens hergestellt. Die entscheidende Frage ist, ob und wenn ja welche Einwände es gegen einen vorliegenden Vorschlag gibt. Dieses Vorgehen erlaubt es dann, die sachliche Kritik mit dem Ziel einzuarbeiten, den vorliegenden Vorschlag zu verbessern. Die Ergebnisse werden in einer Datenbank festgehalten, um so für künftige Arenen hilfreiche Anregungen zu erhalten.

Eine zentrale Arbeitsmethode in der agilen Verwaltung heißt „scrum“. Dabei wird zu jedem Vorgang ein Umsetzungsteam gebildet, das sich selbstständig bestimmte *Sprints* (Zeitintervalle) zur Bearbeitung der Vorgänge setzt. Ein Sprint besteht wiederum aus vier Elementen: *Sprint Planning*, *Daily Scrums*, *Sprint Review* und *Sprint Retrospektive*. Im *Sprint Planning* plant das Team den nächsten Sprint. Dabei werden die Anforderungen in konkrete Aufgaben (*Tasks*) zerlegt, die innerhalb eines Tages bearbeitet werden können. Zu Beginn eines jeden Arbeitstages trifft sich das Team zu einem rund viertelstündigen Meeting, dem *Daily Scrum*. So wird einmal am Tag der direkte *Face-to-face*-Austausch mit allen Teammitgliedern gewährleistet. Jedes Teammitglied erläutert kurz, was seit dem letzten Meeting erledigt wurde, was bis zum nächsten Meeting geplant wird und welche Probleme die weiteren Schritte behindern können. Am Ende eines jeden Sprints wird im Rahmen des *Sprint Review* ein funktionsfähiges Produkt (*Done*) dem Auftraggeber (*Product Owner*) vorgelegt. Seine Rückmeldungen dazu bilden die Grundlage weiterer Überarbeitungen. In den anschließenden *Sprint Retrospective* wird die Arbeit des Projektteams überprüft, um sie kontinuierlich zu verbessern. Die Prinzipien lauten: Planen – Prüfen – Anpassen und „Experimentieren statt streiten“ (vgl. Lévesque und Steinbrecher 2017).

Neben dem Mangel an theorieorientierter Literatur fehlt es auch an grundlegender Literatur zur agilen Verwaltung selbst. Am grundlegendsten mit der agilen Verwaltung beschäftigten sich die Beiträge von Hill (2015, 2018), der Agilität als (neues) Paradigma der Verwaltung bezeichnet. Nach Hill (2015, S. 405) verfolgen alle agilen Methoden im weiteren Sinne folgende Grundgedanken:

- Handlungen werden nicht von Konzeptionen getrennt, Kontrolle erfolgt nicht im Nachhinein, sondern integriert.
- Das experimentelle und iterative Vorgehen erlaubt eine schnellere Reaktionsfähigkeit, besser angepasste und funktionsfähige Lösungen sowie größere Kundenzufriedenheit.

- Rückkoppelungs- und Austauschprozesse erweitern die gemeinsame Wahrnehmung und steigern den Realitätsgehalt und die Wirksamkeit.
- Die interdisziplinäre Zusammenarbeit in Teams erhöht die Expertise, erlaubt wechselnde Rollen und stärkt Motivation und *Commitment*.
- Durch Konzentration auf tatsächliche und aktuelle Bedürfnisse der Auftraggeber/Kunden entstehen geringere Kosten und eine geringere Gesamtaufzeit.

---

### 3 Praktische Anwendung

Die erste und bislang einzige Stadt in Europa, die eine Verwaltung hat, die explizit agil arbeitet, ist die knapp 40.000-Einwohner-Stadt Ängelholm. Ängelholm liegt am Öresund, an der Westküste Schwedens, zwischen Malmö und Göteborg. Nach dem Beginn eines Organisationsentwicklungsprojekts im Jahre 2013 stellte zu Beginn des Jahres 2015 Ängelholm seine Verwaltung mit ihren knapp 3000 Mitarbeiter\*innen vollständig auf Agilität um. Als Projektziele wurden festgehalten: Eine klare Ausrichtung auf die Bürger\*innen, eine verbesserte Zusammenarbeit und gegenseitige Achtsamkeit zwischen den Mitarbeiter\*innen und eine hohe Beteiligung von ihnen an der Prozessgestaltung (vgl. Steinbrecher 2018, S. 222). Zu Beginn wurde ein *Call-Center* – vergleichbar den deutschen Bürgerbüros – eingerichtet. Allerdings erledigt dieses *Call-Center* mit seinen rund 60 Mitarbeiter\*innen rund 70 Prozent aller Bürgerkontakte abschließend, also deutlich mehr als in vielen deutschen Bürgerbüros. Diese 70 Prozent umfassen im Wesentlichen die normale Antragsbearbeitung von klassischen Verwaltungsvorgängen, wie beispielsweise das Pass- und Meldewesen. Bei den restlichen 30 Prozent der Bürgeranliegen können sich die Sachbearbeiter auf die ‚komplexeren‘ Bereiche ihrer Arbeit im *Back-Office* konzentrieren. Insofern unterscheidet sich Ängelholm nicht von zahlreichen deutschen Kommunalverwaltungen.

Neu in der agilen Verwaltung ist die Einrichtung der bereits beschriebenen Arenen als ein Kernstück agiler Verwaltungsarbeit. Diese Arenen – konzipiert als temporäre, cross-funktionale Arbeitsgruppen – arbeiten in Ängelholm zurzeit in drei Themenbereichen: Bildung und Familie, Gesundheit und Soziale Entwicklung. Dabei werden die betroffenen Bürger\*innen direkt in die Entscheidungsprozesse miteinbezogen. Jede Arena wird von zwei Prozesssteuerer\*innen begleitet, die diese Tätigkeit neben ihrer normalen Sachbearbeitung erledigen.

Wie Steinbrecher (2018) betont, hat die agile Verwaltungsarbeit in Ängelholm die klassische nicht abgelöst, sondern ergänzt. Es stellt sich nun vielmehr jeweils die Frage, mit welchem der beiden Arbeitsweisen einem Problem sachgerecht begegnet wird. Insofern hilft die agile Verwaltungsarbeit den Mitarbeiter\*innen der Stadtverwaltung dabei, ihre eigene Arbeit zu reflektieren. Empirische Evaluationsberichte gibt es bislang noch nicht, lediglich ein paar Hinweise. So erfreut sich die Kommunalverwaltung offensichtlich einer relativ großen Beliebtheit bei Mitarbeiter\*innen, die sich aus ganz Schweden dort bewerben. Genaue Zahlen sind jedoch nicht veröffentlicht.

In Deutschland gibt es bislang keine öffentliche Verwaltung, die vollständig agil arbeitet. Auf Bundes- oder Länderebene spielt die agile Verwaltung bislang noch keine Rolle. Seit 2016 gibt es aber erste Versuche, Kommunalverwaltungen mit agilen Arbeitsmethoden teilweise neu zu strukturieren. Neben der Hochschule der Medien in Stuttgart spielt das Anfang 2016 in Karlsruhe gegründete „Forum Agile Verwaltung“ dabei eine wesentliche Rolle. Es versteht sich selbst als Austausch- und Experimentierplattform ohne kommerzielles Interesse, das sich zum Ziel gesetzt hat, die Verwaltung für die Kultur der Agilität zu öffnen – und umgekehrt. Sie fassen auf ihrer *Homepage* (<https://agile-verwaltung.org/>) die zentralen Merkmale der agilen Verwaltung kurz und knapp folgendermaßen zusammen: Das Ganze in den Blick nehmen, „cross-funktionale“ Teams bilden, die Anspruchsgruppen einbeziehen, mit überschaubaren Änderungen und Teilergebnissen experimentieren, regelmäßiges *Feedback* von innen und außen verschaffen und das System so wieder besser bzw. angemessener machen.

Die Stadt Karlsruhe ist einer der Vorreiter innerhalb der Städte und Kommunen Deutschlands. Die strukturellen Veränderungen der dortigen Stadtverwaltung lassen sich in groben Zügen wie folgt darstellen: Neben der bestehenden Dezernatsstruktur wurde dabei ergänzend eine themenorientierte Querstruktur anhand sogenannter Korridorthemen eingerichtet. Die Korridorthemen wurden mit Strategiezielen, Strategien und Leitprojekten verknüpft, für die jeweils ein(e) Dezernent\*in verantwortlich ist. Die jeweiligen Leitprojekte werden von fachübergreifenden Arbeitsgruppen bearbeitet, welche eine Stabsstelle koordiniert. Die traditionelle Verwaltungsarbeit bleibt – vergleichbar in Ängelholm – davon unberührt; eine gewisse Vorbildwirkung und Lerneffekte sind jedoch beabsichtigt. Mitte des Jahres 2018 hat sich außerdem das Netzwerk „#ANDI – Agiles Netzwerk Digitale Innovation“ gegründet. Dies besteht aus Vertreter\*innen der Städte Karlsruhe, Mannheim, Freiburg, Konstanz und der Metropolregion Rhein-Neckar. Erst Ansätze der Installation agiler Verwaltungselemente sind auch auf Bundesebene zu beobachten, so etwa bei der Deutschen Gesellschaft für Internationale Zusammenarbeit (GIZ) und der Bundeswehr. Dort wurde mit dem *Cyber Innovation Hub* eine Einheit gegründet, die mittels agiler Methoden die Innovationsfähigkeit der Bundeswehr erhöhen soll.

Noch fehlt es empirischer Forschung zur Wirksamkeit der agilen Verwaltung. Ein erster Schritt dahin ist der Beitrag von Richenhagen (2018). Er untersucht den Zusammenhang des erhöhten Krankenstandes in der öffentlichen Verwaltung und einer agilen Verwaltung bzw. genauer gesagt, inwiefern das Fehlzeitengeschehen in der öffentlichen Verwaltung durch zukünftige Entwicklungen hin zur agilen Verwaltung beeinflusst werden könnte. Allerdings verfügt Richenhagen nur über Aggregatdaten des Bundes bzw. der AOK zu den Fehlzeiten und kann so zu den individuellen Ursachen der Fehlzeiten keine Angaben machen. Seiner These nach werden die Mitarbeiter\*innen in der agilen öffentlichen Verwaltung weniger Fehlzeiten haben, weil sie durch ein Mehr an Eigenverantwortung und Motivation in der agilen Verwaltung mehr gesundheitliche Ressourcen und eine verbesserte Beschäftigungssituation vorfinden. Dies kann dabei helfen, die negativen Merkmale im Bereich von Arbeitsinhalt und Arbeitsorganisation kognitiv, emotional und aktiv handelnd aus-

zugleichen. Weitere empirische Forschung ist an dieser Stelle von Nöten, um wirkliche messbare Erfolge des agilen Verwaltungshandeln zu belegen.

---

## 4 Hürden für die agile Verwaltung

Was hemmt die Verwaltung agiler zu werden? Gibt es Grenzen, die der Verwaltung immanent sind, welche Agilität einschränken bzw. nur schwer umsetzbar machen? Hill (2018, 2015) sieht verschiedene Hindernisse, welche die öffentliche Verwaltung daran hindert, eine Neuausrichtung hin zu einer agilen Verwaltung durchzuführen. Demnach sind es weniger die rechtlichen Rahmenbedingungen, sondern eher die kulturellen Rahmenbedingungen der Verwaltung in Deutschland: So steht die legalistische *Verwaltungskultur*, das Denken in Zuständigkeiten einem ganzheitlichen Denken und Handeln sowie Innovationen und damit auch agilem Handeln im Weg. So sind in der Verwaltungspraxis durchaus Spielräume vorhanden, die agiles Verwalten strukturell möglich machen, wie etwa das Entscheidungsermessens im weiteren Sinne. Auch das deutsche Verwaltungsverfahrensrecht gibt einen rechtlichen Spielraum für agiles Verwaltungshandeln. Dieses ist geprägt vom Grundsatz der Nichtförmlichkeit, d. h. die Verfahren müssen einfach und zweckmäßig sein. Ein Beispiel dafür, wie Verwaltung in veränderten Realitäten in der komplexen Umwelt von Bürokratien handeln kann, ist das informelle Verwaltungshandeln.

Den Bezug auf fehlende Bereitschaft zum riskanten Handeln bzw. auf den Zusammenhang zwischen Agilität und Sicherheit stellt Hill (2015, S. 140) her. Weil der Mensch sich Sicherheit wünscht, versucht er die Erfolge seiner Agilität abzusichern. Daraus entsteht Trägheit, also das Gegenteil von Agilität. Demnach folgt die Trägheit der Verwaltung aus deren Sicherheit und Kontinuität. Die agile Verwaltung will diese Trägheit überwinden. Die Risikoaversion der Mitarbeiter\*innen, deren häufig fehlendes unternehmerisches Denken sowie die mangelnde Unterstützung durch die Führungsebenen der Verwaltung und das Fehlen einer positiven Fehlerkultur sind ausschlaggebende Gründe, die Verwaltungen darin hindern agil(er) zu werden. Ein agiles (Verwaltungs-)Management müsse sich entsprechend darum bemühen, die Agilität selbst abzusichern und nicht die Ergebnisse der Agilität.

Die Umsetzung einer agilen Verwaltung steht und fällt jedoch mit der Mitwirkung von hochqualifiziertem und -motiviertem Personal. Die Mitarbeiter\*innen müssen dazu bereit sein, das Silo-Denken in Zuständigkeiten und Abteilungsgrenzen zu überwinden und stattdessen umfassender mit anderen Akteuren innerhalb *und* außerhalb der Verwaltung zusammenzuarbeiten. Insbesondere ein Generationenwechsel in der öffentlichen Verwaltung, dessen zukünftige Mitarbeiter\*innen weniger in Hierarchien, sondern vernetzt denken, um innovative Lösungen für die anstehenden Probleme zu finden, könnte das Handeln in der Verwaltung agiler machen. Dazu ist wiederum ein Umdenken von Nöten, hin zu einem strategischen Personalmanagement, insbesondere auch bei der Rekrutierung neuen Personals. Dies ist vor allem unter dem Gesichtspunkt, welche Typen von Mitarbeiter\*innen die Verwaltung anzieht, relevant. Erkenntnisse aus der *Public Service-Motivation*-Forschung können hierbei hilfreich sein.

## 5 Perspektiven für Staat und Verwaltung

Die Zunahme an Komplexität und Dynamik in ihrer Umwelt gefährdet zunehmend das rechtlich eindeutige Handeln der öffentlichen Verwaltung (vgl. Hill 2015). Für das Management von großen Infrastrukturprojekten oder anderer Vorhaben scheint die klassische funktional-hierarchische Organisation der Verwaltung, sowohl in Krisenzeiten aber auch im Hinblick auf Innovationen, zu schwerfällig zu sein. Insofern ist der gesellschaftliche Erwartungsdruck, Verwaltungshandeln in Teilen neu zu organisieren, relativ groß.

Kann die agile Verwaltung diese Erwartungen erfüllen? Ist es ein neues Paradigma des Verwaltungshandelns oder „nur“ eine Chance für ein wirksameres Verwaltungshandeln? Könnte die Digitalisierung möglicherweise ein *Push*-Faktor sein die Verwaltung agiler zu machen? Wie könnte es weiter gehen mit der agilen Verwaltung in Deutschland?

Der Digitalisierung kommt bei der Entwicklung der öffentlichen Verwaltung zu mehr Agilität eine Schlüsselrolle zu. Insbesondere hinsichtlich der *Kommunikation* kann die Digitalisierung die Entwicklung der öffentlichen Verwaltung zu mehr Agilität unterstützen. Sowohl die Kommunikation zwischen Strukturen bzw. bei *Prozessen* innerhalb der Verwaltung als auch die Kommunikation zur Zivilgesellschaft, hin zu einer partizipativen Verwaltung, welche im Dialog mit den Bürger\*innen problemorientiert handelt, kann digitalisiert stattfinden. Allein die Tatsache, dass die Digitalisierung, z. B. in Form der E-Akte, es möglich macht, dass mehrere Beteiligte zur gleichen Zeit ortsunabhängig auf die gleiche Akte zugreifen können, ist eine Grundvoraussetzung agiler Verwaltungsarbeit. Die Digitalisierung kann aber beispielweise auch bei der Bildung der Arenen durch digitale Medien helfen, die entsprechenden Akteure innerhalb und außerhalb „an einen Tisch“ zu bringen. Dies setzt aber voraus, dass die Verwaltung mit einer entsprechend leistungsfähigen IT ausgestattet ist, was in Deutschland häufig nicht der Fall ist. Vielmehr ist aufgrund einer wachsenden Innovationslücke zwischen Verwaltung und Gesellschaft eine digitale Spaltung entstanden, die durch Entwicklungen der Verwaltung hin zu mehr Agilität möglicherweise in Teilen geschlossen werden könnte. Gleichwohl bleibt die *Face-to-face*-Kommunikation innerhalb der Treffen der Arenen die wichtigere Form der Kommunikation in der agilen Verwaltung.

Angesichts der Beharrungstendenzen der öffentlichen Verwaltung, insbesondere in Deutschland, bleibt abzuwarten, ob es der agilen Verwaltung gelingt, sich zu einem dominierenden Konzept im Verwaltungshandeln zu entwickeln. Eine komplette Umstellung bewährter Verwaltungsstrukturen auf allen Ebenen ist sicher nicht sinnvoll, darin sind sich Förderer wie Kritiker des Konzepts einig. So ist zu vermuten, dass es weiterhin weite Bereiche innerhalb der Verwaltung geben wird, die im Sinne des klassischen Weberschen Ideals geführt werden, weil sie sich zur Erledigung von standardisierten und stark strukturierten Daueraufgaben, wie beispielsweise im Passamt, als effektive Routinen von Verwaltungshandeln erwiesen haben. Hier kann die Digitalisierung Verwaltungsabläufe beschleunigen, diese müssen aber nicht agil sein.

Eine agile Verwaltung versucht durch die *Vernetzung* unterschiedlicher Fachbereiche über Organisationsgrenzen hinweg, durch mehr Beteiligung und durch die frühzeitige

Einbindung relevanter Akteure aus der Verwaltung und der Zivilgesellschaft einen qualitativ besseren Verwaltungsauftrag zu erzeugen. Dies ist der Versuch, neue Agilitäts-elemente wie zielführende Arbeitsstrukturen, schnelle Zielanpassung und Ressourcensteuerung in bestehende Systeme der öffentlichen Verwaltung zu integrieren. All diese Elemente bedürfen auch einer stetigen Veränderung der *Verwaltungskultur*. Veränderungen müssen eine gewisse Eigendynamik erzeugen, die das Verhalten der Führungskräfte und der Mitarbeiter\*innen ändert. Ansonsten ist es sehr wahrscheinlich, dass Agilität nicht auf dem Weg zu einem neuen Paradigma des Verwaltungshandelns ist, sondern irgendwann als ein populäres *buzzword* endet.

Vielelleicht stellt die agile Verwaltung eher ein Prinzip für die Zukunft dar, Wege zu finden, traditionelles Vorgehen mit agilen Ansätzen zu kombinieren und Agilität selbst umzusetzen und weiterzuentwickeln. Der Agilität ist selbst immanent, dass sie nie abgeschlossen ist. Nach Hill (2015, S. 410) besteht die zentrale Herausforderung der Organisation einer agilen Verwaltung im „richtigen Verhältnis von Agilität und Flexibilität zur Stabilität und Trägheit“. Diesem Spannungsverhältnis zu begegnen, stellt eine der zentralen Herausforderungen für die Zukunftsfähigkeit des Konzepts der agilen Verwaltung dar.

---

## Literatur

- Agiles Manifest. 2001. *Manifest für Agile Softwareentwicklung*. <https://agilemanifesto.org/iso/de/manifesto.html>. Zugriffen am 18.12.2019.
- Argyris, Chris, und Donald A. Schön. 1999. *Die lernende Organisation. Grundlagen, Methoden, Praxis*. Stuttgart: Klett-Cotta.
- Bartonitz, Martin. 2018. In *Agile Verwaltung. Wie der Öffentliche Dienst aus der Gegenwart die Zukunft entwickeln kann*, Hrsg. Veronika Lévesque, Thomas Michl, Wolf Steinbrecher, Cornelia Vonhof und Ludger Wagner. Berlin: Springer Gabler.
- Bearing Point. 2013. *Fünf Hebel für eine agile Verwaltung*. <https://www.bearingpoint.com/de-de/unser-erfolg/insights/fuenf-hebel-fuer-eine-agile-verwaltung/>. Zugriffen am 18.12.2019.
- Förster, Kerstin, und Roy Wendler. 2013. *Theorien und Konzepte zu Agilität in Organisationen*, Dresden Beiträge zur Wirtschaftsinformatik 63/12. Dresden: Fakultät Wirtschaftswissenschaften. <http://www.nbn-resolving.de/urn:nbn:de:bsz:14-qucosa-129603>. Zugriffen am 18.12.2019.
- Hill, Hermann. 2015. Wirksam verwalten – Agilität als Paradigma der Veränderung. *Verwaltung Archiv* 106(4): 397–416.
- Hill, Hermann. 2018. Agiles Verwaltungshandeln im Rechtsstaat. *DÖV* 13:497–504.
- Lévesque, Veronika, und Wolfgang Steinbrecher. 2017. Agile Arbeitsmethoden in der öffentlichen Verwaltung. *Innovative Verwaltung* 5:28–30.
- Parsons, Talcott. 1951. *The social system*. London: Routledge.
- Richenhagen, Gottfried. 2018. Erhöhte Krankenstände in der öffentlichen Verwaltung – Ein Erklärungsversuch mit einem Ausblick auf die agile Verwaltung. In *Gesundheit und Arbeit 4.0 – Wenn Digitalisierung auf Mitarbeitergesundheit trifft*, Hrsg. David Matusiewicz, Volker Nürnberg und Stephanie Nobis. Heidelberg: medhochzwei.
- Steinbrecher, Wolf. 2018. Agilisierung einer kommunalen Verwaltung – das Beispiel Ängelholm (Schweden). In *Agile Verwaltung. Wie der Öffentliche Dienst aus der Gegenwart die Zukunft entwickeln kann*, Hrsg. Martin Bartonitz, Veronika Lévesque, Thomas Michl, Wolf Steinbrecher, Cornelia Vonhof und Ludger Wagner, 221–234. Berlin: Springer Gabler.
- Wernham, Brian. 2012. *Agile project management for Government*. London: Maitland & Strong.



---

# Digitale Kommunikationsinfrastrukturen

Jeanette Hofmann

## Inhalt

1 Klärung des Begriffs .....	148
2 Theoretische Grundlagen .....	148
3 Geschichte der digitalen Infrastruktur .....	150
4 Staatliche Regulierung digitaler Infrastruktur .....	153
5 Perspektiven .....	155
Literatur .....	157

---

## Zusammenfassung

Infrastrukturen sind räumliche und zeitliche Integrationsmaschinen, die zur Expansion neigen. Durch die Normalisierung von Leistungen und Nutzungsweisen tragen sie in unsichtbarer Weise maßgeblich zur Stabilität gesellschaftlicher Ordnung bei. Je umfassender Infrastrukturen das öffentliche und private Leben koordinieren und optimieren, desto größer wird die Anfälligkeit gegenüber Zusammenbrüchen. Die Digitalisierung steigert das Verhältnis zwischen Wohlfahrtsgewinn und Verletzlichkeit, indem sie die Integration der Infrastrukturen vorantreibt und neue Machtstrukturen ermöglicht.

---

## Schlüsselwörter

Verletzlichkeitsparadox · Netzneutralität · Kommunikationsnetze · Interkonnektivität · Plattformen

---

J. Hofmann (✉)

Politik der Digitalisierung, Wissenschaftszentrum Berlin für Sozialforschung, Berlin, Deutschland  
E-Mail: [jeanette.hofmann@wzb.eu](mailto:jeanette.hofmann@wzb.eu)

## 1 Klärung des Begriffs

Der im Französischen entstandene Begriff Infrastruktur stammt aus dem späten 19. Jahrhundert und bezieht sich ursprünglich auf die Konstruktion von Eisenbahnen, genauer auf den für ihren Betrieb erforderlichen ‚Unterbau‘. Die allgemeine Idee einer unterliegenden Struktur, die darüber liegende Transport- und Organisationsleistungen ermöglicht, kennzeichnet das Verständnis von Infrastrukturen bis heute. Eine einheitliche Definition von Infrastrukturen hat sich bislang nicht durchsetzen können. Aus wirtschaftswissenschaftlicher Sicht handelt es sich um „shared means for many ends“ (Frischmann 2012, S. 4–5), die erhebliche gesellschaftliche Wohlfahrtsgewinne (positive Externalitäten) hervorbringen, sofern sie diskriminierungsfrei für jedermann zur Verfügung gestellt werden. Demnach stellen Infrastrukturen Beziehungen zwischen Dingen her, als Voraussetzung für die verlässliche Organisation von Bewegung und Zirkulation über größere räumliche Distanzen. Dies ermöglicht wiederum die Herstellung und Verbreitung einer Vielzahl von Gütern und Dienstleistungen. Neue Wortschöpfungen wie die ‚Daten-‘ oder ‚Cloud-Infrastruktur‘ signalisieren, dass das Konzept auch in digitalen Kontexten Vorstellungskraft erzeugt.

Die Ausbreitung des Begriffs begann in den 1950er-Jahren, als er zunächst in den militärischen Sprachgebrauch der NATO einwanderte. Das ‚Infrastruktur-Programm‘ zielte auf den Ausbau und die Standardisierung militärischer Anlagen. Als neues Modewort eroberte er dann in den 1960er-Jahren das staatliche Planungswesen, das mit dem Aufbau von Transport- und Kommunikationssystemen, aber auch mit der Bereitstellung von Bildungs-, Gesundheits- und Kultureinrichtungen befasst war. Seit dieser Zeit ist der Begriff positiv aufgeladen: Mit dem Ausbau von Infrastrukturen werden Zivilisation, Modernität, Wohlstand und Fortschritt assoziiert, aber auch die Normalisierung von Leistungen und Nutzungsweisen, die einen wesentlichen Anteil an der Stabilität gesellschaftlicher Organisation haben. Spezifische Metriken erlauben den Vergleich infrastruktureller Versorgungsniveaus zwischen der Ersten und der Dritten Welt, zwischen Stadt und Land oder Nord und Süd. Am Beispiel des Internets zeigt sich, welch umfassende gesellschaftliche Umwälzungsprozesse Infrastrukturen auslösen können.

---

## 2 Theoretische Grundlagen

Infrastrukturen zeichnen sich durch ein besonderes Verhältnis von Sichtbarkeit und Unsichtbarkeit aus. Einerseits genießen sie einen hohen symbolischen Stellenwert, der sich in der repräsentativen Architektur von Bahnhöfen, Fernsehtürmen und Prachtstraßen ausdrückt. Andererseits verschmelzen sie so nahtlos mit den Alltagsroutinen ihrer Nutzer\*innen, dass sie kaum wahrgenommen werden. Erst das Nicht-Funktionieren und der Unfall lassen ihre existenzielle Bedeutung, ihre Funktionslogik und Bedingtheit plötzlich ins Bewusstsein treten. Schneestürme oder Computerviren können nicht nur das öffentliche Leben zum Erliegen bringen, sie führen uns auch vor, wie stark Infrastrukturen untereinander verwoben sind. Van Laak (2017, S. 11) spricht

in diesem Zusammenhang von einem „Verletzlichkeitsparadox“: Je umfassender und verlässlicher Infrastrukturen unseren Alltag organisieren, desto drastischer sind die Folgen ihres Zusammenbruchs. Dieser Einsicht verdankt sich die Kategorie der ‚kritischen Infrastrukturen‘, die zu besonderen Schutzmaßnahmen für Infrastrukturen mit großer Bedeutung für das öffentliche Leben verpflichtet.

Infrastrukturen lassen sich als (freilich selektive) gesellschaftliche Integrationsmaschinen mit einer sich tendenziell ausdehnenden zeitlichen und räumlichen Reichweite verstehen. Im Prinzip ermöglichen Kommunikationsnetze wie das Internet einen friktionslosen Austausch rund um den Erdball; und sie strukturieren diesen Austausch zugleich. Infrastrukturen, so Larkin (2013), ähneln einer Sprache, die man sich aneignet. Diese Sprache umfasst nicht nur die grammatischen Regeln der Nutzung, sondern auch ein Gespür für die Handlungsmöglichkeiten, die sie eröffnen. Bemerkenswerterweise erzielen Infrastrukturen solche Wirkungen in dem Maße, in dem sie Teil von Alltagsroutinen werden und im kollektiven Unbewussten agieren. Von Infrastrukturen kann man eigentlich erst sprechen, so van Laak (2017), wenn sie selbstverständlich geworden sind. Aus dieser Beobachtung ergibt sich ein wichtiger Hinweis auf ihre Beschaffenheit. Infrastrukturen lassen sich demnach nicht auf ihre materiell-technische und funktionale Dimension reduzieren; ihre strukturelle Bedeutung erschließt sich erst, wenn man sie als Amalgam betrachtet, das neben ihrer materiellen Form auch politische Steuerungsabsichten, gesellschaftliche Konventionen sowie Anschlüsse an weitere Infrastrukturen umfasst.

Auch wenn die staatliche Planung und Finanzierung eine wichtige Rolle im Ausbau von Infrastrukturen spielt, vollzieht sich ihre Entstehung und Expansion doch eher ungeplant. So geht das Internet auf eine Vielzahl unkoordinierter Initiativen zurück, die darauf zielten, die wachsende Anzahl von Großrechnern in Wissenschaft und Wirtschaft miteinander zu vernetzen. Zur Infrastruktur werden solche lokalen Experimente erst, wenn es einer ihrer Varianten gelingt, sich als akzeptierter Standard zu etablieren, an dem sich alle weiteren Ausbauprojekte orientieren müssen. Nicht zuletzt deshalb ist ihre Entstehungsgeschichte voller Auseinandersetzungen. Das Design wie auch die Funktionen von Infrastrukturen sind selten alternativlos. Zudem erfordern die verfügbaren Optionen häufig Abwägungen zwischen verschiedenen Gütekriterien: Die schnelle Lösung ist unter Umständen weniger flexibel oder die sichere Lösung schließt bestimmte Anwendungen aus. Entsprechend formieren sich in den frühen Tagen einer Infrastruktur Machtkämpfe um technische, wirtschaftliche und politische Richtungsentscheidungen, die sich dann als verschüttete Zeitgeschichte in ihrem Design sedimentieren.

Obwohl Infrastrukturen den Anschein von Stabilität erwecken, sind sie doch beständig in Bewegung. Die ökonomische Theorie der Netzwerkeffekte besagt, dass der Wert einer Infrastruktur wie etwa das Telefonnetz mit der Anzahl verbundener Menschen und Objekte steigt (Katz und Shapiro 1986). Von expandierenden Infrastrukturen geht daher ein mehr oder minder zwangloser Anschlusszwang aus. Wenn sich der Flug nur noch über das Internet und das Hotelzimmer nur mit einer Kreditkarte buchen lassen, dann führt die Nicht-Nutzung zu individuellen Nachteilen und Marginalisierungserfahrungen. Allerdings können Infrastrukturen auch stagnieren oder schrumpfen. Außerhalb der regionalen Ballungsräume in Deutschland

lässt sich seit langem beobachten, dass Schulen, Bibliotheken und Geschäfte wieder schließen und somit ihren Status des Selbstverständlichen verlieren. Auch beim Breitbandausbau, dem große wirtschaftliche und gesellschaftliche Bedeutung beigemessen wird, zeigen sich große nationale und regionale Unterschiede.

Die Entstehung und Entwicklung von Infrastrukturen sind Gegenstand der politischen Regulierung. Daher wirkt sich der Wandel gesellschafts- und wirtschaftspolitischer Großwetterlagen unmittelbar auf ihre Gestaltung aus. Bis in die 1980er-Jahre galt der Betrieb von Infrastrukturen in Deutschland überwiegend als staatliche Aufgabe. Der Ausbau von Transportsystemen und Kommunikationsnetzen orientierte sich an dem im Grundgesetz verankerten Ziel der „Einheitlichkeit“ und ab 1994 der „Gleichwertigkeit“ von Lebensverhältnissen in Deutschland. In den letzten Jahrzehnten sind viele Infrastrukturen privatisiert und ihr Ausbau und Betrieb dem Markt überantwortet worden. Das hat Folgen für die Zugangsbedingungen (Graham 2010). So besteht in Deutschland zwar ein Rechtsanspruch auf einen Telekommunikationsanschluss, der privatwirtschaftliche Ausbau des Glasfasernetzes fällt dagegen nicht in den Bereich der Grundversorgung.

Die Untersuchung von Infrastrukturen ist keine leichte Aufgabe. Je geräuschloser sie funktionieren und je größer sie sind, desto schwerer ist es, sie in den Blick zu nehmen (Bowker und Star 1999). Zudem entstehen neue Infrastrukturen, die die gesamte Gesellschaft durchdringen und nicht mehr wegzudenken sind, relativ selten. Das Internet verkörpert eine dieser raren Entwicklungen, die sich bis heute vor unseren Augen vollzieht. Im Folgenden wird ein kurzer Abriss über die Geschichte und Funktionsweise des Netzes gegeben, an den sich die Beschreibung seiner privaten und staatlichen Regulierung anschließt.

---

### 3 Geschichte der digitalen Infrastruktur

Die Durchsetzung des Internets war ein recht unwahrscheinliches Ereignis. Noch in den frühen 1990er-Jahren galt das Internet als akademisches Spielzeug, das bald durch ein besseres, international förmlich vereinbartes und nationalstaatlich betriebenes Datennetz ersetzt werden würde. Dem voraus ging die Entstehung von Datennetzen in den 1970er-Jahren, als große Computerhersteller wie IBM und DEC eigene Netzarchitekturen entwickelten, die jedoch nur unter größtem Aufwand miteinander interagieren konnten. Die Lösung für das Problem inkompatibler Technologien besteht in der Einigung auf herstellerübergreifende Normen. Kommunikationsinfrastrukturen wie das Telefonnetz oder die Briefpost sind ohne internationale Standards gar nicht denkbar. Allerdings sind technische Normsetzungsprozesse häufig langwierig und konfliktbeladen, weil sich Wettbewerber auf eine Vorgehensweise einigen müssen, die im Verdacht steht, Gewinner und Verlierer bzw. große und kleine Marktanteile zu produzieren.

In den 1970er-Jahren war vollkommen offen, wie ein universales Datennetz beschaffen sein würde. Unklar war zudem, welche Organisation ausreichend Definitions- und Marktmacht mobilisieren könnte, um eine weltweit anerkannte Architektur für Datennetze zu etablieren. Zwei Akteursgruppen konkurrierten ab den

1980er-Jahren um die Definitionshoheit über den künftigen Datenverkehr: die überwiegend staatlich organisierten Telefongesellschaften und die aufstrebende Computerindustrie (Abbate 1999).

Die staatlichen Telefongesellschaften planten ein international einheitliches, von den nationalen Postbehörden betriebenes öffentliches Datennetz mit einem zentral definierten Katalog von Anwendungen. Das Gegenmodell zielt auf ein *inter net*, das die Vielzahl bereits bestehender Netze miteinander verbinden sollte. Im Vordergrund stand hier die Interkonnektivität, um die babylonische Vielfalt im Datenverkehr zu überwinden. Während das Modell des öffentlichen Datennetzes eine zentrale Qualitätskontrolle von Netzbetrieb und Datenflüssen vorsah, beschränkte sich das Konzept des Netzes der Netze auf minimale Designanforderungen wie die folgende: „be conservative in what you do, be liberal in what you accept from others“ (Postel 1980, S. 13). Diesem Verzicht auf eine hierarchische Netzarchitektur hat man später die außerordentliche Innovationsdynamik des Internets zugeschrieben.

Wie hat sich das Internet gegen die politische Macht, die hinter der Idee des öffentlichen Datennetzes stand, durchsetzen können? *Timing* und Zugangshürden spielen eine große Rolle in der Etablierung von Infrastrukturen, wie man derzeit auch in der Konkurrenz zwischen Plattformbetreibern für Ferienwohnungen, Fahrräder oder Flugbuchungen beobachten kann. Internetdienste wie *Email* standen nicht nur früher zur Verfügung, sie kosteten auch nichts. Schlussendlich ausschlaggebend aber war wohl das *WorldWideWeb*, ein Kommunikationsdienst, der sich ab 1991 schnell im offenen Internet durchsetzen konnte, weil das Netz der Netze keinen Erlaubnisvorbehalt kennt und technisch für keine spezielle Anwendung optimiert ist. Der Wettbewerb zwischen dezentralen und zentral gesteuerten Netzarchitekturen setzt sich jedoch fort. Dave Clark (2016) erzählt die Geschichte des Internets als eine stetige Abfolge von Verzweigungen, in denen verschiedene technische oder wirtschaftliche Lösungen um die Vorherrschaft ringen.

Bis heute bildet das Internet einen Zusammenschluss aus autonomen Netzen, die untereinander verbunden werden müssen, um einen weltweiten Datenverkehr zu ermöglichen. Im Unterschied zur Telefoninfrastruktur, deren physische Leitungen und Nummerierungssysteme die geopolitische Ordnung der Nationalstaaten, Regionen und Städte widerspiegeln, ist der territorialstaatliche Bezug des Internets indirekter. Der Datenfluss orientiert sich nicht an geographischen Entfernung, sondern an den jeweiligen Übergangspunkten zwischen den Netzen der Zugangsprovider. Wichtige Zwischenstationen für die Datenrouten sind *Internet Exchange Points*, die sogenannten Netznoten, an denen *Internet Service Provider* (ISPs) ihre Netze zusammenschließen, um den Datenfluss über die einzelnen Netze hinweg zu organisieren.

Die Verbindungsarrangements zwischen Internetzugangsprovidern legen die Bedingungen fest, unter denen ihre Netze den Datenverkehr für die Kunden des jeweils anderen Netzes weiterleiten. Generell unterscheidet man zwei Typen von Vereinbarungen: Beim *peering* leiten zwei gleichgroße Netze die Datenströme des Partners entgeltfrei weiter; „Transit-Vereinbarungen“ bestehen zwischen unterschiedlich großen Anbietern, wobei der kleinere für die Weiterleitung seiner Daten Zahlungen leistet. Obwohl die Verbindungen zwischen den einzelnen Netzen eine

fundamentale Voraussetzung für den Zusammenhalt des Internets darstellen, erfolgen sie ganz überwiegend informell und frei von externer Regulierung. Neuere Untersuchungen kommen zu dem Schluss, dass nahezu alle Verbindungsarrangements bis heute auf sogenannten *handshake agreements* zwischen den Providern beruhen (Meier-Hahn 2018).

Der Markt für Interkonnektivität hat sich allerdings mit dem Aufkommen digitaler Videoübertragungen verändert. Um die Video-*Streams* möglichst störungsfrei bis zu den Zuschauer\*innen zu bringen, entstanden seit den späten 1990er-Jahren sogenannte *Content Delivery Networks*, die für die Übertragung zeitkritischer Dienste optimiert sind. Neben *transit* und *peering* prägt sich damit ein neues Koordinationsmodell für das Netz der Netze heraus, auf das die informellen Normen der Vergangenheit nicht ohne weiteres anwendbar sind. Eine besondere Position nehmen hier die Internetzugangsprovider ein, die als Intermediäre zwischen den Nutzer\*innen und *Content-Anbietern* wie *Youtube*, *Netflix* oder *Spotify* angesiedelt sind. Ihre Stellung als mächtige *Gatekeeper* auf dem Weg zu den Endusersn hat zunächst in den USA politische Forderungen nach der Wahrung von Netzneutralität hervorgerufen. Das von dem Juristen Tim Wu (2003) formulierte regulative Prinzip der Netzneutralität beruht auf dem Grundsatz der Gleichbehandlung aller Daten und wendet sich gegen Vorfahrtsregelungen für einzelne Anbieter oder Anwendungen im Netz. Die öffentliche Diskussion über Netzneutralität hat ein neues Licht auf den unsichtbar gewordenen Betrieb der Netzinfrastruktur geworfen und diesen zeitweilig repolitisirt. Auch wenn es in vielen Weltregionen inzwischen gesetzliche Regelungen zur Wahrung der Netzneutralität gibt, schwelt der Konflikt über die Kontrolle des Datenverkehrs und die Verteilung der Gewinne zwischen den Netz- und Inhaltsanbietenden weiter.

Obwohl das Internet durch große Dezentralität gekennzeichnet ist, gibt es einige Strukturelemente, die einer globalen Verwaltung bedürfen. Dazu gehören unter anderem die Internetadressen und das Domainnamensystem. Vor allem für die Namen und Nummern des Internets muss sichergestellt sein, dass diese nur einmal vergeben und genutzt werden. Im Falle früherer Kommunikationsinfrastrukturen wurden für solche Koordinationsaufgaben internationale Organisationen wie der Weltpostverein oder die *International Telecommunication Union* gegründet. Für das Internet wurde ebenfalls über eine solche internationale Lösung unter dem Dach der Vereinten Nationen nachgedacht. Diese hat sich allerdings nicht durchsetzen können, weil vor allem die US-amerikanische Regierung eine private Form der Aufsicht über das Domainnamensystem zur Bedingung machte. Dahinter stand die Auffassung, dass sich die Entwicklung des Internets sehr schnell vollziehe, der Staat dagegen träge, bürokratisch und deshalb ungeeignet sei, um die Infrastruktur des Datennetzes zu verwalten.

1998 gründete die US-Regierung die *Internet Corporation for Assigned Names and Numbers* (ICANN), die seither für die Regulierung des Domainnamensystems zuständig ist. Nationale Regierungen wirken an den Entscheidungen von ICANN mit, üben jedoch lediglich eine beratende Funktion aus. Auch die Verwaltung der Internetadressen folgt dem Prinzip der wirtschaftlichen Selbstregulierung. Es sind vorwiegend die *Internet Service Provider*, die sich auf Regeln für die Adressenver-

gabe einigen. Die verschiedenen Verfahren der konsensualen Selbstverwaltung, die sich seit Ende der 1990er-Jahre unter dem Begriff ‚Internet Governance‘ herausgebildet haben, zielen darauf, eine möglichst große Vielfalt von Akteuren und Interessen in den Prozess der Infrastrukturverwaltung miteinzubeziehen. Das globale *Multi-Stakeholder*-Modell, das allen Interessierten zur Beteiligung offensteht, versteht sich ausdrücklich als Alternative zu intergouvernementalen Formen der Repräsentation. Allerdings ziehen der *Multi-Stakeholder*-Ansatz und die Unternehmen wie ICANN, die ihn praktizieren, immer wieder Kritik auf sich. Als Schwächen der Selbstregulierung gelten undurchsichtige Entscheidungsprozesse, die ungleiche Ressourcenverteilung und Einflussmöglichkeit zwischen wirtschaftlichen und zivilgesellschaftlichen *Stakeholdern* und deren Folgen für die Qualität der Regulierungsmaßnahmen (Hofmann 2016).

---

## 4 Staatliche Regulierung digitaler Infrastruktur

Auch wenn die globale Infrastruktur des Internets überwiegend privat verwaltet und betrieben wird, ist auf der nationalen und europäischen Ebene doch eine Zunahme staatlicher Eingriffe zu beobachten. Vielfach handelt es sich dabei um Rahmenregelungen, die Vorgaben für eine wirtschaftliche Selbstregulierung enthalten. Dem vorausgegangen ist die Privatisierung des bis dahin staatlichen Telefonnetzes Mitte der 1990er-Jahre. 1998 wurde das Bundesministerium für Post und Telekommunikation von der Bundesnetzagentur abgelöst, die seither den Markt für Telekommunikation überwacht. Eine wichtige Aufgabe besteht in der Sicherstellung des Wettbewerbs und in der Umsetzung entsprechender EU-Richtlinien und -Verordnungen. Allerdings ist die Bundesnetzagentur kein unabhängiges Regulierungsorgan. Sie ist dem Bundeswirtschaftsministerium unterstellt, und der Bund hält noch gut 30 % der Aktien an der Deutschen Telekom AG, dem ehemaligen Staatsbetrieb. Im internationalen Vergleich wirkt die Liberalisierung des deutschen Telekommunikationsmarktes daher eher halbherzig.

Neben der Regulierung der Netzinfrastruktur sind auch die digitalen Inhalte Gegenstand staatlicher Gesetzgebung. Eine sehr wichtige Rolle für die Entwicklung des Internets spielt das ‚Haftungsprivileg‘ für die Anbieter von Kommunikationsdiensten, das Unternehmen wie *Youtube*, *Twitter* oder *Facebook* von der Verantwortung für die Inhalte ihrer Mitglieder ausnimmt. Ohne ein solches Haftungsprivileg müssten die Anbieter die Rechtmäßigkeit jeder öffentlichen Äußerung auf ihren Plattformen prüfen; ein Aufwand, der der Vermarktung usergenerierter Inhalte faktisch die Grundlage entziehen würde. Was für Infrastrukturbetreiber wie die Post, die ja auch nicht für den Inhalt der Briefe, die sie transportiert, verantwortlich ist, noch selbstverständlich war, ist zum Problem geworden, seit das *Web 2.0* den Menschen die Möglichkeit gibt, selbst öffentlich zu kommunizieren. Seither stellt sich die Frage, wie mit strafbaren Äußerungen und illegalen Angeboten im Netz verfahren werden soll. Die im Jahr 2000 vom Europäischen Parlament beschlossene *E-Commerce*-Richtlinie legt lediglich fest, dass die Dienstanbieter unter bestimmten Umständen nicht haften.

Das Haftungsprivileg für Anbieter ist ein Beispiel dafür, dass die staatliche Regulierung nicht notwendigerweise beschränkenden Charakter hat, sondern die Weiterentwicklung von Infrastrukturen auch ermöglichen kann. Allerdings ist das Haftungsprivileg nicht unumstritten und sein Geltungsbereich wird zunehmend eng gefasst. Gegenwärtig konzentriert sich die politische Diskussion darauf, wie zuverlässig und schnell ein Diensteanbieter strafbare Inhalte löschen muss, sobald er davon Kenntnis hat. Das 2017 von der Bundesregierung beschlossene Netzwerkdurchsetzungsgesetz (NetzDG) gibt bewusst knapp gehaltene Fristen vor. Zugleich bekräftigt das Gesetz die Tendenz, digitale Zugangs- und Inhalteanbieter sachlich wie auch technisch für die Strafverfolgung in Dienst zu nehmen. Nicht die Gerichte prüfen die Strafbarkeit von Inhalten, sondern private Unternehmen, die dafür wiederum Filtersysteme einsetzen. Algorithmisch gestützte *Upload-Filter* werden auch für die Kontrolle urheberrechtlich geschützter Inhalte eingesetzt.

Der Datenschutz ist ein ebenso wichtiges Regulierungsthema, denn personenbezogene Daten spielen für die digitale Infrastruktur inzwischen eine große wirtschaftliche Rolle. Ein Spezifikum des Internets besteht darin, dass die Nutzer\*innen zwar für den Zugang zum Datennetz eine Gebühr entrichten, die Mehrzahl der Kommunikationsdienste wie Suchmaschinen, Internettelefonie oder soziale Netzwerke aber unentgeltlich bzw. werbefinanziert angeboten werden. Um Anzeigen möglichst zielgenau zu platzieren, ist in den frühen 2000er-Jahren ein neues Geschäftsmodell entstanden, das personenbezogene Daten faktisch in den Rang einer Währung hebt. Als Alternative zu herkömmlichen Bezahlmodellen verwerten die Anbieter seither den wachsenden Datenfluss, den sie im Zuge der fortlaufenden Beobachtung ihrer Kund\*innen sammeln. Die Durchsetzung des *Smartphones* und das System der „Apps“ hat die Möglichkeit geschaffen, das Verhalten der Menschen rund um die Uhr zu erfassen und detaillierte Userprofile zu erstellen. Inzwischen hat sich die datenbasierte Wertschöpfung zu einem mächtigen Innovationstreiber der digitalen Infrastrukturen entwickelt.

Aus datenschutzrechtlicher Sicht ist die Inwertsetzung personenbezogener Daten problematisch, weil sie das grundlegende Prinzip der informationellen Selbstbestimmung untergräbt. Sofern digitale Kommunikationsdienste eine unverzichtbare, den Alltag prägende infrastrukturelle Bedeutung gewinnen und es an relevanten datenschutzfreundlichen Alternativen mangelt, verschwindet die Freiheit, sich gegen die Preisgabe der Privatsphäre zu entscheiden. Die 2018 in Kraft getretene europäische Datenschutzgrundverordnung zielt darauf, diese Entwicklung aufzuhalten, indem bestehende Prinzipien wie Datensparsamkeit, die informierte Einwilligung und die Zweckbindung der Datenverarbeitung gestärkt und zugleich neue Instrumente wie Datenschutz durch Technikgestaltung und das Recht auf Datenportabilität umgesetzt werden. Die nächsten Jahre werden zeigen, ob Prinzipien wie Datensparsamkeit in Zeiten wachsender Datenströme noch greifen.

Das Schlagwort der digitalen Gesellschaft proklamiert, dass sich das Internet zu einem zentralen Trägermedium sozialer Organisation entwickelt. Immer rarer werden die Strukturen, Institutionen und Handlungen, die nicht digital vermittelt oder assistiert, vermessen und bewertet werden. Dafür verantwortlich sind zum einen die Geräte und hohen Datenübertragungsgeschwindigkeiten, die das *Always on*-Dasein

ermöglichen; zum anderen aber auch die Entstehung von Plattformen, eines neuen Typs von Kommunikationsinfrastruktur, der im wachsenden Umfang gesellschaftliche Koordinationsprozesse organisiert. Technisch gesehen handelt es sich bei Plattformen um Datenbanksysteme, die ihre große Komplexität hinter standardisierten Programmierschnittstellen (*application programming interface*, API) verstecken. Die APIs vereinfachen das öffentliche Kommunizieren für die Menschen und kanalisieren zugleich die Entwicklung neuer *Apps* unter der Kontrolle der Plattformen (Plantin et al. 2018).

Man kann sich Plattformen als global verteilte, sich beständig aktualisierende Speichersysteme vorstellen, die den Austausch von Informationen in Echtzeit ermöglichen. In den frühen 2000er-Jahre entstanden auf diese Weise erstmals Publikationskanäle für Jedermann. Im Prinzip hatte das Internet die Möglichkeiten des Lesens und Schreibens zwar auch zuvor schon geboten, aber Plattformen vereinfachen das Publizieren. Indem sie den Kommunikationsfluss unter ihren Mitgliedern algorithmisch steuern, ‚kuratieren‘ sie zudem spezifische Öffentlichkeiten. Ökonomen betrachten Plattformen wie *Ebay*, *Amazon*, *Youtube* oder *Uber* als zweiseitige Märkte für den Handel von Gütern wie auch von Arbeitskraft. Mark Zuckerberg, der Gründer von *Facebook*, hat einmal als Ziel formuliert, *Facebook* solle das Betriebssystem der Gesellschaft werden. Obwohl die unterliegende Architektur des Internets unverändert ist, hat die „*platformization*“ (Helmond 2015) doch einen tiefgreifenden Wandel der digitalen Infrastruktur angestoßen. Bemerkbar macht sich dieser nicht zuletzt in der raschen Ausbreitung einer Plattformlogik. Das Geschäftsmodell wie auch die Geschäftsbedingungen weniger monopolförmiger Plattformbetreiber wirken in immer mehr Bereichen von Wirtschaft und Gesellschaft strukturbildend (Langley und Leyshon 2017). Selbst lokale Märkte für Güter und Dienstleistungen werden nun auf global operierenden Plattformen vernetzt. Die dabei entstehenden großen Datenvolumina unter der Kontrolle weniger Unternehmen bilden das Rohmaterial für die nächste Generation von Dienstleistungen, die sich auf den Einsatz von Künstlicher Intelligenz und Robotik stützen.

---

## 5 Perspektiven

Augenblicklich beobachten wir, wie sich das entstehende *Internet of Things* (IoT) aus dem Bereich der Industrieanwendungen in den Alltag vortastet. IoT wird als globale Infrastruktur definiert, die aus einer Art gemeinsamer Sprache für Objekte besteht. Diese Sprache stattet physische wie auch virtuelle Dinge mit einer globalen Identität, physischen Attributen und normierten Schnittstellen aus. Vermittels Sensoren können Dinge Informationen über ihren Zustand ermitteln und weitergeben, der sich dann wiederum modifizieren lässt, von beliebigen Orten und beliebigen Akteuren menschlicher oder nichtmenschlicher Natur. Eine Vielzahl zusätzlicher Schnittstellen zwischen dinglichen und symbolisch-kalkulatorischen Objekten ist die Folge. IoT soll das Internet nicht ersetzen, sondern dessen Reichweite und Wirkungsweise ausdehnen. Zu den Anwendungsfeldern gehören bestehende Infrastrukturen im Bereich der Produktion und Landwirtschaft, dem Handel und der

Logistik, aber auch alltagsnähere Bereiche wie die Fahrzeugkommunikation, *Smart Cities* oder *Smart Homes*.

Je nach Blickwinkel stellt sich das Internet der Dinge als neue Infrastruktur der Infrastrukturen dar oder als kommende Generation digitaler Anwendungen. Als Infrastruktur betrachtet, zeigen sich auffällige Parallelen zu den frühen Tagen des Internets. Wiederum besteht ein Bedarf nach einheitlichen technischen Standards, um die verschiedene Ansätze und Akteure konkurrieren. Im Verkehrsbereich geht es um die Vernetzung von Fahrzeugen und Verkehrsleitsystemen. Um die dafür erforderlichen Standards gruppieren sich unterschiedliche Industriekonsortien. Das vernetzte Heim benötigt ebenfalls herstellerübergreifende Standards, die das Zusammenspiel zwischen den Geräten sicherstellen, Sicherheitsupdates ermöglichen sowie Datenschutz- und Haftungsansprüchen genügen. Obwohl *Smart Home*-Produkte längst auf dem Markt sind, gelingt es den vielen Standardisierungsinitiativen in diesem Bereich nicht, sich auf ein gemeinsames Normsetzungsforum zu einigen.

Das Internet der Dinge soll nicht nur bestehende Aufgaben automatisieren und optimieren, sondern auch neuen Produkten und Dienstleistungen zum Durchbruch verhelfen. Erwartet wird etwa eine größere Formen- und Funktionsvielfalt von Robotern im Alltagsleben sowie eine Ausbreitung von Drohnen, deren Einsatz dann wiederum neue Haftungs- und Verkehrsregeln auch im Luftraum erforderlich machen wird. Die vielen Daten, die das Internet der Dinge mit sich bringt, sind von großem gesellschaftlichem und wirtschaftlichem Wert. Sie werden deshalb Gegenstand einer Datenpolitik, die durch wirtschaftliche Interessen, demokratische Grundrechte, gesellschaftliche Verteilungsdiskussionen sowie Konzepte und Kulturen staatlicher Regulierung geprägt sein wird.

Obwohl die Expansionsdynamik des Datennetzes ungebrochen ist, verliert der Begriff Internet an Bedeutung in der Beschreibung dieser Entwicklung. Noch in den 2000er-Jahren bestand die Vorstellung vom Internet als virtuellem Raum, in den man sich hineinbegibt – und den man folglich auch wieder verlassen kann. Bis heute wird statistisch erhoben, wie viele Stunden die Menschen täglich *im Internet* verbringen. Derzeit lebt die Vorstellung vom Internet als Raum aber hauptsächlich im militärischen Sprachgebrauch in Begriffen wie ‚Cyber-Angriffen‘ und *Cyber Warfare* weiter. Während die Bezeichnung Internet und die damit assoziierte Netzinfrastruktur langsam in die Unsichtbarkeit absinkt, hat sich öffentlich ein neues Bild von Digitalisierung durchgesetzt. An die Stelle des Raums ist die Idee eines Netzes getreten, das zunehmend alle Bereiche der Gesellschaft durchdringt und nun neben Computern und Menschen auch Objekte miteinander verbindet (Castells 1996). Absehbar ist, dass neben der Eroberung des Luftraums auch der menschliche Körper von der Expansion des Netzes erfasst wird. Im Namen einer optimierten Gesundheitsvorsorge und Risikokontrolle wird so ein neues Niveau der Lesbarkeit der Menschheit normalisiert.

Aus der Infrastrukturperspektive besehen, fällt auf, dass sich der ‚Unterbau‘ und die darauf basierenden Organisationsleistungen so stark wechselseitig überlagern, dass eine kategoriale Unterscheidung zwischen beiden immer weniger möglich und sinnvoll ist. Mit der Digitalisierung, so scheint es, erreicht das Konzept der Infrastruktur einen neuen Grad der Universalität. Als selektiver Integrationsmechanismus

steigert die expandierende Dateninfrastruktur allerdings auch die Machtzentration und die Bedeutung des Verletzlichkeitsparadoxen. Wünschenswert wäre eine öffentliche Diskussion über die Folgen und möglichen regulatorischen Konsequenzen dieser Entwicklung.

---

## Literatur

- Abbate, Janet. 1999. *Inventing the Internet*. Cambridge: MIT Press.
- Bowker, Geoffrey, und Susan Leigh Star. 1999. *Sorting things out. Classification and its consequences*. Cambridge: MIT Press.
- Castells, Manuel. 1996. *The information age. Economy, society, and culture, Volume 1: The rise of the network society*. Oxford: Blackwell Publishers.
- Clark, David D. 2016. The contingent Internet. *Daedalus* 145(1): 9–17. [https://doi.org/10.1162/DAED\\_a\\_00361](https://doi.org/10.1162/DAED_a_00361).
- Frischmann, Brett M. 2012. *Infrastructure. The social value of shared resources*. New York: Oxford University Press.
- Graham, Stephen, Hrsg. 2010. *Disrupted cities. When infrastructure fails*. New York: Routledge.
- Helmond, Anne. 2015. The platformization of the Web. Making Web data platform ready. *Social Media + Society* 1(2): 1–11. <https://doi.org/10.1177/2056305115603080>.
- Hofmann, Jeanette. 2016. Multi-Stakeholderism in Internet governance. Putting a fiction into practice. *Journal of Cyber Policy* 1(1): 29–49. <https://doi.org/10.1080/23738871.2016.1158303>.
- Katz, Michael L., und Carl Shapiro. 1986. Product compatibility choice in a market with technological progress. *Oxford Economic Papers* 38(0): 146–165. <https://doi.org/10.1093/oxfordjournals.oep.a041761>.
- Laak, Dirk van. 2017. Eine kurze (Alltags-)Geschichte der Infrastruktur. *Aus Politik und Zeitgeschichte* 67(16–17): 4–11.
- Langley, Paul, und Andrew Leyshon. 2017. Platform capitalism. The intermediation and capitalization of digital economic circulation. *Finance and Society* 3(1): 11–31. <https://doi.org/10.2218/finsoc.v3i1.1936>.
- Larkin, Brian. 2013. The politics and poetics of infrastructure. *Annual Review of Anthropology* 42(1): 327–343. <https://doi.org/10.1146/annurev-anthro-092412-155522>.
- Meier-Hahn, Uta. 2018. *Die Konnektivitätsökonomie des Internets. Architektur – Konventionen – Community*. Berlin: Dissertation am Fachbereich Wirtschaftswissenschaft der Freien Universität Berlin.
- Plantin, Jean-Christophe, Carl Lagoze, Paul N. Edwards, und Christian Sandvig. 2018. Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society* 20(1): 293–310. <https://doi.org/10.1177/1461444816661553>.
- Postel, Jon, Hrsg. 1980. *Transmisson Control Protocol*. <https://doi.org/10.17487/RFC0761>.
- Wu, Tim. 2003. Network neutrality, broadband discrimination. *Journal on Telecommunications and High Technology Law* 2(1): 141–176.



# Digitale Transparenz

Caroline Fischer und Sascha Kraus

## Inhalt

1 Klärung des Begriffs .....	160
2 Theoretische Grundlagen .....	163
3 Praktische Anwendung .....	166
4 Umsetzungsstand und Auswirkungen .....	167
5 Perspektiven für Staat und Verwaltung .....	168
Literatur .....	169

## Zusammenfassung

Transparenz ist kein neuer Begriff, sondern im Zusammenhang mit Rechtsstaatlichkeit, Gewaltenteilung oder Demokratie schon lange Gegenstand politischer Theorie und Praxis. Transparenz bedeutet, dass Akteure, wie etwa Verwaltungsorganisationen, relevante Informationen über ihre Entscheidungsprozesse, Funktionsweisen und Performanz gegenüber externen Akteuren offenlegen. Für politische und Verwaltungsakteure gewinnt Transparenz im Zuge der Digitalisierung an zusätzlicher Bedeutung. Moderne Informations- und Kommunikationstechnologien vereinfachen Transparenzschaftung, sowohl in der Geschwindigkeit als auch im Ressourceneinsatz. Sie können so zu neuen Formen und einer neuen Qualität von Transparenz in Politik und Verwaltung beitragen. Transparenz- und Datenportale oder Bürgerhaushalte sind digitale Instrumente, die diesem Zweck dienen sollen. Ob digitale Transparenz politische und administrative Prozesse tatsächlich effizienter, effektiver und durchsichtiger macht und Bürger\*innen diese dadurch besser verstehen, ist jedoch eine offene Frage.

C. Fischer (✉) · S. Kraus

Universität Potsdam, Potsdam, Deutschland

E-Mail: [caroline.fischer.ii@uni-potsdam.de](mailto:caroline.fischer.ii@uni-potsdam.de); [sascha.kraus@uni-potsdam.de](mailto:sascha.kraus@uni-potsdam.de)

**Schlüsselwörter**

Open Government · E-Government · Geheimhaltung · Privatsphäre ·  
Arkanprinzip

---

## 1 Klärung des Begriffs

In den letzten dreißig Jahren hat Transparenz in der öffentlichen Diskussion und administrativen Praxis zunehmend an Popularität gewonnen. Gleichwohl wird der Begriff häufig nicht (eindeutig) definiert und unzureichend von verwandten Begriffen abgegrenzt. In Wissenschaft und Praxis finden sich zahlreiche abstrakte Umschreibungen von Transparenz als Instrument zur Schaffung von Klarheit und Durchsichtigkeit in Staat und Verwaltung in Abgrenzung zum Geheimen und Opa ken. Andere wiederum betonen Nachvollziehbarkeit und Vorhersehbarkeit von Regeln und politischen Entscheidungen. Nach Stephan Grimmelikhuijsen und Albert Meijer (2014, S. 139) kann Transparenz in Politik und Verwaltung wie folgt definiert werden:

„Transparency is the availability of information about an organization or actor allowing external actors to monitor the internal workings or performance of that organization.“

Bezogen auf Staat und Verwaltung bezeichnet digitale Transparenz sowohl die Veröffentlichung von Informationen als auch den Zugang zu ihnen mithilfe moderner Informations- und Kommunikationstechnologien (IKT), nicht zuletzt des Internets. Die Bereitstellung und Auswertung von staatlichen Informationen soll es Externen ermöglichen, Akteure in Politik und Verwaltung zu kontrollieren und gegebenenfalls zur Rechenschaft ziehen. Sie soll so zu einem effizienteren und effektiveren Regieren und Verwalten beitragen.

Die Konstituierung von Transparenz als institutionalisierte Beziehung zwischen mindestens zwei Akteuren bietet analytischen Mehrwert und erleichtert die Systematisierung von Transparenzeffekten. Entsprechend können drei grundlegende Elemente von Transparenzmaßnahmen identifiziert werden: (1) ein *Objekt*, das Gegenstand der Transparenzschaftung ist, (2) ein *Subjekt*, auf das sich die Transparenzschaftung bezieht und welches die in diesem Zusammenhang zur Verfügung gestellten Informationen weiterverarbeitet sowie schließlich (3) *Mittel* und *Instrumente*, mit deren Hilfe die Transparenzschaftung erfolgt. Dass Transparenz die spezifische Ausgestaltung einer Beziehung zwischen mindestens zwei Akteuren ausdrückt, wird spiegelbildlich auch in der Definition von *Geheimhaltung* deutlich (Richter 2017, S. 236 f.). Hierbei schließen Akteure, welche über sensible und vertrauliche Informationen verfügen, andere Akteure aus diversen Gründen aktiv und bewusst von diesen Informationen aus.

Transparenz ist kein eindimensionales Konzept, vielmehr müssen verschiedene Formen und Varianten unterschieden werden. Idealtypisch lassen sich zunächst zwei Richtungen von Transparenz unterscheiden:

- *Vertikale Transparenz*: Transparenz kann nach oben oder unten gerichtet sein. Aufwärts gerichtete Transparenz bedeutet, dass ein hierarchisch höher gestellter Akteur (Prinzipal) das Verhalten oder die Performanz eines hierarchisch untergebrachten Akteurs (Agent) beobachten kann. Abwärts gerichtete Transparenz ermöglicht es wiederum dem Agenten, den Prinzipal zu beobachten. Vertikale Transparenzschaftung findet etwa zwischen Vorgesetzten und Mitarbeiter\*innen, Ministerien und deren nachgeordneten Behörden sowie zwischen Staat und Bürger\*innen statt.
- *Horizontale Transparenz*: Transparenz kann nach außen oder innen gerichtet sein. Nach außen gerichtete Transparenz ermöglicht es Akteuren in Organisationen, das Organisationsumfeld zu beobachten. Nach innen gerichtete Transparenz bedeutet, dass externe Akteure das Verhalten oder die Performanz von Organisationen und ihren Mitgliedern beobachten können. Horizontale Transparenzschaftung in Politik und Verwaltung ist zwischen verschiedenen Organisationen oder Organisationseinheiten, insbesondere aber gegenüber Bürger\*innen denkbar.

Weiterhin lassen sich verschiedene objektbezogene Formen von Transparenz unterscheiden. Grundlegend müssen individuelle und institutionelle Transparenz voneinander abgegrenzt werden. In der Regel wird unter Transparenz die Transparenz des Staates gegenüber den Bürger\*innen verstanden (*institutionelle Transparenz*), nicht aber der Bürger\*innen gegenüber dem Staat (*individuelle Transparenz*). Im vorliegenden Artikel wird ausschließlich institutionelle Transparenz behandelt, genauer gesagt:

- *Politische Transparenz* meint die Transparenz von Parlamenten und Regierungen sowie ihrer Mitglieder. Dazu gehören allgemeine Informationen zu Parlaments- und Regierungaktivitäten, aber auch die Bereitstellung von Informationen zu gewählten Vertreter\*innen (Abstimmungsverhalten, Nebeneinkünfte etc.).
- *Verwaltungstransparenz* bezeichnet die Transparenz von Organisationen der Ministerial- und Vollzugsverwaltung. Sie umfasst die Bereitstellung von Informationen zu den Aufgaben, Strukturen und Zielen sowie zu den Aktivitäten und Prozessen der öffentlichen Verwaltung.

Dies ist eine idealtypische Unterscheidung. In der Realität überlappen sich beide Formen und sind miteinander verflochten. Zum Beispiel machen die Besonderheiten der deutschen Ministerialbürokratie mit ihrer Nähe zur Politik und den damit verbundenen Aufgaben der Entscheidungsvorbereitung und Programmentwicklung eine klare Trennung zwischen politischer und administrativer Transparenz schwierig (Richter 2017, S. 237).

Zudem lassen sich zahlreiche Varianten der Transparenzschaftung in Bezug auf deren Instrumente und Modi differenzieren. Diese sind vor allem im Hinblick auf die Analyse von Transparenzmaßnahmen sowie auch ihrer jeweiligen Effekte relevant:

- Prozess- und Ergebnistransparenz: *Prozesstransparenz* kann als Zugang zu Informationen über Beratungs-, Verhandlungs-, Entscheidungs- sowie Leistungserstellungsprozesse verstanden werden (das ‚Wie‘). *Ergebnistransparenz* hingegen

bezieht sich auf *Inputs*, *Outputs* und *Outcomes* von politischen und administrativen Entscheidungen (das ‚Was‘). Insgesamt kann Prozesstransparenz als umfassender betrachtet werden, weil nicht bloß Ergebnisse offengelegt werden, sondern auch Informationen zu deren Entstehung.

- Retrospektive und Echtzeit-Transparenz: *Retrospektive Transparenz* meint die (un)regelmäßige Veröffentlichung von Informationen zu Prozessen und Ergebnissen zu einem nachgelagerten Zeitpunkt. Hingegen werden bei der *Echtzeit-Transparenz* relevante Informationen unmittelbar und fortlaufend zur Verfügung gestellt, etwa bei Live-Übertragungen von Parlamentsdebatten oder Gremiensitzungen.
- Passive und aktive Transparenz: *Passive Transparenz* beschreibt den Zugang zu Informationen auf Nachfrage oder Anweisung externer oder hierarchisch übergeordneter Akteure (*transparency by demand*). Sie entsteht beispielsweise durch Informationsfreiheitsanfragen. Passive Transparenz setzt voraus, dass bekannt ist, welche Informationen nachgefragt werden können (Informationsregister). *Aktive Transparenz* hingegen meint die proaktive Bereitstellung von Informationen (*transparency by default*), etwa über Datenportale (*Open Government Data*). Hieran wird deutlich, dass Transparenz keinesfalls mit Informationsfreiheit oder *Open Government Data* synonym ist.
- Intendierte und nicht-intendierte Transparenz: *Intendierte Transparenz* ist ein beabsichtigter Zugang zu Informationen. *Nicht-intendierte Transparenz* entsteht hingegen, wenn Informationen veröffentlicht werden, die aufgrund von Einschränkungen (Datenschutz, nationale Sicherheit etc.) oder aus strategischen Gründen vertraulich oder geheim waren. Sie kann etwa durch Unachtsamkeit, *Hacks*, *Leaks* oder *Whistleblowing* entstehen.

Zusätzlich zur Form der veröffentlichten Information und dem damit einhergehenden Veröffentlichungsprozess muss in nominale und effektive Transparenz unterschieden werden. *Nominale Transparenz* kann als Transparenz auf dem Papier verstanden werden, wohingegen sich *effektive Transparenz* auf die tatsächliche Transparenz von Staat und Verwaltung bezieht, die für Bürger\*innen entsteht. Die Lücke zwischen beiden wird auch als „Illusion von Transparenz“ (*transparency illusion*) bezeichnet. Eine solche Lücke besteht etwa, wenn zwar zahlreiche Informationen veröffentlicht werden, diese aber aufgrund ihrer Fülle oder Komplexität von Bürger\*innen nicht verstanden und genutzt werden (*information overload*). Effektive Transparenz hängt damit immer auch vom Subjekt der Transparenzschaftung ab.

Im politischen und akademischen Diskurs werden Transparenz und *Open Government* häufig synonym verwendet und nur unzureichend voneinander abgegrenzt. *Open Government* bezeichnet ein Paradigma für offenes Regierungs- und Verwaltungshandeln, welches durch die drei Säulen Transparenz, Partizipation und Kollaboration politisches sowie administratives Handeln verbessern möchte. Transparenz hingegen spielt zwar als Grundlage von Partizipation und Kollaboration eine wesentliche Rolle für *Open Government*, ist aber konzeptionell gesehen der spezifischere Begriff.

## 2 Theoretische Grundlagen

Transparenz ist keine Erfindung des 20. oder gar 21. Jahrhunderts, sondern im Zusammenhang mit Rechtsstaatlichkeit, Gewaltenteilung oder Demokratie schon lange Gegenstand politischer Theorie. Einen ausführlichen Überblick zur Geschichte des Transparenzbegriffs und seines Vorläufers, der Publizität, bieten Christopher Hood und David Heald (2006) sowie Vincent Rzepka (2013). Es ist eine der ältesten politischen Ideen, dass eine Regierung regelgebunden handelt (Rechtsstaatlichkeit) und ihr Handeln kontrolliert wird (Gewaltenteilung und -kontrolle). Hierfür ist Transparenz eine zentrale Voraussetzung.

Seinen Ursprung hat der Begriff der Transparenz in der Beschreibung von Lichtdurchlässigkeit. Diese Bedeutung von Durchlässigkeit und Durchsichtigkeit spiegelt sich auch im politischen Begriff der Transparenz wieder. Bereits Jean-Jacques Rousseau schreibt dem Naturzustand des Menschen eine vollkommene Transparenz zu, verbleibt aber in seinem Verständnis auf einer psychologischen Ebene des „durchsichtigen“ menschlichen Charakters. Bei Immanuel Kant wird Publizität zur politischen Norm. Publizität meint sowohl eine Veröffentlichungspflicht des Staates als auch die Meinungsfreiheit der Bürger\*innen. Sie dient bei Kant der öffentlichen Kontrolle von Politik und ist damit die Grundlage für Repräsentation.

Jeremy Bentham weitet dieses Konzept aus und gilt als Schöpfer des politischen Transparenzbegriffes, den er vor allem in „*A Fragment on Government*“ (1776 [1843]), „*Panopticon*“ (1787 [1843]) und „*Constitutional Code*“ (1830 [1843]) darlegt. Er erweitert Kants Veröffentlichungspflicht um eine Besuchs- und Medienöffentlichkeit. Politische Institutionen sollen den Bürger\*innen offenstehen und so die politische Entscheidungsfindung transparent(er) machen. Bentham fügt damit dem produktorientierten Blick auf Transparenz einen prozessorientierten Ansatz hinzu. Transparenz wird darauf aufbauend auch als Basis von Deliberation und Partizipation beschrieben.

In späteren Konzepten zu *Open Government* ist Transparenz die Basis für die weiteren Säulen Partizipation und Kollaboration. Gleichzeitig, so argumentieren beispielsweise feministische Theorien, dient Transparenz dazu, problematische Machtstrukturen und eine entsprechende Selbstrekrutierung offenzulegen und abzuschaffen. Transparenz ermöglicht dadurch Partizipation von Minderheiten. Sie wird daher immer wieder zur Sicherstellung von Fairness und Vermeidung von Diskriminierung ins Feld geführt.

Bentham weitet Publizität aber nicht nur auf Prozesse aus, sondern ergänzt eine qualitative Anforderung: deren *Simplizität*, also Klarheit, Korrektheit und Vollständigkeit. Simplizität qualifiziert Publizität zur Transparenz und soll verzerrte Informationen und Täuschung verhindern. Bentham deutet damit bereits die Unterscheidung in nominale und effektive Transparenz an.

Das Konzept der Transparenz überträgt Bentham auf politische Institutionen und die öffentliche Verwaltung, die mit Hierarchie und klar zuordenbaren Verantwortlichkeiten sicherstellen müssen, dass das Volk die politisch Handelnden identifizieren kann (Legitimationsketten). Demokratietheoretisch zielt Transparenz so auf die

Kontrolle politischer Eliten durch die allgemeine Öffentlichkeit. Geheim bleiben darf, was einen Schaden für Privatpersonen erzeugen kann oder eine Gefahr für die nationale Sicherheit darstellt. Bentham schränkt Transparenz also ein, anstatt sich für radikale Transparenz auszusprechen. Die Gründe hierfür, Schutz der *Privatsphäre* und nationale Sicherheit, stellen bis heute die zentralen Einschränkungen von Transparenz dar, etwa in Informationsfreiheitsgesetzen.

Die transparente Institutionenstruktur Benthams spiegelt sich in seiner architektonischen Idee des Panoptikums wieder, das gleichzeitig die größten Probleme von Transparenz deutlich macht. Das Panoptikum ist in seiner ursprünglichen Idee ein gläsernes Gefängnis, von dessen Zentrum aus alle rundherum angeordneten Zellen eingesehen werden können. Gleichzeitig aber ist kein Blick aus den Zellen ins Zentrum möglich. Dieses Konzept wird unter anderem von Michel Foucault als Symbol allgegenwärtiger Disziplinarmacht kritisiert, insbesondere wenn diese Idee auf andere öffentliche Gebäude ausgedehnt wird. Die Transparenz des Staates gegenüber dem Individuum würde hier verkehrt in eine Transparenz des Individuums gegenüber dem Staat. Solche Bedenken gegenüber einem „Überwachungsstaat“ durchziehen die Transparenzdebatte bis heute.

Im Konzept des *New Public Management* (NPM) soll Transparenz, etwa durch Audits und *Benchmarking*, die Überprüfung der Zielerfüllung und eine *Output*-Steuerung der öffentlichen Verwaltung ermöglichen (Schedler und Proeller 2011). Der „Dienstleistungsstaat“ soll rechenschaftspflichtig sein gegenüber den Bürger\*innen, die als Kund\*innen der Verwaltung verstanden werden. Gleichzeitig verstärken Privatisierung und *Outsourcing* im Zuge von NPM-Reformen Transparenzprobleme, weil ausgelagerte Aufgaben nicht mehr den staatlichen Transparenzpflichten unterliegen.

In den letzten dreißig Jahren hat Transparenz sich vor allem durch die zunehmende Digitalisierung sowie durch die erfolgreiche Arbeit von Nichtregierungsorganisationen und Initiativen wie *Transparency International* oder die *Sunlight Foundation*, aber auch durch Reformansätze wie *New Public Management* (NPM) zu einer neuen globalen Norm entwickelt. Die Befürworter von mehr Transparenz in Staat und Verwaltung sehen darin ein Allheilmittel zur Stärkung der (westlichen) Demokratie. Kritiker warnen hingegen vor einem „gläsernen Bürger“, also der fehlenden Abgrenzung von individueller und institutioneller Transparenz. Auch wird die Gefahr von Handlungs- und Entscheidungsblockaden in Politik und Verwaltung durch ein zu hohes Maß an Transparenz gesehen. Eine totale Transparenzgesellschaft wäre zudem eine inhumane und tyrannische Kontroll- und Überwachungsgesellschaft (Han 2012).

Die Grenze zwischen staatlicher Transparenz und *Geheimhaltung* ist immer auch eine gesellschaftliche Abwägungsfrage, die im Laufe der Zeit und je nach politischem, ökonomischem und technologischem Kontext unterschiedlich beantwortet werden kann (Wewer 2014). Zum Beispiel kann ein hohes Maß an Transparenz auf einigen Politikfeldern hilfreicher sein als auf anderen: Während Transparenz in der Umwelt- und Gesundheitspolitik unumgänglich ist, kann übertriebene Transparenz internationale Verhandlungen erheblich erschweren oder gar blockieren.

Einige Autoren betrachten Transparenz als eine Norm, die einen Wert an sich besitzt, keinen weiteren Nutzen haben muss und durchaus Kosten verursachen darf.

Die Mehrheit der Literatur sieht in Transparenz aber keinen Selbstzweck und plädiert dafür, auch hier zwischen Kosten und Nutzen abzuwegen. Transparenz sollte dennoch nicht nur an ihren Wirkungen gemessen werden, sondern hat als demokratische Grundnorm einen intrinsischen Wert.

Als positive *Wirkungen* werden der Transparenz politischer und administrativer Prozesse die Reduktion von Korruption, eine effizientere Arbeit von Regierung und Verwaltung sowie die Stärkung der Legitimation eines Staates zugeschrieben. Ob Transparenz Vertrauen schafft oder sogar verringert, die Arbeit der Regierung untergräbt und dabei hohe (Opportunitäts-)Kosten erzeugt, ist umstritten. Cucciniello et al. (2017) haben in ihrer Meta-Analyse zu Effekten von Transparenz gezeigt, dass diese das Risiko von Korruption senkt und sich positiv auf das Finanzmanagement von (staatlichen) Organisationen auswirkt. Das kann die Zufriedenheit der Bürger\*innen mit Regierung und Verwaltung positiv beeinflussen und sich auf deren Partizipation auswirken. Deutlich wird dennoch, dass die meisten Wirkungen von Transparenz empirisch bisher nicht eindeutig nachgewiesen werden konnten. Transparenzmaßnahmen bringen vielmehr häufig sowohl positive als auch negative oder gar keine nachweisbaren Effekte hervor.

Hood und Heald (2006, S. 218) merken an, dass viele der prognostizierten Wirkungen von Transparenz, wie z. B. eine wachsende Erkenntnis der Bürger\*innen durch besseren Zugang zu mehr Informationen, schlicht nicht messbar sind. Unabhängig davon wurden auch *pervertierende Wirkungen* von Transparenz identifiziert, wenn etwa durch einen bewussten *information overload* bestimmte Tatsachen verschleiert werden (*snowing*). Die Veröffentlichung von komplexen Daten kann dazu führen, dass diese nicht weitergenutzt werden können (fehlende Simplizität). Formal werden dann zwar womöglich Vorgaben erfüllt, aber es entsteht keine tatsächliche Transparenz für die Bürger\*innen. Ob diese öffentliche Informationen nutzen können oder in deren Masse verloren sind, hängt unter anderem vom Bildungsstand ab. Transparenz muss also immer zielgruppenspezifisch geschaffen werden, Standardlösungen für alle Anspruchsgruppen kann es nicht geben. Auch im digitalen Zeitalter sind daher weiterhin Formen von Transparenz nötig sind, die auch Bürger\*innen ohne IT-Kenntnisse nutzen können (analoge Transparenz).

Wenn Transparenz als Norm in Politik und Verwaltung nicht akzeptiert ist, können entsprechende Maßnahmen zu *Ausweich- und Umgehungsverhalten* führen. So können nutzlose Informationen offengelegt, Entscheidungsprozesse in arkane Räume verlagert (von offenen Debatten in informelle Vorabsprachen) oder die Art und Weise der Aktenführung verändert werden. Ursache hierfür kann auch die Angst vor der Offenlegung von Fehlern sein (*blame avoidance*). Transparenzmaßnahmen hängen immer auch eng mit *Machtfragen* zusammen. Insbesondere in stark weberianisch geprägten Verwaltungen steht Transparenz dem *Arkanprinzip* des Staates entgegen. Im Weberianischen Bürokratiemodell sind zwar Regelbefolgung und klare Prozesse vorgesehen, nicht jedoch ein (mehr oder weniger unbeschränkter) Informationszugang für Bürger\*innen. Die deutsche Verwaltung ist bis heute von einer Tradition der Amtsverschwiegenheit und Geheimhaltung geprägt. Entsprechend werden Behörden versuchen, ihr Fach- und Dienstwissen als Herrschaftswissen zu verteidigen (Wegener 2006).

### 3 Praktische Anwendung

Im 21. Jahrhundert sind Transparenz und Digitalisierung untrennbar miteinander verbunden. Der Einsatz von IKT und insbesondere des Internets ermöglichen ein erhöhtes Maß an Transparenz in Datenbeständen, von Aktivitäten und Verantwortlichkeiten. Große Datenbestände lassen sich leichter handhaben und es wird einfacher, Informationen kostengünstig und zeitnah für externe Akteure zur Verfügung zu stellen (Bannister und Connolly 2011). Insgesamt ermöglicht Digitalisierung neue Formen und eine neue Qualität von Transparenz in Politik und Verwaltung, die vor dem digitalen Zeitalter zwar theoretisch denkbar, aber praktisch kaum umsetzbar waren (Lucke 2010). Allerdings führt Digitalisierung nicht automatisch zu mehr Transparenz, wie Effekte wie der ‚information overload‘ zeigen. Auch führt die Verengung auf digitale Transparenz zu einer Ungleichbehandlung der Bürger\*innen, die diesen Zugangsweg nicht nutzen können oder wollen. Entsprechend sollte bei vertretbarem Verwaltungsaufwand auch immer der analoge Zugang zu entsprechenden Daten und Informationen möglich sein. Im Folgenden werden exemplarisch einige digitale Lösungen aufgeführt, welche Transparenz in Politik und Verwaltung schaffen können:

- Webseiten und Informationsportale: Mittlerweile betreiben fast alle Regierungen und ihre Verwaltungsbehörden zahlreiche Webseiten sowie umfangreiche Informationsportale. Diese geben etwa Auskunft über zuständige Behörden und Mitarbeiter\*innen oder Verwaltungsleistungen und bieten in vielen Ländern auch *E-Government-Services* an.
- Parlaments- und Ratsinformationssysteme: Diese stellen Dokumente (Berichte, Plenarprotokolle, Beschlussfassungen etc.) sowie allgemeine Informationen zu Aufgaben, Funktion und Struktur der jeweiligen Organisation und ihrer Mitglieder (etwa Nebentätigkeiten und -einkommen von Abgeordneten, Abstimmungsverhalten) zur Verfügung. Solche Anwendungen sind in demokratischen Staaten weit verbreitet. Teilweise haben Bürger\*innen auch die Möglichkeit, sich über derartige digitale Plattformen an Bürgerhaushalten zu beteiligen. Wegweisend war hier die Schweizer Bundesversammlung, welche bereits in den 1990er-Jahren ein Portal mit umfangreichem Informationsangebot, zeitnah veröffentlichten Abstimmungsprotokollen und Live-Streams von laufenden Debatten geschaffen hat ([www.parlament.ch](http://www.parlament.ch)).
- Informationsfreiheitsgesetze (IFGs): In mehr als 110 Ländern weltweit besteht die Möglichkeit, auf der Grundlage von Gesetzen Zugang zu Informationen aus Politik und Verwaltung zu beantragen. Hierbei spielen Webportale mit Archiven zu vergangenen IFG-Anfragen sowie webbasierte Antragsassistenten eine wichtige Rolle, weil diese Informationsfreiheitsanfragen deutlich erleichtern. Diese Angebote werden häufig von zivilgesellschaftlichen Akteuren zur Verfügung gestellt. Bekannte Beispiele sind „Frag den Staat“ ([www.frag-den-staat.de](http://www.frag-den-staat.de)) in Deutschland und „What Do They Know“ ([www.whatdotheyknow.com](http://www.whatdotheyknow.com)) im Vereinigten Königreich.

- *Open Government Data*: Viele Regierungen und Verwaltungen stellen über Portale Regierungs- und Verwaltungsdaten proaktiv, systematisch und barrierefrei zur freien Nutzung, Weiterverarbeitung und -verbreitung zur Verfügung. Solche offenen Daten können einerseits an sich zu mehr Transparenz führen, andererseits können darauf basierende Applikationen und *Mashups* (Rekombination von Daten) stärkere Transparenz schaffen. Ein Beispiel ist der sogenannte offene Haushalt in Österreich, in dem kommunalen Finanzdaten aus dem öffentlichen Sektor hinterlegt sowie vergleichbar und visualisierbar sind ([www.offenerhaushalt.at](http://www.offenerhaushalt.at)).
- *Tracking*-Systeme: Derartige Informationssysteme ermöglichen es, den aktuellen Status von Vorgängen in Politik und Verwaltung nachvollziehbar zu machen. Mögliche Einsatzgebiete sind Anträge, Gesetzgebungsprozesse, Vergabeprozesse oder staatliche Einnahmen und Ausgaben. Ein bekanntes Beispiel ist das Dokumentenmanagementsystem OPEN der Stadtverwaltung von Seoul. Dieses *Tracking*-System erlaubt es Bürger\*innen, die Genehmigungsprozesse der Stadtverwaltung online einzusehen.

---

## 4 Umsetzungsstand und Auswirkungen

In Deutschland wurden in den letzten zehn Jahren auf Bundes- und Landesebene insbesondere mit der Verbreitung von Informationsfreiheits- und Transparenzgesetzen, aber auch von *E-Government*- oder *Open-Data*-Gesetzen, verschiedene Formen digitaler Transparenz etabliert. Bis auf Bayern, Niedersachsen und Sachsen haben sich mittlerweile alle Bundesländer ein Informationsfreiheitsgesetz gegeben, das neben dem IfG des Bundes gilt. In Bremen, Hamburg und Rheinland-Pfalz wurden diese zu Transparenzgesetzen hin entwickelt und Transparenzportale eingerichtet, in denen Verwaltungsbehörden neben allgemeinen Informationen und Dokumenten auch proaktiv ihre Daten veröffentlichen. Auch das Land Berlin plant derzeit, sein Informationsfreiheitsgesetz zu einem Transparenzgesetz weiterzuentwickeln. Auf Bundesebene sowie in einigen Ländern und Kommunen existieren *Open-Data*-Portale, über die vor allem maschinenlesbare offene Regierungs- und Verwaltungsdaten zur freien Verfügung gestellt werden. Auch wurden in zahlreichen Kommunen Ratsinformationssysteme und Bürgerhaushalte etabliert. Viele Kommunen ermöglichen zudem mittlerweile Statusabfragen, etwa für den Bearbeitungsstand von Personalausweisen, Pässen oder Führerscheinen. Solche *Tracking*-Systeme werden zudem immer stärker durch private Anbieter etabliert. Etwa ist es mit der App „BAföG-direkt“ möglich, den aktuellen Bearbeitungsstand des eigenen Antrags auf Ausbildungsförderung einzusehen. Insgesamt handelt es sich dabei aber in der Regel eher um retrospektive Ergebnistransparenz als um Echtzeit-Transparenz von Prozessen.

Wie diese Formen der digitalen Transparenzschaftung wirken, kann noch nicht hinreichend beantwortet werden. Evaluationsberichte zu IfGs sowie der *Open-Data*- und Transparenzportale geben jedoch Hinweise auf Effekte dieser Transparenzmaßnahmen (Richter 2017, S. 243 ff.; Ziekow et al. 2012). Dabei muss grundsätzlich

zwischen der Wirkung von Transparenzmaßnahmen auf Staat und Verwaltung sowie auf Bürger\*innen unterschieden werden. In den letzten Jahren wurden Transparenzmaßnahmen in die Arbeits- und Handlungsroutinen der öffentlichen Verwaltung auf allen staatlichen Ebenen integriert und zahlreiche Informationen und Daten veröffentlicht. Zugleich scheint es aber weiterhin interne Widerstände zu geben, sodass Transparenzmaßnahmen in der deutschen Verwaltung häufig eher zögerlich und halbherzig umgesetzt werden. Zum Beispiel stellen Ziekow et al. (2012) in ihrer Evaluation des Informationsfreiheitsgesetzes des Bundes fest, dass sich dabei mitunter Ausweich- und Umgehungsverhalten wie der gezielte Einsatz von hohen Gebühren bei unliebsamen und zeitintensiven Anfragen oder eine veränderte Aktenführung etabliert haben.

In Bezug auf die Wirkung von Transparenzmaßnahmen auf Bürger\*innen zeigt eine erste Analyse, dass Informationsfreiheitsrechte bisher kaum genutzt werden und frei verfügbare Verwaltungsinformationen nur begrenztes Interesse finden. Dies ist keinesfalls eine deutsche Eigenheit, sondern deckt sich mit internationalen Erfahrungen (Richter 2017, S. 243 ff.). Und auch analoge Transparenzformate werden und wurden nicht häufiger genutzt. Vielmehr bieten digitale Transparenzmaßnahmen einer ohnehin schon politisch aktiven Minderheit von Netzaktivist\*innen und Journalist\*innen eine weitere Möglichkeit, Zugang zu staatlichen Informationen zu erhalten. Indem diese aber als Multiplikatoren wirken, kann digitale Transparenz dennoch bei den Bürger\*innen ankommen, wie sich auch in anderen Ländern gezeigt hat (Meijer et al. 2015, S. 509).

---

## 5 Perspektiven für Staat und Verwaltung

Aufgrund der fortschreitenden Digitalisierung von Politik und Verwaltung ist zu erwarten, dass entsprechende Angebote in Zukunft noch stärker gefordert und auch angeboten werden, weil digitale Transparenz schlicht einfacher, günstiger und schneller ist als analoge Transparenz. Immer mehr Bundesländer entwickeln ihre Informationsfreiheitsgesetze hin zu Transparenzgesetzen und setzen damit ein Zeichen für aktive Transparenz gegenüber den Bürger\*innen. Hier stechen vor allem die Stadtstaaten heraus. Ob sich hierzulande aber auch invasivere Formen der Transparenzschaaffung wie die Echtzeit-Transparenz von Beratungs-, Verhandlungs- sowie Entscheidungsprozessen durchsetzen, ist fraglich.

Die Entwicklung hin zu Transparenz scheint im deutschen Kontext vor allem von der Politik und der Zivilgesellschaft getrieben, allerdings noch nicht umfänglich in der deutschen Verwaltung(skultur) angekommen und verankert zu sein. Dies zeigt sich am Ausweich- und Umgehungsverhalten von Verwaltungen, beispielsweise an verschleppten oder unbeantworteten Informationsfreiheitsanfragen oder der fehlenden Einspeisung von (sinnvollen) Daten in *Open-Data*-Portale. Entsprechend sollte sichergestellt werden, dass als Reaktion auf die Forderung nach mehr Transparenz Prozesse nicht in arkane Räume verlagert werden. Transparenz darf kein ‚Papiertiger‘ sein, sondern ihre Implementation sollte sichergestellt werden.

Weiterhin werden in vielen Fällen neue Anwendungen und Prozesse geschaffen, die von Mitarbeiter\*innen betrieben und gepflegt werden müssen, welche über die entsprechenden Kompetenzen verfügen. Unabhängig von der eingesetzten Technologie können nicht alle Informationen aus Politik und Verwaltung veröffentlicht werden, weil sonst bloße Datenfriedhöfe ohne jeglichen Nutzen entstehen. Vielmehr muss der *Informationsbedarf* der Nutzer offener Verwaltungsinformationen stärker analysiert und als Grundlage für Transparenz in den Blick genommen werden. Neben digitalen Kompetenzen muss das Verwaltungspersonal daher im Sinne einer Daten- oder Informationskompetenz den Wert von transparenten Daten und Informationen erkennen können. Auf der anderen Seite muss gerade im Hinblick auf digitale Transparenz intensiver betrachtet werden, welche Kompetenzen die Bürger\*innen im Sinne einer *information literacy* mitbringen müssen, um mit offenen Daten und Informationen aus Politik und Verwaltung umzugehen, diese zu verstehen und zu verwenden. Hier muss diskutiert werden, wer für die Ausprägung solcher Kompetenzen verantwortlich ist und wie diese erfolgen kann. Zugleich verdeutlicht dies, dass weiterhin Formen von Transparenz nötig sind, die Bürger\*innen ohne IT-Kenntnisse nutzen können (analoge Transparenz).

Es bleibt abzuwarten, ob die digitale Entwicklung tatsächlich auch zu einer höheren effektiven Transparenz für die Bürger\*innen führt, oder aber lediglich große Daten- und Informationsbestände geschaffen werden, die nicht oder aber nur wirtschaftlich genutzt werden können. Die verantwortlichen Akteure aus Staat und Verwaltung, aber auch der Zivilgesellschaft und Wirtschaft, müssen hier genauer definieren, mit welchem Ziel beispielsweise *Open Government* verfolgt wird – zur Transparenzschaftung oder als Basis von Kollaboration und Innovation. Wenn Transparenz geschaffen werden soll, müssen Informationen so offengelegt werden, dass diese für Bürger\*innen oder zumindest für Medien als vermittelnde Instanz nutzbar sind. Wenn Kollaboration und Innovation als Ziele gesteckt werden, müssen hingegen stärker maschinenlesbare Daten offengelegt werden, die dann aber nicht mit Transparenzschaftung verwechselt werden dürfen.

---

## Literatur

- Bannister, Frank, und Regina Connolly. 2011. The trouble with transparency. A critical review of openness in e-government. *Policy and Internet* 3(1): 1–30.
- Bentham, Jeremy. 1843. *The works of Jeremy Bentham*, Hrsg. John Bowring. Nachdruck der Bowring-Originalausgabe von 1838–1843. Edinburgh: William Tait. 11 vols. Online Library of Liberty. <https://oll.libertyfund.org/titles/bentham-works-of-jeremy-bentham-11-vols>. Zugriffen am 16.02.2020.
- Cuccinello, Maria, Gregory Porumbesco, und Stephan Grimmelikhuijsen. 2017. 25 years of transparency research. Evidence and future directions. *Public Administration Review* 77(1): 32–44.
- Grimmelikhuijsen, Stephan, und Albert Meijer. 2014. Effects of transparency on the perceived trustworthiness of a Government organization. Evidence from an online experiment. *Journal of Public Administration Research and Theory* 24(1): 137–157.
- Han, Byung-Chul. 2012. *Transparenzgesellschaft*. Berlin: Matthes und Seitz.

- Hood, Christopher, und David Heald, Hrsg. 2006. *Transparency. The key to better governance?* Oxford: Oxford University Press.
- Lucke, Jörn von. 2010. Transparenz 2.0. – Transparenz durch E-Government. In *Transparenz. Multidisziplinäre Durchsichten durch Phänomene und Theorien des Undurchsichtigen*, Hrsg. Stephan Jansen, Eckhard Schröter und Nico Stehr, 396–412. Wiesbaden: VS.
- Meijer, Albert, Paul t'Hart, und Ben Worthy. 2015. Assessing government transparency. An interpretive framework. *Administration and Society* 50(4): 501–536.
- Richter, Philipp. 2017. Es werde Licht! Und es ward Licht? Zur Wirkung von Transparenz auf die Legitimität öffentlicher Verwaltung. *Politische Vierteljahrsschrift* 58(2): 234–257.
- Rzepka, Vincent. 2013. *Die Ordnung der Transparenz. Jeremy Bentham und die Genealogie einer demokratischen Norm*. Münster: LIT.
- Schedler, Kuno, und Isabella Proeller. 2011. *New public management*. Stuttgart: UTB.
- Wegener, Bernhard. 2006. *Der geheime Staat. Arkantradition und Informationsrecht*. Göttingen: Morango.
- Wewer, Göttrik. 2014. Allheilmittel Transparenz? Anmerkungen zur Diskussion. *Verwaltung und Management* 20(1): 4–18.
- Ziekow, Jan, Alfred Debus, und Elisabeth Musch. 2012. *Evaluation des Gesetzes zur Regelung des Zugangs zu Informationen des Bundes – Informationsfreiheitsgesetz des Bundes (IFG)*. Speyer: Institut für Gesetzesfolgenabschätzung und Evaluation.



---

# Informationsfreiheits- und Transparenzgesetze

Herbert Kubicek

## Inhalt

1	Begriffliche Klärungen .....	172
2	Konzeptionelle Grundlagen .....	175
3	Praktische Anwendung und Evaluation .....	180
4	Perspektiven für Staat und Verwaltung .....	183
	Literatur .....	184

---

## Zusammenfassung

Seit Beginn des 21. Jahrhunderts haben Bund und Länder per Gesetz den Zugang zu amtlichen Informationen grundlegend geändert. Mussten zuvor die Bürgerinnen und Bürger begründen, warum sie bestimmte Informationen einsehen wollten, muss nun die verpflichtete Behörde begründen, warum sie ein Zugangsbegehren ablehnt. In allgemeiner Form regeln dies Informationsfreiheitsgesetze (IFG) und Transparenzgesetze (TG). Daneben gibt es bereichsspezifische Gesetze, insbesondere zum Umwelt- und Verbraucherschutz, die auch regulatorische Ziele verfolgen. Der Zugang erfolgt auf Antrag oder per Veröffentlichungspflicht über zentrale Register oder Portale im Internet. In Evaluationsstudien wurde zwar für mehrere Gesetze untersucht, inwieweit, von wem und wozu die Zugangsrechte genutzt werden, am umfassendsten in einer Evaluation des Hamburgischen Transparenzgesetzes. Danach überwiegen private vor politischen Interessen der Nutzerinnen und Nutzer. Inwieweit die als Gesetzeszweck genannten gesellschaftlichen Effekte wie Transparenz und Beteiligung tatsächlich erreicht werden, kann wegen grundsätzlicher methodischer Schwierigkeiten der Gesetzesfolgenabschätzung nicht ermittelt werden. Fehlende empirische Nachweise können ein Grund sein, warum einige Bundesländer noch kein IFG verabschiedet haben.

---

H. Kubicek (✉)

ifib: Institut für Informationsmanagement Bremen GmbH, Universität Bremen, Bremen, Deutschland  
E-Mail: [kubicek@ifib.de](mailto:kubicek@ifib.de)

## Schlüsselwörter

Informationsfreiheit · Transparenz · Umweltinformationen ·  
Verbraucherinformationen · Gesetzesevaluation

---

## 1 Begriffliche Klärungen

Beim Zugang der Bürgerinnen und Bürger sowie der Wirtschaft und der Zivilgesellschaft zu amtlichen Informationen ist zwischen *allgemeinen* und *bereichsspezifischen* Zugangsregelungen zu unterscheiden.

### 1.1 Allgemeine Zugangsregelungen

Allgemeine Zugangsrechte gewähren die in der Kurzform als *Informationsfreiheitsgesetz (IFG)* oder *Transparenzgesetz (TG)* bezeichneten Gesetze des Bundes und einer Reihe von Bundesländern. Der offizielle Titel heißt beim Bund „*Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz – IFG)*“. Mit weitgehend ähnlichen Gesetzen, zunächst auf Landesebene, wurde seit 1998 in Deutschland schrittweise nachvollzogen, was international als *Freedom of Information* bezeichnet wird. Die Freiheit des Zugangs besteht darin, dass zuvor bestehende Beschränkungen und Begründungspflichten für den Zugang zu Informationen der Verwaltung aufgehoben werden. Bis dahin hatten nur die an einem Verwaltungsverfahren Beteiligten nach den *Verwaltungsverfahrensgesetzen* des Bundes und der Länder ein *Akteneinsichtsrecht*, das individuell begründet werden musste. Bürgerinnen und Bürger waren darauf angewiesen, welche Informationen die Behörden aufgrund bereichsspezifischer Vorschriften oder freiwillig veröffentlichen. Mit den neuen Regelungen ist der Zugang zu Informationen ohne Begründung möglich. Dies gilt neben dem Bund inzwischen mit gewissen Variationen für 12 der 16 Bundesländer, aber nicht für Bayern, Hessen, Niedersachsen und Sachsen (Abb. 1).

In Hamburg und Rheinland-Pfalz heißen die allgemeinen Zugangsgesetze „Transparenzgesetz“. Sie, aber nicht nur sie, gewähren zusätzlich den Zugang zu *Open Data*, d. h. zu maschinell weiter verarbeitbaren Daten der Verwaltungen unter freien Lizzenzen. Der Bund hat in seinem IFG seit 2006 trotz grundsätzlicher Empfehlungen aus der im Gesetz selbst vorgesehenen Novellierung 2011 lediglich die Gebührenregelungen 2013 geändert. Die Veröffentlichung von Verwaltungsdaten wurde in einer *Open-Data-Gesetz* genannten Änderung des *E-Government-Gesetzes* geregelt. Sehr speziell ist das Transparenzgesetz in Nordrhein-Westfalen aus dem Jahr 2009. Es schreibt insbesondere die Veröffentlichung von Beziügen, Vergütungen und Abfindungen aller Führungskräfte, Aufsichts- und Beiräte von Landesbehörden und Unternehmen vor, an denen das Land beteiligt ist.

Der Zugang erfolgt auf Antrag bei der Stelle, die über die begehrte Information verfügt, oder durch proaktive Bereitstellung näher bezeichneter Informationen über

**Abb. 1** Bundesländer mit und ohne IFG oder TG (Juni 2018) (Eigene Darstellung)



ein zentrales *Informationsregister* oder *Transparenzportal*. Der Anspruchsgegenstand „Information“ wird sehr weit gefasst. Im § 2 IFG des Bundes heißt es, dass *amtliche Information* „jede amtlichen Zwecken dienende Aufzeichnung, unabhängig von der Art ihrer Speicherung“ darstellt. Und weiter: „Entwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen, gehören nicht dazu“. Darunter fallen nicht nur Akten, sondern auch Korrespondenz, Protokolle, Vermerke, interne Dienstanweisungen, auf Papier oder digital, und auch Daten in Datenbanken und *E-Mails*.

Berechtigt (*Anspruchsinhaber*) ist jede natürliche und juristische Person, Deutsche ebenso wie Ausländer, wenn sie „rechtsfähig“ sind. Verpflichtet (*Anspruchsgegner*) werden die unmittelbaren und nachgeordneten Behörden des Bundes bzw. der Länder. Angesichts der Gründung von Gesellschaften durch staatliche Stellen und der Beauftragung von Unternehmen mit Aufgaben der Daseinsvorsorge werden diese auch verpflichtet. Ausgeschlossen sind in der Regel Gerichte, Parlamente, Sicherheitsbehörden und teilweise auch Rundfunkanstalten.

Unterschiedlich wird in den Flächenländern mit der Verpflichtung der Kommunen umgegangen. Nach herrschender Auffassung der Kommunen muss das jeweilige Land mit der gesetzlichen Verpflichtung zu bestimmten Leistungen auch die damit verbundenen Ausgaben finanzieren (*Konnektätsprinzip*). Da in den jüngeren Gesetzgebungsverfahren keine Einigung erzielt werden konnte, wurde z. B. im rheinland-pfälzischen Transparenzgesetz eine Übergangsfrist von fünf Jahren vereinbart und in Baden-Württemberg der entsprechende Paragraf bei der Verabschiebung im Landtag ausgenommen.

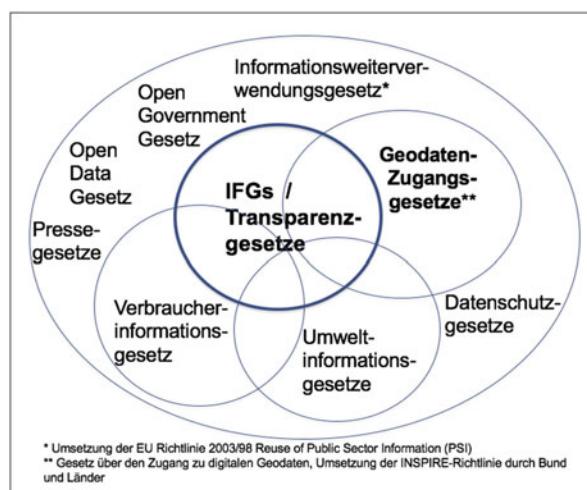
Da gerade auf der kommunalen Ebene ein allgemeiner Informationszugang am ehesten eine tatsächliche Kontrolle der Verwaltung erlauben würde, gibt es vor allem in Bayern und Nordrhein-Westfalen Initiativen für *kommunale Informationsfreiheitssatzungen*, die der Stadt- oder Gemeinderat verabschieden kann. In einer Reihe von Kommunen ist dies auch geschehen. Sie sind an das Bundes-IFG angelehnt, nennen im Einzelnen unterschiedliche zu veröffentlichte Dokumente oder Ablehnungsgründe. Ihr Ziel und ihr Gegenstand überschneiden sich mit denen von *Ratsinformationssystemen*. Ihre Bedeutung liegt auch darin, dass sie die oft stark eingeschränkten Informationsrechte der Ratsmitglieder erweitern und damit auch die repräsentative Kontrolle der Verwaltung durch die Bürgerinnen und Bürger auf kommunaler Ebene verbessern.

## 1.2 Bereichsspezifische Zugangsregelungen

Abb. 2 gibt einen Überblick über die wichtigsten Regelungen, ohne Anspruch auf Vollständigkeit und z. B. ohne Sozialgesetzbuch, Polizeigesetz u. ä.

Als erste bereichsspezifischen Regelung haben Bund und Länder 2005 die EU Richtlinie 2003/4 EG über den Zugang der Öffentlichkeit zu Umweltinformationen in *Umweltinformationsgesetzen (UIG)* umgesetzt. Sie schaffen den rechtlichen Rahmen für den freien Zugang zu sowie für die Verbreitung von Umweltinformationen. Sie beinhalten einen Auskunftsanspruch und eine Sollvorschrift für die proaktive elektronische Bereitstellung der vorhandenen Umweltdaten über ein zentrales (Landes-)Portal. Ein UIG hat als Spezialgesetz Vorrang vor den IFGen, so dass z. B. die Pflicht zur Meldung von Informationen an das zentrale Informationsregister in Bremen nicht für Umweltinformationen gilt, die bereits im Bremer Umwelt-Informationssystem veröffentlicht werden. Um diesen sachlich nicht begründbaren Unterschied auszugleichen, haben z. B. Berlin und Schleswig-Holstein bei der

**Abb. 2** Relevante Gesetze für den Zugang zu amtlichen Informationen (Eigene Darstellung)



---

Novellierung ihrer IFGen Umweltinformationen in die Liste der zu veröffentlichten Informationen aufgenommen. Dies gilt auch für die neueren Transparenzgesetze.

Einen den Transparenzgesetzen vergleichbaren Anspruch auf Nutzung und Weiterverarbeitung von Daten begründen die überwiegend 2009 erlassenen *Geodatenzugangsgesetze* des Bundes und der Länder in Umsetzung der INSPIRE-Richtlinie der EU. Sie verpflichten die datenhaltenden Stellen, auch der Kommunen, zur einheitlichen Erschließung konkret vorgegebener Daten durch geeignete Metadaten und Datendienste.

Mit dem „*Gesetz zur Verbesserung der gesundheitsbezogenen Verbraucherinformation (Verbraucherinformationsgesetz – VIG)*“ des Bundes von 2007, zuletzt geändert 2013, wird der Zugang zu Informationen über Lebens- und Futtermittel und Verbraucherprodukte eröffnet, die für die Gesundheit und Sicherheit der Verbraucherinnen und Verbraucher relevant sind. Hier wurde auf entsprechende Landesgesetze verzichtet, weil über Gesundheitsgefahren von Lebensmitteln, die bundesweit verkauft werden, auch bundesweit einheitlich informiert werden soll.

Das *Informationsweiterverwendungsgesetz (IWG)* und das *Open-Data-Gesetz* des Bundes begründen keinen zusätzlichen Anspruch auf Zugang, sondern regeln nur das Wie der Informationsweitergabe, falls Zugang gewährt wird. Das IWG schreibt diskriminierungsfreie Nutzungsbedingungen vor. Die als *Open-Data-Gesetz* bezeichnete Ergänzung des *E-Government-Gesetzes* des Bundes von 2017 beinhaltet eine Reihe von Prinzipien, die Bundesbehörden zu beachten haben, wenn sie Daten über das Portal *GovData.de* bereitstellen (§ 12a EGovG).

Die *Datenschutzgesetze* des Bundes und der Länder gewähren individuelle Auskunftsansprüche der Betroffenen gegenüber allen Stellen, die Daten zu ihrer Person verarbeiten. Sie setzen allen Zugangsgesetzen Grenzen, wenn es um personenbezogene oder auch nur personenbeziehbare Daten geht.

Zu erwähnen sind schließlich noch die *Pressegesetze* des Bundes und der Länder, die der Presse einen weitgehenden Auskunftsanspruch gewähren.

---

## 2 Konzeptionelle Grundlagen

Auch hier ist zwischen den allgemeinen und den bereichsspezifischen Regelungen zu unterscheiden.

### 2.1 Allgemeine Zugangsregelungen

Das politische Ziel des Paradigmenwechsels durch Informationsfreiheits- und Transparenzgesetze besteht in dem voraussetzungsfreien, möglichst einfachen und unbeschränkten Zugang zu allen vorhandenen amtlichen Informationen. Dieses Ziel ist selbst Mittel zur Erreichung höherrangiger Ziele. Als Gesetzeszwecke werden in den Landesgesetzen genannt:

- die Transparenz des Verwaltungshandelns,
- die Kontrolle staatlichen Handelns,
- die Nachprüfbarkeit von politischen Entscheidungen,
- die Stärkung demokratischer Beteiligungsrechte,
- die Nutzung des *Internet* für einen Dialog zwischen Staat und Gesellschaft.

Diese werden teilweise aus dem *Demokratie- und Rechtsstaatsgebot* (Art. 20 Abs. 1 GG) und der Informationsfreiheit nach Art. 5 Abs. 1 Satz 1 GG hergeleitet. Nach herrschender Auffassung handelt es sich dabei um Abwehrrechte, die Zensur verbieten, aber keinen unmittelbaren Anspruch auf Informationszugang begründen (Ziekow et al. 2012, S. 50 ff.). So garantiert Art. 5 Abs. 1 die ungehinderte Information aus öffentlich zugänglichen Quellen. Welche Quellen öffentlich zugänglich gemacht werden, entscheidet der Gesetzgeber. Dem *Öffentlichkeitsgebot* wird vor allem mittelbar durch den Auskunftsanspruch der Presse entsprochen, weil ein individueller Zugangsanspruch für jeden Einzelnen als praktisch nicht umsetzbar gilt (Mecklenburg und Pöppelmann 2009, S. 18 f.). Dieser ist auch deswegen nicht zwingend, weil nach Artikel 20 GG die Ausübung der Macht des Volkes in Wahlen und Abstimmungen und durch die Organe der Gesetzgebung, der vollziehenden Gewalt und der Rechtsprechung erfolgt. Die Begründung, dass das Volk seine Kontrollrechte nur ausüben kann, wenn es gleichen Zugang zu den Informationen der Verwaltung hat, entspringt somit keiner direkten Vorgabe des Grundgesetzes, sondern einem gewachsenen Verständnis des Demokratiegebots, das durch die neuen technischen Möglichkeiten des *Internet* gefördert wird, beim Bund und zwischen den Bundesländern aber durchaus noch Unterschiede aufweist. In den Bundesländern, die noch kein IFG erlassen haben, besteht keine verfassungsrechtliche Möglichkeit, dies einzuklagen.

Weil Zugangsrechte in Konflikt mit anderen Grundrechten geraten, beinhalten alle Zugangsgesetze weitgehend identische *Ablehnungsgründe*: Ein Zugang ist nicht zu gewähren, wenn die Bekanntgabe dem Schutz der öffentlichen Sicherheit, des internen Entscheidungsprozesses, von personenbezogenen Daten, von Betriebs- und Geschäftsgeheimnissen oder des geistigen Eigentums entgegensteht. Die Regelungen unterscheiden sich danach, ob sie die anderen Rechtsgüter als unbedingte Schranke oder Abwägungsgebot vorgeben, im Konfliktfall mit dem Datenschutz das Einverständnis der Betroffenen einzuholen ist oder durch Schwärzung ein Teilzugang gewährt werden kann.

Kritisch wird gegen diese Beschränkungen zweierlei eingewendet: Sicherheitsbelange werden oft nur als vage Gefährdungen vorgetragen und nicht als Risiken im Sinne von Schaden mal Eintrittswahrscheinlichkeit definiert, so dass eine annähernd objektive Güterabwägung kaum möglich ist. Und wenn ein laufender Entscheidungsprozess generell als Ablehnungsgrund gelten soll, kollidiert dies mit allen Angeboten der frühzeitigen Bürgerbeteiligung, die ja gerade stattfinden soll, bevor ein Entscheidungsprozess abgeschlossen ist.

Im Hinblick auf die Art des allgemeinen Zugangs kann man *drei Generationen* von Regelungen unterscheiden:

- Die *erste Generation* der IFG (1998 in Brandenburg, 1999 in Berlin, 2000 in Schleswig-Holstein und 2002 in NRW sowie im Bund 2006) konzentrierte sich auf den Informationszugang durch Antrag bei der Stelle, die über die begehrte Information verfügt, und schreibt dazu nur die Pflicht zur Veröffentlichung von Organisations- und Aktenplänen vor. Man muss die entsprechende Stelle kennen, um dieses Recht wahrzunehmen.
- Dieses Hindernis wurde 2006 mit dem BremIFG überwunden, das eine umfassendere Veröffentlichungspflicht für eine Reihe von näher bezeichneten Dokumenten und deren Bereitstellung über ein zentrales Informationsregister vorsieht.
- Die *dritte Generation* entstand 2012 mit dem HambTG, das das IFG des Landes ablöste und neben dem Zugang per Antrag und der Bereitstellung von Dokumenten in einem zentralen Register auch die Bereitstellung von Daten in maschinenlesbarer Form vorschreibt. Lag zuvor der primäre Zweck darin, dass sich Bürgerinnen und Bürger selbst informieren, ist nun nach dem Konzept *Open Data* auch beabsichtigt, dass der Zugang genutzt wird, um Informationen für Dritte aufzubereiten und weiterzuverbreiten. Dies war in den ersten IFGen noch ausdrücklich ausgeschlossen. Nun wird neben dem Ziel der Transparenz auch die Förderung wirtschaftlicher Innovationen verfolgt.

Die Gesetze unterscheiden sich auch im Hinblick auf die *Kontrollmechanismen*:

- Für die Kontrolle der Einhaltung wurde analog zu den Datenschutzgesetzen die Position von *Beauftragten für Informationsfreiheit* geschaffen. Sie wurde in allen Fällen den Datenschutzbeauftragten zusätzlich übertragen, die nun *Landes-/Bundesbeauftragte(r) für Datenschutz und Informationsfreiheit* (BfDI, LfDI) heißen. Sie dienen als Beschwerdestelle und haben Berichtspflichten.
- Alle Antragstellenden haben im Ablehnungsfall das Recht, sich zunächst an die/den BfDI bzw. LfDI zu wenden, die diesen Fällen nachgehen, jedoch nur argumentativ vermitteln können. Wenn dies zu keinem Erfolg führt, kann das zuständige *Verwaltungsgericht* angerufen werden.
- BfDI und LfDI haben eine in der Regel jährliche Berichtspflicht gegenüber den Parlamenten und der Öffentlichkeit. Die Berichte basieren im Wesentlichen auf eingegangenen Beschwerden.
- In einigen Fällen sind auch Statistiken der eingegangenen, bewilligten und abgelehnten Anträge zu führen und zu veröffentlichen.
- *Sanktionen* bei Nichtbefolgung der Vorschriften sind in keinem der Gesetze enthalten.

Neben dieser gesetzlich vorgesehenen Kontrolle gibt es die Plattform „*Frag den Staat*“, die im Sinne eines politischen *Watchdog* anbietet, Anträge auf Informationszugang an die richtige Stelle weiterzuleiten, mit Zustimmung der Antragstellenden die Antworten zu veröffentlichen und im Falle der Ablehnung Widerspruchsmöglichkeiten zu skizzieren. Eine Rechtsberatung ist nicht zulässig. Diese 2011 von der *Open Knowledge Foundation* gegründete Institution firmiert heute als „*Portal für*

Informationsfreiheit und Transparenz“ mit einem *Blog*, einem *Newsletter* und einer Datenbank mit über 30.000 Anfragen. Partner sind *Transparency International*, Mehr Demokratie e.V., die Deutsche Gesellschaft für Informationsfreiheit, das Netzwerk Recherche, der Deutsche Journalistenverband, der Chaos Computer Club u. a..

Einen systematischen rechtswissenschaftlichen Vergleich der allgemeinen Zugangsgesetze gibt es nicht. Mehr Demokratie e.V. und die *Open Knowledge Foundation* haben 2017 ein *Transparenzranking* veröffentlicht, in dem die vorliegenden Gesetze nach sechs Kriterien verglichen wurden:

- Informationsrechte
- Auskunftspflichten
- Ausnahmen
- Antragstellung
- Gebühren
- Informationsfreiheitsbeauftragte.

Von 100 möglichen Punkten hat Hamburg mit 69 Punkten den relativ besten Wert erreicht, das Saarland und Baden-Württemberg mit 32 Punkten den schlechtesten Wert. Bayern, Hessen, Niedersachsen und Sachsen ohne ein entsprechendes Gesetz erhielten 0 Punkte (Abb. 3)

Die Bezeichnung Transparenzranking ist allerdings irreführend, weil nicht die Transparenz der Verwaltungen verglichen wird, sondern nur die gesetzlichen Vorschriften. Diese in Punkten abzubilden und dann Punkte für unterschiedliche As-

<b>Platz im Ranking</b>	<b>Bundesland</b>	<b>erreichte Punktzahl</b>
1	Hamburg	69 %
2	Schleswig-Holstein	66 %
3	Bremen	62 %
4	Berlin	61 %
5	Rheinland-Pfalz	56 %
6	Nordrhein-Westfalen	45 %
7	Mecklenburg-Vorpommern	41 %
8	Brandenburg	39 %
9	Sachsen-Anhalt	38 %
10	Thüringen	32 %
10	Saarland	32 %
10	Baden-Württemberg	32 %
16	Bayern	0 %
16	Hessen	0 %
16	Niedersachsen	0 %
16	Sachsen	0 %
	Bund	38 %

**Abb. 3** Ranking der IFG und TG durch Mehr Demokratie e.V. und Open Knowledge Foundation (Open Knowledge Foundation 2017)

pekte zu addieren, ist methodisch jedoch problematisch. Das Ranking selbst ist auch nicht transparent, weil nicht angegeben wird, wer auf welche Weise die Punkte vergeben hat. Aber es ist immerhin ein erster Schritt, der zu Nachbesserungen führen könnte.

## 2.2 Bereichsspezifische Zugangsregelungen

Die bereichsspezifischen Zugangsgesetze verfolgen, wie erwähnt, auch andere Ziele und schaffen dementsprechend auch andere Regimes.

Nach den *Umweltinformationsgesetzen (UIG)* sollen die informationspflichtigen Stellen vor allem Informationen über den Zustand der Umwelt verbreiten, über Luft, Atmosphäre, Wasser, Boden, natürliche Lebensräume, Küsten und Meeresgebiete, gentechnisch veränderte Organismen u. a. m., sowie Maßnahmen, die sich darauf auswirken oder deren Schutz bezwecken. Diese Informationen sind über ein zentrales *Internet*-gestütztes Informationssystem zugänglich zu machen. Eine Veröffentlichungspflicht besteht neben Berichten auch für Daten aus der Überwachung, z. B. Emissionskontrolle und Umweltverträglichkeitsprüfungen, also Daten, die bei Unternehmen erhoben werden und Verstöße gegen Vorschriften offenbaren können, an deren Veröffentlichung die betroffenen Unternehmen kein Interesse haben. Die Gesetze geben dem öffentlichen Interesse jedoch explizit Vorrang und stellen fest, dass Emissionswerte keine Betriebsgeheimnisse sind.

Das *Verbraucherinformationsgesetz (VIG)* gilt für gesundheitsrelevante Informationen zu Lebensmitteln und Verbraucherprodukten und umfasst auch Informationen aus Überwachungsmaßnahmen und festgestellte Verstöße gegen Bestimmungen des Lebensmittel- und Futtermittelgesetzbuchs und des Produktsicherheitsgesetzes. Mit der Novellierung 2012 wurde der Geheimnisschutz aufgehoben, wenn das öffentliche Interesse überwiegt. Anträge auf Zugang zu Informationen über eine Rezeptur, von der Gesundheitsgefährdungen ausgehen, können nicht mehr mit dem Einwand des Betriebs- und Geschäftsgeheimnisses abgelehnt werden. Explizit regelt das Gesetz diese Abwägungen nur für den Zugang auf Antrag. Für die proaktive Veröffentlichung enthält es lediglich eine Kannbestimmung.

Diese ist jedoch explizit und detailliert im *Lebensmittel- und Futtermittelgesetzbuch* in Umsetzung einer EU-Richtlinie geregelt. Lebensmittelwarnungen sind ein heikles Problem. Sie sollen frühzeitig erfolgen, um Schäden zu begrenzen. Aber ein bloßer Verdacht, der sich bei gründlicher Prüfung nicht bestätigt, kann unwiderrufliche Folgen für das Unternehmen haben. § 40 LFGB ist der Versuch, eine Lösung im Verbraucherinteresse zu finden, die Fehlmeldungen vermeidet. Wenn bei einem Lebens- oder Futtermittel der hinreichende Verdacht auf eine Gefährdung der Sicherheit oder Gesundheit besteht oder gegen Vorschriften zum Schutz der Verbraucher verstößen wird, soll zunächst das betroffene Unternehmen eine Warnung veröffentlichen oder ein Produkt zurückrufen. Nur wenn dies nicht geschieht, informiert die zuständige (Überwachungs-)Behörde die Öffentlichkeit. Aufgrund einer Normenkontrollklage hat das Bundesverfassungsgericht die Regelung für teilweise unwirksam erklärt, weil das Gesetz keine Befristung der Speicherung

vorsieht. Grenzen haben Gerichte auch gesetzt, als Kommunen Beanstandungen bei Hygienekontrollen von Gaststätten mit dem Namen der betroffenen Gaststätten und mit den jeweiligen Bescheiden oder vereinfacht in Form einer Ampel veröffentlicht haben.

---

### 3 Praktische Anwendung und Evaluation

Über die Nutzung der Zugangsrechte liegen für fünf Gesetze Evaluationsstudien vor, weil in den Gesetzen eine Evaluation vorgeschrieben wurde:

- 2010 das IFG Mecklenburg-Vorpommern durch ein Gutachten im Auftrag des LfDI von Sabine Kuhlmann (DHV Speyer) und Michael Rodi (Universität Greifswald),
- 2010 das BremIFG durch das Institut für Informationsmanagement Bremen (ifib),
- 2012 das IFG des Bundes durch das Institut für Gesetzesfolgenabschätzung und Evaluation der Universität für Verwaltungswissenschaften Speyer (InGFA),
- 2012 das LIFG Rheinland-Pfalz durch das IngGFA,
- 2013 die Umsetzung der Veröffentlichungspflicht nach § 11 BremIFG durch das Institut für Informationsmanagement Bremen (ifib) und
- 2017 das Hamburgische TG durch das InGFA.

Die frühen Evaluationen des Bundes-IFG und des Landesgesetzes von Rheinland-Pfalz konzentrierten sich auf die Auskunftsanträge, da diese Gesetze im Gegensatz zum HambTG und dem novellierten BremIFG kaum Veröffentlichungspflichten vorsahen. Die 2017 durchgeführte Evaluationen des HambTG ist vom Themenspektrum und Methodeneinsatz die umfangreichste. Sie soll zusammen mit Befunden aus der Evaluation des BremIFG näher betrachtet werden. Dabei werden beispielhaft die methodischen Probleme und die Grenzen einer verlässlichen Bestimmung der Wirkungen und damit der Erreichung der Gesetzeszwecke deutlich.

Eine *retrospektive Gesetzesfolgenabschätzung* soll den Zielerreichungsgrad einer Rechtsvorschrift erfassen sowie die Auswirkungen des Gesetzes und auch die nicht-intendierten Effekte (insbesondere Vollzugs-/Implementierungsprobleme) identifizieren, um Optimierungspotenziale aufzuzeigen. Dies geschieht aus einer rechtswissenschaftlichen und einer sozialwissenschaftlichen Perspektive. Letztere soll die unterschiedlichen Sichtweisen des politischen Gesetzgebers, der verpflichteten Behörden und der begünstigten unterschiedlichen Nutzergruppen gegenüberstellen. Methodisch werden dafür quantitative und qualitative Erhebungen durchgeführt. Neben Statistiken zu den Angeboten und ihrer Nutzung gehören dazu auch Befragungen der verschiedenen *Stakeholder*. Die „Öffentlichkeit“, an die sich die Gesetze wenden, wird nach dem Speyerer Modell nur insoweit erfasst, als sie das Transparenzportal nutzt oder in sozialen Medien auf Ansprachen reagiert. Mit dieser Selektion wird nicht der Teil der Öffentlichkeit erfasst, der die gewährten Zugangs-

rechte nicht kennt und/oder aus unterschiedlichen Gründen nicht wahrnehmen will oder kann. In der Evaluation des BremIFG wurde daher auch eine repräsentative telefonische Bevölkerungsumfrage durchgeführt, bei der sich zeigte, dass 86,7 % noch nie etwas von einem IFG für Bremen gehört haben (Kubicek und Lippa 2010, S. 31).

Ein zentraler Indikator ist der *Output*, d. h. Anzahl und Art der bereitgestellten Informationen (Dokumente und Daten), aufgeschlüsselt nach Dokumentenart, Themenbereich und bereitstellender Behörde und verpflichteter Organisation. Im Fall von Hamburg hat sich eine relativ starke Konzentration gezeigt. Von knapp 66.000 Informationen auf dem Transparenzportal entfallen 65 % auf *Beschlüsse und Baugenehmigungen* bzw. 60 % auf die Themenbereiche Infrastruktur sowie Politik und Wahlen. Die absoluten Zahlen sind jedoch kein aussagekräftiger Indikator. So hat Bremen die Anzahl der veröffentlichten Dokumente fast verdoppelt, als knapp 30.000 auch länger zurückliegende Pressemitteilungen der Senatskanzlei eingestellt wurden.

Aussagekräftig ist hingegen eine Veröffentlichungsquote, um zu prüfen, ob alle zu veröffentlichten Informationen auch tatsächlich veröffentlicht wurden. Dies wurde in der Hamburger Evaluation nur für *Verträge der Daseinsvorsorge* geprüft, weil hier häufig Betriebs- und Geschäftsgeheimnisse als Ausnahmetatbestand angeführt werden. Von über 3000 Verträgen wurden nur 736 veröffentlicht. Ein ähnlicher Verstoß gegen die Veröffentlichungspflichten wurde in einer Bremer Umsetzungsstudie festgestellt. Dort wurde als zusätzliche Methode auch für andere Dokumententypen wie Verwaltungsvorschriften, Planungen, Protokolle und Gutachten geprüft, ob diese außerhalb des Transparenzportals veröffentlicht werden. Tatsächlich war dies bei einigen Behörden in nennenswertem Umfang der Fall. Dies widerlegt die These, Behörden würden aus *Geheimhaltungsinteresse* Dokumente zurückhalten. Vielmehr erschien es vielen Stellen einfacher, Dokumente auf der *Web*-Seite ihrer Behörde zu veröffentlichen, statt sie erst mit Metadaten zu versehen und in das zentrale Portal einzustellen. Sie waren davon überzeugt, dass Interessenten diese Dokumente mit der *Google*-Suche auch finden. Die proaktive Veröffentlichung unterbleibt auch wegen einer *Organisationslücke* (Kubicek 2013). Im Gegensatz zur Bearbeitung von Anträgen gab es in den beispielhaft untersuchten vier Behörden keine expliziten Regelungen, wer was bei welchen Dokumenten in Bezug auf eine Veröffentlichung entscheiden soll, z. B. ob ein Ablehnungsgrund vorliegt und was gegebenenfalls geschwärzt werden soll. Diese rechtliche Entscheidung ist völlig getrennt von der, wer ein Dokument mit Metadaten versieht und in das Portal lädt und wer sich um die Aktualisierung kümmert. Auch die Hamburger Evaluation berichtet, dass es trotz eines Vorbereitungsprojekts mit einer behördenübergreifenden Arbeitsgruppe erhebliche Unterschiede bei der Regelung der Verantwortlichkeiten gibt (Herr et al. 2017, S. 86).

Die Nutzung der Portale (*Outcome*) umfasst die Anzahl der gestellten Anträge und der Zugriffe. In Hamburg ist die Anzahl der Anträge von knapp 1400 im Jahr 2013 auf 628 im Jahr 2015 zurückgegangen, als das Transparenzportal *online* ging. Die proaktive Veröffentlichung kann somit den Aufwand für die Bearbeitung von Einzelanfragen reduziert haben. Allerdings kann die Zahl der Anträge nicht exakt

bestimmt werden, da telefonische Anfragen und Auskünfte, bei denen kein Bezug auf das IFG genommen wird, von den Sachbearbeitern zumeist nicht als Antrag nach IFG aufgefasst und daher nicht dokumentiert werden. Bei der Novellierung des BremIFG wurde daher wegen der nicht genauen Abgrenzbarkeit des Gegenstands, der zu erwartenden Unvollständigkeit und des großen Aufwandes über alle Sachgebiete hinweg, die Pflicht zur Führung einer Antragsstatistik aufgehoben. Stattdessen wurde 2016 eine jährliche Berichtspflicht über die Erfüllung der pro-aktiven Veröffentlichungspflicht der in § 11 vorgegebenen Liste von verschiedenen Arten von Dokumenten eingeführt, deren Zahl über das zentrale Portal gut zu ermitteln ist.

In Hamburg haben die meisten Anträge Privatpersonen *aus persönlichem Interesse* gestellt, gefolgt von Rechtsanwälten (rund 10 %) und an dritter Stelle von Wirtschaftsunternehmen oder Personen mit wirtschaftlichem Interesse. Der Anteil der Anträge von Journalisten, Wissenschaftlern, Verbänden u. a. liegt bei jeweils ein bis zwei Prozent (Herr et al. 2017, S. 188). 20 % haben angegeben, dass ihr Informationsbedarf mit den zugänglich gemachten Informationen „voll“ und 45 % „eher“ befriedigt wurde (Herr et al. 2017, S. 158).

Für das Transparenzportal wird statistisch nur die *Anzahl der abgerufenen Seiten*, aber nicht der Besucher berichtet. Von April 2015 bis Februar 2017 sind die monatlichen Abrufe von rund zwei Millionen auf 300.000 bis 200.000 zurückgegangen, die Anzahl der abgerufenen Detailseiten hingegen ist seit September 2016 gestiegen. Das kann bedeuten, dass zunächst das Portal selbst Aufmerksamkeit geweckt hat und erst mit der Zeit die Nutzung für den Zugang zu konkreten Informationen zugenommen hat. Wer das Portal wozu genutzt hat, wurde in einer *Online-Umfrage* unter den Nutzenden ermittelt, an der jedoch nur 412 Personen teilgenommen haben. Mit etwas mehr als 60 Prozent steht auch hier der Abruf von Privatpersonen aus persönlichem Interesse im Vordergrund, davon 52 % mit einem Interesse an einem konkreten Vorgang und 28 % aus einem allgemeinen politischen Interesse, gefolgt von Wirtschaftsunternehmen (17 %) und Wissenschaftlerinnen und Wissenschaftlern mit rund 13 %. Interessenverbände einschließlich Umweltverbände machen knapp vier Prozent aus, Rechtsanwälte knapp zwei Prozent (Herr et al. 2017, S. 140 f.). Fast ein Viertel der Befragten sind Dauernutzer mit mehr als zehn Nutzungen in den letzten 12 Monaten.

Hauptgrund für die gesetzlich vorgeschriebene Evaluation war die Sorge, dass dadurch ein zu hoher *Aufwand bei den Behörden* erzeugt werden könnte. Im Fall Hamburg hält sich dieser Aufwand in den Fachabteilungen nach der durchgeführten Umfrage in Grenzen. Den erhofften Kulturwandel in Richtung mehr Offenheit sehen sowohl die Behördenleitungen als auch die Beschäftigten und die befragten Nutzerinnen und Nutzer rund zur Hälfte, die Behördenleitungen zu einem etwas höheren Anteil als die Beschäftigten.

Der Evaluationsbericht räumt ein, dass die als Zweck des Gesetzes genannte bessere *Kontrolle der Verwaltung* durch die Veröffentlichungen nicht als kausale Wirkung ermittelt, sondern nur als Einschätzung erfasst werden konnte. Diese Zielerreichung wird sowohl in der Nutzerbefragung als auch in der Befragung der Mitglieder des Beirats überwiegend skeptisch gesehen. Die Nutzungsmotive liegen eher im persönlichen und wirtschaftlichen Bereich. Dass Baugenehmigungen zu den am meisten aufgerufenen Dokumenten zählen, zeigt dies ganz konkret.

Umweltinformationsgesetze existieren auf Bundes- und Länderebene seit mehr als zwanzig Jahren, weil dies durch eine EU-Richtlinie vorgeschrieben wurde. Dazu konnte keine einzige abgeschlossene, sondern nur eine laufende Evaluation für das UIG des Bundes gefunden werden. Sie wurde seit 2016 bis Mai 2019 vom Unabhängigen Institut für Umweltfragen durchgeführt.

Für das *Verbraucherinformationsgesetz, das für Bund und Länder gilt*, hatte der Deutsche Bundestag um einen Erfahrungsbericht und eine Evaluation gebeten, die 2010 in Form von drei Studien in Auftrag gegeben wurde (Deutscher Bundestag 2010). Einige Empfehlungen wurden in der Novellierung 2012 berücksichtigt. So wurde die Berufung auf Betriebsgeheimnisse durch eine mehrstufige Abwägung mit dem öffentlichen Interesse in Abhängigkeit von drohenden Gesundheitsgefahren ersetzt. Rechtsverstöße durch Grenzwertüberschreitungen müssen veröffentlicht werden.

---

## 4 Perspektiven für Staat und Verwaltung

Transparenz und Informationszugang haben in Politik und Politikwissenschaft einen hohen Wert. Teilweise wird anhand der Reichweite und Verbindlichkeit der Zugangsrechte auf die Transparenz von Staat und Verwaltung geschlossen oder sogar der Grad der Demokratisierung beurteilt. Aber kann man begründet behaupten, dass die Bundesländer, die noch kein IFG haben, weniger transparent oder daher weniger demokratisch sind als die anderen? Wohl kaum.

Mit den Zugangsrechten und Veröffentlichungspflichten wollen die Gesetzgeber in den Ländern die Transparenz des Verwaltungshandelns, die Kontrolle staatlichen Handelns, die Nachprüfbarkeit von politischen Entscheidungen und die Stärkung demokratischen Beteiligungsrechte verbessern. Einige Gesetze schreiben eine wissenschaftliche Evaluation vor. Das Speyerer Institut für Gesetzesfolgenabschätzung hat dazu die erwähnte Methodik einer kombinierten rechtswissenschaftlichen und einer empirisch-sozialwissenschaftlichen Analyse entwickelt. Wie auch bei anderen Evaluationskonzepten werden dabei *Output*, *Outcome* und *Impact* ermittelt. Während *Output*, die bereitgestellten oder zugänglich gemachten Informationen, und *Outcome*, Umfang und Art der Nutzung, grundsätzlich gut ermittelt und zugeordnet werden können, bestehen prinzipielle Schwierigkeiten, den *Impact*, die beabsichtigten und auch nicht beabsichtigten Wirkungen, zu erfassen. Bei den genannten Gesetzeszwecken handelt es sich um einen solchen *Impact*. Man kann, wie das Speyerer Institut, zwar die Besucher des Hamburger Portals befragen, ob sie die Hamburger Verwaltung als transparent empfinden. Das Ergebnis ist jedoch nicht besonders aussagekräftig, da es „die“ Verwaltung nicht gibt, sondern stets Unterschiede zwischen den Ressorts bestehen, und weil auch nicht genau definiert ist, was die Antwortenden unter „transparent“ verstehen. Ob dadurch die Kontrolle und Nachprüfbarkeit staatlichen Handelns verbessert wird, hängt nicht nur davon ab, ob kritische Informationen auch veröffentlicht werden – bei vielen Verträgen ist dies trotz gesetzlicher Vorschriften nicht der Fall -, sondern auch davon, ob die einzelnen Bürgerinnen und Bürger in der Lage sind, den Inhalt der Dokumente zu verstehen.

und zu bewerten, und auf welchen Wegen eine Kontrolle oder Nachprüfung erfolgen kann, wenn Unstimmigkeiten festgestellt werden.

Noch schwieriger ist die Beantwortung der Frage, ob und wenn ja, wie sich Staat und Verwaltung durch die Erweiterung der Informationszugangsrechte verändert haben. Was Verwaltungen veröffentlichen und was nicht, hängt von vielen Faktoren ab. Ein einziger Skandal kann das Vertrauen, das durch Informationszugang gewachsen ist, wieder zerstören. Auch ist zu berücksichtigen, dass Verwaltungen immer auch Wege finden, intern so zu kommunizieren, dass Veröffentlichungspflichten umgangen werden.

Bei den bereichsspezifischen Gesetzen wie den Umweltinformationsgesetzen und dem Verbraucherinformationsgesetz ist es methodisch einfacher, Wirkungen auf die Verbraucher und Rückwirkungen auf Unternehmen und Verwaltungen zu ermitteln. Aber auch hier gibt es Erhebungs- und Zurechnungsprobleme. Welchen Beitrag die gesetzlichen Zugangsrechte und Informationspflichten zum gesundheitlichen Schutz vor Umweltbelastungen und Schadstoffen in Lebensmitteln oder Kinderspielzeug geleistet haben, ist nur punktuell und mit hohem Aufwand zu ermitteln, weil dabei zu viele Faktoren und Bedingungen eine Rolle spielen. Zudem wird gerade im Umweltbereich deutlich, dass gesicherte Informationen über Schadstoffbelastungen, wie z. B. in der Dieselkrise, nicht automatisch zu Maßnahmen zu deren Reduzierung führen.

Als Fazit bleibt daher festzuhalten, dass es einen weit verbreiteten Glauben an die demokratieförderlichen Wirkungen von Informationszugangsgesetzen gibt, jedoch kein fundiertes Wissen. Durch aufwändige und langfristig angelegte Studien könnte man wie in epidemiologischen Studien mehr Evidenz gewinnen. Doch es fehlt anscheinend die politische Bereitschaft, dafür die erforderlichen Mittel bereit zu stellen, sei es, dass man es so genau nicht wissen will oder dass man weiß, dass auch dann keine sicheren Erkenntnisse entstehen.

Aus gesellschaftlicher Perspektive ist bei der Beurteilung dieses Befundes zu bedenken, dass die hier behandelten individuellen Zugangsrechte nur einer und im Vergleich zu anderen wohl der schwächste und häufig überschätzte Mechanismus zur Sicherung von Transparenz und Kontrolle staatlichen Handelns sind. Wir haben das Parlament mit Regierungs- und Oppositionsfaktionen, staatliche Aufsichtsbehörden, zivilgesellschaftliche *Watchdogs* und als stärksten Faktor die unabhängigen und professionellen Medien Presse und Rundfunk. Die von den Medien aufgedeckten Skandale der letzten zehn Jahre haben ohne Zweifel einen vielfach größeren Einfluss auf politische und gesellschaftliche Veränderungen als die in dieser Zeit geschaffenen erweiterten Zugangsgesetze.

---

## Literatur

- Deutscher Bundestag. 2010. Bericht der Bundesregierung über die Ergebnisse der Evaluation des Verbraucherinformationsgesetzes. Drucksache 17/1800 vom 14.05.2010. <http://dip21.bundestag.de/dip21/btd/17/018/1701800.pdf>. Zugegriffen am 05.06.2020.
- Herr, Marius, Christoph Müller, Bettina Engewald, Axel Piesker, und Jan Ziekow. 2017. Abschlussbericht zur Evaluation des Hamburgischen Transparenzgesetzes. Speyer: Univers-

- sität Speyer. [http://www.foev-speyer.de/files/de/fbpdf/\\_vti\\_cnf/InGFA/Abschlussberichte/AB\\_EvaluationdesHmbTG.pdf](http://www.foev-speyer.de/files/de/fbpdf/_vti_cnf/InGFA/Abschlussberichte/AB_EvaluationdesHmbTG.pdf). Zugriffen am 05.06.2020.
- Kubicek, Herbert. 2013. Die Umsetzung der Veröffentlichungspflicht nach § 11 BremIFG. Bremen: Institut für Informationsmanagement Bremen (ifib). [https://www.ifib.de/publikationsdateien/ifib\\_IFG\\_Umsetzung.pdf](https://www.ifib.de/publikationsdateien/ifib_IFG_Umsetzung.pdf). Zugriffen am 05.06.2020.
- Kubicek, Herbert, und Barbara Lippa. 2010. Evaluation des Bremer Informationsfreiheitsgesetzes (BremIFG). Bericht über die Umsetzung des BremIFG sowie seine Auswirkungen im Zeitraum 1. August 2006 bis 31.12.2009. Bremen: Institut für Informationsmanagement Bremen (ifib). [https://www.ifib.de/publikationsdateien/20100401\\_IFG-Evaluation\\_Bericht\\_ifib\\_barrierefrei-2.pdf](https://www.ifib.de/publikationsdateien/20100401_IFG-Evaluation_Bericht_ifib_barrierefrei-2.pdf). Zugriffen am 05.06.2020.
- Mecklenburg, Wilhelm, und Benno H. Pöppelmann. 2009. Informationsfreiheitsgesetz. Gesetztexte, Kommentierungen, Fallbeispiele, Erläuterungen. Berlin: Deutscher Journalisten-Verband e.V. <https://netzwerkrecherche.org/wp-content/uploads/2014/07/ifg-kommentar-buch.pdf>. Zugriffen am 05.06.2020.
- Open Knowledge Foundation. 2017. Transparenzranking. Vergleich der Informationsgesetze in Deutschland. <https://okfn.de/projekte/transparenzranking/>. Zugriffen am 05.06.2020.
- Ziekow, Jan, Alfred Debus, und Elisabeth Musch. 2012. *Evaluation des Gesetzes zur Regelung des Zugangs zu Informationen des Bundes – Informationsfreiheitsgesetz des Bundes (IFG)*. Speyer: Institut für Gesetzesfolgenabschätzung und Evaluation.



---

# Datenschutz

Göttrik Wewer

## Inhalt

1 Klärung der Begriffe .....	188
2 Konzeptionelle Grundlagen .....	190
3 Praktische Anwendungsfelder .....	191
4 Tatsächliche Auswirkungen .....	193
5 Perspektiven für Staat, Verwaltung und Politik .....	195
Literatur .....	197

---

## Zusammenfassung

Der Schutz der Persönlichkeit und der Privatsphäre ist im digitalen Zeitalter, wo wir gewollt oder ungewollt überall Datenspuren hinterlassen, wichtiger denn je, aber es ist fraglich, ob dieses Ziel mit dem herkömmlichen Ansatz erreicht werden kann. Welches der Rechtsregime, die global miteinander konkurrieren, als erfolgreicher gelten kann, hängt auch davon ab, welche Kriterien angelegt werden. Insgesamt leidet die Debatte darunter, dass über abstrakte Prinzipien gestritten wird, aber empirische Kenntnisse darüber, was deren Anwendung tatsächlich bewirkt, weitgehend fehlen. Die Diskussion über Datenschutz bedarf einer empirischen Wende.

---

## Schlüsselwörter

Datensicherheit · Informationelle Selbstbestimmung · Persönlichkeitsschutz ·  
*Privacy Paradox · Post-Privacy*

---

G. Wewer (✉)

Lorenz-von-Stein-Institut für Verwaltungswissenschaften an der Christian Albrechts-Universität zu Kiel, Kiel, Deutschland

E-Mail: [g.wewer@bvdp.de](mailto:g.wewer@bvdp.de)

## 1 Klärung der Begriffe

Staat und Verwaltung haben, soweit sie das konnten, schon immer Daten erhoben, um ihre Aufgaben erfüllen und um planen zu können. Die amtliche Statistik, die früh technische Hilfsmittel einsetzte, um große Mengen von Daten möglichst zügig verarbeiten zu können, ist Ausdruck dieses Bestrebens. Wenn heute eine „evidenzbasierte Politik“ gefordert wird, die sich (allein) auf Zahlen, Daten und Fakten stützen soll, dann liegt dem häufig ein technokratisches Politikverständnis zugrunde, das nicht wahrhaben möchte, dass Daten nie für sich selbst sprechen, sondern immer interpretiert werden müssen, und dass dabei Einstellungen und Werthaltungen, Interessen und Ideologien eine Rolle spielen. Dass Staat und Verwaltung Daten brauchen, wenn sie wirksam steuern wollen, und dass politische Entscheidungen wissenschaftliche Erkenntnisse nicht ignorieren sollten, ist davon unberührt.

Mit der automatisierten Datenverarbeitung, die verstärkt in der zweiten Hälfte des 20. Jahrhunderts einsetzte, als Lochkarten und Großrechner durch die ersten *Computer* ersetzt wurden, begann auch die Debatte darüber, wie die Daten der Bürger, die von Staat und Verwaltung gesammelt wurden, besser vor eventuellem Missbrauch geschützt werden könnten. Zwar sorgte das Amtsgeheimnis, das strafbewehrt ist, in der Regel dafür, dass die Angaben der Bürger die behördlichen Aktenschränke nicht verließen, aber je mehr Daten Staat und Verwaltung über sie sammeln, verarbeiten und – zumindest theoretisch – verknüpfen konnten, desto größer erschien das Risiko, ihnen gegenüber zum „gläsernen Bürger“ zu werden. Zwar veröffentlichten Statistikämter nur aggregierte Datensätze, die keine Rückschlüsse auf den Einzelnen zulassen, aber wenn das, was Behörden alles über den Bürger wissen, beliebig miteinander verknüpft werden könnte oder in die falschen Hände geraten sollte, dann drohten durchaus Gefahren für Freiheit, Sicherheit und Demokratie („1984“).

Diese Debatte führte in Hessen 1970 zum weltweit ersten Datenschutzgesetz, dem sieben Jahre später das Bundesdatenschutzgesetz folgte. Bis 1981 hatten alle deutschen Länder einschlägige Gesetze. Mit der „Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ (Datenschutzrichtlinie) versuchte die Europäische Gemeinschaft 1995 erstmals, die nationalen Regelungen in den Mitgliedstaaten vorsichtig zu harmonisieren. Mit der „Verordnung 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“ (Datenschutz-Grundverordnung), die im Unterschied zu einer Richtlinie unmittelbar geltendes Recht und 2018 in Kraft getreten ist, hat die Europäische Union (EU) einen weiteren Schritt auf diesem Weg getan.

Ergänzt werden soll die Datenschutz-Grundverordnung durch eine spezielle Verordnung für die elektronische Kommunikation, für die die EU-Kommission Anfang 2017 einen Entwurf vorgelegt hat. Diese Verordnung würde die „Richtlinie 2002/58/EG über die Verarbeitung personen-bezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation“ (kurz: *ePrivacy-Richtlinie*) aus dem Jahre 2002 ablösen, die gewisse Vorgaben für den Datenschutz in der Telekommunikation gemacht hat, jedoch kein unmittelbar geltendes Recht darstellte. Sie wurde 2009 durch

die sogenannte *Cookie-Richtlinie* (2009/136/EG) ergänzt, die eine ausdrückliche Einwilligung der Betroffenen bei der Nutzung solcher Instrumente vorsah.

Geschützt werden sollen nach dem Gesetz nicht alle Daten, sondern nur jene, die sich auf eine konkrete Person beziehen oder beziehbar sind, so dass Rückschlüsse auf deren Identität oder Verhalten gezogen werden könnten. *Personen-bezogene Daten* sind „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“ (§ 3 Abs. 1 BDSG). Solche Daten dürfen von Behörden oder von Unternehmen nur dann verarbeitet werden, wenn das gesetzlich ausdrücklich erlaubt ist, wenn der Betroffene ausdrücklich einverstanden ist oder wenn ein übergeordnetes Interesse geltend gemacht werden kann (etwa weil eine bestimmte Dienstleistung, die vom Kunden gewünscht wird, ohne die Nutzung dieser Daten nicht erbracht werden kann). Da relativ wenige Datenpunkte genügen, um einen Menschen, der sich selbst nicht offenbart, aber zum Beispiel eine *Website* besucht oder einen Dienst im Internet genutzt hat, „bestimmbar“ zu machen, sind letztlich nahezu alle Daten, die sich auf Individuen beziehen, *personen-bezogene Daten*, die nur unter engen Vorgaben verarbeitet werden dürfen.

Der Begriff „Datenschutz“, der einst aus dem Arbeitsschutz beim Umgang mit Maschinen abgeleitet wurde, ist missverständlich: Im Kern geht es nicht darum, die Daten zu schützen (*data protection*), obwohl auch das getan werden muss, sondern um Menschenwürde, Persönlichkeit und Privatsphäre (*privacy protection*), weil ohne individuelle Rückzugsräume weder eine freiheitliche Gesellschaft noch eine funktionierende Demokratie denkbar sind. Datenschutz ist also kein Selbstzweck, sondern lediglich Mittel zum Zweck: Möglichst zu verhindern, dass die Menschen „gläsern“ werden, damit sie nicht nach Belieben kontrolliert, überwacht und manipuliert werden können.

Anfangs meinte der Begriff den Schutz der Daten selbst vor Verlust, Diebstahl oder Manipulation, also den *technischen Datenschutz* (Datensicherheit, *IT-Sicherheit*), was bis heute eine anspruchsvolle Aufgabe ist, aber nach und nach setzte sich die Auslegung durch, vorrangig ginge es um den Schutz der Person, also den *individuellen Datenschutz*. Die verschiedenen Sichtweisen überlagern sich bis heute: Man kann Datenschutz als Schutz der Privatsphäre und der Persönlichkeit verstehen, als das Recht auf informationelle Selbstbestimmung oder als Schutz vor missbräuchlicher Datenverarbeitung.

Das „Recht auf informationelle Selbstbestimmung“, das das *Bundesverfassungsgericht* 1983 im sogenannten Volkszählungsurteil kreiert hat, zielt darauf ab, dass der Einzelne selbst entscheiden und kontrollieren kann, was mit seinen Daten geschieht. Aus dem allgemeinen Persönlichkeitsrecht hat das Gericht 2008 außerdem ein „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ abgeleitet, das auch als IT-Grundrecht, *Computer-Grundrecht* oder Grundrecht auf digitale Intimsphäre bezeichnet wird. Ähnlich wie die Unverletzlichkeit der Wohnung soll auch die Unverletzlichkeit des eigenen Rechners gegen Eingriffe von außen geschützt werden (Hermann 2010). Eine *Online*-Durchsuchung durch staatliche Behörden ist nur gestattet, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein besonders wichtiges Rechtsgut bestehen und ein Richter diese Maßnahme angeordnet hat.

## 2 Konzeptionelle Grundlagen

Wen man von autoritären Regimen absieht, in denen Datenschutz nichts gilt, dann lassen sich in funktionierenden Demokratien zwei Grundmodelle unterscheiden: das amerikanische Modell, in dem die Erhebung, Speicherung und Verwertung von Daten, auch personen-bezogenen Daten, grundsätzlich erlaubt ist, solange das nicht ausdrücklich untersagt ist („Erlaubnis mit Verbotsvorbehalt“), und das deutsche bzw. europäische Modell, wonach die Verarbeitung solcher Daten prinzipiell verboten ist, wenn das Gesetz keine Ausnahme vorsieht oder der Betroffene förmlich zugestimmt hat („Verbot mit Erlaubnisvorbehalt“). Nach dem einen Modell soll der Bürger vorsorglich vor der Verwertung seiner Daten geschützt werden, wenn er das nicht ausdrücklich gebilligt hat, nach dem anderen Modell ist zunächst alles erlaubt, solange es nicht Missbräuche gibt, die unterbunden werden sollen.

Welches dieser beiden Grundmodelle erfolgreicher ist, ist nicht einfach zu beantworten, weil dann zunächst die Frage geklärt werden muss, was unter Erfolg verstanden werden soll. Der Schutz der Privatsphäre steht sicher an erster Stelle, aber wenn die meisten den Allgemeinen Geschäftsbedingungen, die den Anbietern von Produkten und Diensten eine ungehinderte Nutzung der Daten ihrer Kunden erlauben, pauschal zustimmen, ohne sie auch nur gelesen zu haben, dann geben sie ihre Rechte mehr oder weniger freiwillig auf. Zu verhandeln gibt es ohnehin nichts: Entweder stimmt man zu oder man kann das Angebot nicht nutzen. Eine Lösung für dieses „Privacy Paradox“ (Alessandro Acquisti), wonach uns Datenschutz theoretisch wichtig ist, wir aber im Alltag jede Menge Daten bereitwillig preisgeben, ohne zu wissen, was damit geschieht, hat noch niemand gefunden.

Ähnliches gilt für die „informierte Einwilligung“ oder „informierte Zustimmung“ (*informed consent*) zur Verarbeitung der eigenen Daten, die nach geltendem Recht zudem absolut freiwillig und bewusst erfolgen soll. Bei der zunehmenden Vernetzung der Geräte und Dienste im *Internet of Things*, bei *Smart Homes* und „intelligenten“ Fahrzeugen, die mit zahlreichen Sensoren und Kameras ausgestattet sind, halten es manche für eine bloße Illusion, immer zu wissen, welche Daten man gerade produziert und wer sie alles zu welchen Zwecken auswertet. Wenn Menschen trotz Bedenken überwiegend mitmachen, weil sie die Angebote derart einfach, bequem und attraktiv finden, oder schlichtweg resignieren, weil man sich dem sowieso nicht entziehen kann, dann wäre das sicher kein Indikator für die Wirksamkeit dieses Schutzmodells.

Fraglich ist außerdem, ob der faktische Datenschutz das einzige Kriterium sein kann, wenn es um die Bewertung der verschiedenen Schutzregime geht. In allen anderen Politikfeldern geht es darum, das „magische Fünfeck“ von Transparenz, Partizipation, Effektivität, Effizienz und Legitimation möglichst optimal auszubalancieren (Wewer 1997, S. 479). Ob diese Balance beim Datenschutz gelungen ist, lässt sich nicht nur anhand des Verhaltens derjenigen diskutieren, die eigentlich geschützt werden sollen, sondern auch entlang der Frage, welches Schutzregime mehr technische Innovationen, neuartige Geschäftsmodelle und ökonomische Marktdurchdringung zulässt. Abgesehen von SAP gehört heute kein europäisches oder deutsches Unternehmen mehr zu den wirklich großen Spielern in der digitalen Ökonomie, was nicht nur schlecht ist für den Standort, sondern auch die Chancen mindert, eigene technische Standards global durchzusetzen. Das gilt auch für den Datenschutz.

Wenn Daten das „Öl des 21. Jahrhunderts“ sind, das Innovationen antreibt, wie manche sagen, dann stellt sich die Frage, ob das tradierte Schutzregime, das wir in Deutschland kennen, noch geeignet ist, die Zielkonflikte, die sich bei der Nutzung von Daten ergeben, produktiv aufzulösen. Wer schon vorab sagen muss, wozu die Daten, die er über Personen erheben möchte, unbedingt erforderlich sind, kann kaum etwas Neues entdecken. Wenn Daten nur sparsam und zweckgebunden erhoben werden dürfen und umgehend gelöscht werden müssen, wenn sie dafür nicht mehr benötigt werden, wird es schwierig, Auswertungen vorzunehmen, die Muster erkennen lassen und segensreich etwa bei der Behandlung von Krankheiten sein können. Wenn Staat und Verwaltung ihre Daten nutzen würden, um Leistungen zu erbringen und ihnen unnötige Laufwege zu ersparen, dürften die meisten Bürger das eher begrüßen.

Wer den Gedanken nicht aufgeben möchte, dass der Mensch ein paar Geheimnisse bewahren können muss, wenn er Mensch bleiben will, der muss darüber nachdenken, wie eine Restsphäre an Privatheit geschützt werden kann, obwohl wir im digitalen Zeitalter praktisch überall Datenspuren hinterlassen (acatech 2013; Buchmann 2012, 2013). Was als schützenswert gilt, wird selbst innerhalb Europas unterschiedlich gesehen: Während die Schweden im *Internet* nachsehen können, was ihr Nachbar verdient, ist das Steuergeheimnis in Deutschland eine Heilige Kuh. Das amerikanische Schutzregime orientiert sich an einer doppelten Testfrage (*Reasonable Expectation of Privacy Test*): Hat der Einzelne selbst seine Daten so verwahrt, dass er *subjektiv* davon ausgehen konnte, sie seien geschützt, und würde die Gesellschaft seine persönlichen Erwartungen an Datenschutz und *Privatsphäre objektiv* als vernünftig ansehen oder nicht? Anders gesagt: Wer *Facebook* nutzt, sollte nicht beklagen, seine Daten seien dort nicht geschützt; das kann man vorher wissen. Was die meisten Bürger nicht als schutzwürdig ansehen, das verdient in diesem Regime auch keinen Schutz.

Da es praktisch kaum noch möglich ist, keine digitalen Fußabdrücke zu hinterlassen, plädieren manche dafür, sich lieber im „Leben nach der Privatsphäre“ (*post-privacy*) einzurichten (Heller 2011), statt sich an einen formalen Datenschutz zu klammern, der längst ziemlich ausgeöholt ist. Statt gegen die allgegenwärtige Überwachung anzukämpfen, die sich ohnehin nicht verhindern lasse, sollten wir besser dafür sorgen, dass auch die Mächtigen gläsern werden, empfiehlt der amerikanische Futurist David Brin (1999), denn wenn alles offen zutage liege, könne niemand mehr Macht durch das Ausnutzen der Schwächen anderer ausüben. Die totale Transparenzgesellschaft, in der es keine persönlichen Geheimnisse gibt, ist allerdings eine inhumane Kontrollgesellschaft (Han 2012).

---

### 3 Praktische Anwendungsfelder

Alle, die in den Mitgliedstaaten der Europäischen Union (EU) *personen-bezogene Daten* verarbeiten, müssen seit dem 25. Mai 2018 die „Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“ vom 24. Mai 2016 (2016/679) beachten. Insofern ist das Anwendungsfeld dieses Rechtsregimes zumindest in Europa universell.

Anders als die frühere Richtlinie, die von den EU-Staaten jeweils in nationales Recht überführt werden musste und dabei auch modifiziert werden konnte, ist die neue Datenschutz-Grundverordnung (DSGVO) unmittelbar geltendes Recht, das für ein einheitliches Datenschutzniveau in ganz Europa sorgen soll. Angesichts einer Vielzahl von Öffnungsklauseln ist zwar strittig, inwieweit das gelingt, aber dass hier ein großer Schritt hin zu einer europäischen Harmonisierung getan worden ist, lässt sich nicht bestreiten. Das soll es insbesondere Konzernen, die auf dem ganzen Globus Geschäfte machen, erschweren, Firmen in den Ländern zu errichten, die das niedrigste Schutzniveau für *personen-bezogene Daten* und/oder das größte Vollzugsdefizit der Aufsichtsbehörde aufweisen. Die Verarbeitung von Daten, die in Europa erhoben werden, soll europäischem Recht unterliegen (Wohnsitzprinzip), damit nicht amerikanische oder chinesische Unternehmen behaupten können, für sie würden andere Regeln gelten, da sie ihren Stammssitz nicht in Europa hätten. Ein „Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)“ vom 5. Dezember 2017 (2017/0003 [COD]), die 2019 in Kraft treten, aber nach dem Vorschlag des Europäischen Parlaments eine mindestens einjährige Übergangsfrist enthalten sollte (*ePrivacy*-Verordnung), soll diese Grundsätze auf die elektronische Kommunikation übertragen. „The principle of confidentiality should apply to current and future means of communication, including calls, internet access, instant messaging, applications, e-mail, internet phone calls and personal messaging provided through social media.“

Die europäische Verordnung überträgt im Grunde das deutsche Schutzregime auf ganz Europa und ergänzt es um einige Punkte. Zu den Grundsätzen, die an das deutsche Gesetz erinnern, zählen (nach Art. 5 Abs. 1 DSGVO):

- Die Rechtmäßigkeit der Datenverarbeitung, also eine rechtliche Grundlage dafür oder eine persönliche Einwilligung;
- eine Verarbeitung nach Treu und Glauben, die als redlich und anständig angesehen werden kann;
- Transparenz, die einerseits durch Informationspflichten und andererseits durch Auskunftsrechte gewährleistet werden soll;
- Datenschutz durch Technik (*Privacy by Design*), datenschutzfreundliche Vorstellungen (*Privacy by Default*), Zertifizierungsverfahren und Datenschutzzertesiegel;
- eine eindeutige und legitime Zweckbindung;
- Datenminimierung, also ihre Begrenzung auf das notwendige Maß, das für den Zweck angemessen und erheblich ist;
- die Richtigkeit der Daten, die möglichst immer auf dem aktuellen Stand sein sollen, und das unverzügliche Löschen von Daten, die im Hinblick auf ihre Zwecke unrichtig sind;
- eine zeitliche Begrenzung der Speicherung, insbesondere von Daten, die eine Identifizierung ermöglichen;
- Integrität und Vertraulichkeit: Wer personen-bezogene Daten verarbeitet, hat geeignete technische und organisatorische Vorkehrungen zu treffen, um deren

---

Sicherheit zu gewährleisten, die Daten also vor unbefugter und unrechtmäßiger Verarbeitung und vor ungewolltem Verlust, unbeabsichtigter Zerstörung oder Schädigung zu schützen.

Zu den Punkten, in denen die europäische Verordnung über deutsche Gesetze hinausgeht, gehören insbesondere:

- Ein umfassendes Auskunftsrecht, zu dem jetzt auch das Recht auf eine Kopie der gesammelten Daten gehört (Art. 15 DSGVO);
- ein „Recht auf Datenportabilität“, wonach man seine Daten mitnehmen kann, wenn der Anbieter von Diensten gewechselt wird (Art. 20 DSGVO);
- das bisher nur gerichtlich konstruierte „Recht auf Vergessen“, wenn der Zweck, für den diese Daten gespeichert wurden, nicht mehr gegeben ist (Art. 17 DSGVO);
- ein „Recht auf Berichtigung“, wonach Betroffene unrichtige Angaben über sie korrigieren lassen können (Art. 16 DSGVO).

Nach der deutschen Rechtslage durfte der Abschluss eines Vertrages nicht davon abhängig gemacht werden, dass jemand zustimmte, gezielte Werbung zu bekommen oder seine Daten für Adresshandel bereitzustellen (Kopplungsverbot). Das galt allerdings nur, wenn der Betroffene praktisch keine Alternative zu diesem Angebot hatte. Nach der neuen Verordnung ist eine Einwilligung nur dann gültig, wenn sie sich ausschließlich auf den Vertragszweck bezieht. Was inhaltlich davon getrennt werden kann, muss auch getrennt werden und bedarf einer gesonderten Einwilligung, die auch gesondert widerrufen werden kann, ohne den Vertragszweck zu gefährden (Art. 7 Abs. 4 DSGVO).

Die Verordnung bekräftigt ferner das Recht betroffener Personen, nicht Entscheidungen unterworfen zu werden, die ausschließlich automatisiert erfolgen, aber rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen können (Art. 22 DSGVO) (dazu Bull 2017 sowie Martini und Nink 2017).

Bei Missachtung dieser Grundsätze drohen erhebliche Sanktionen: Bis zu 20 Mio. € oder bei Unternehmen bis zu 4 % des weltweiten Umsatzes des vorangegangenen Geschäftsjahres sowie weitere Maßnahmen der Aufsichtsbehörden (Art. 83 Abs. 5 lit.a DSGVO). Spürbare Sanktionen sollen dafür sorgen, dass die Vorschriften nicht „zahnlos“ bleiben; der Rahmen dürfte aber allenfalls dann ausgeschöpft werden, wenn Unternehmen sie vorsätzlich oder fahrlässig, systematisch und dauerhaft ignorieren. Alles andere wäre unverhältnismäßig.

---

## 4 Tatsächliche Auswirkungen

Dass Vorschriften universell gelten, muss noch nicht bedeuten, dass sie überall eingehalten werden. Wie groß die Vollzugsdefizite des deutschen Bundesdatenschutzgesetzes und der einschlägigen Landesgesetze gewesen sind, ist empirisch noch nicht aufgearbeitet worden. Peter Schaar hat es das „am wenigsten beachtete deutsche Gesetz“ genannt. Wenn das eine zutreffende Diagnose sein sollte, dann würde das die Frage aufwerfen, warum so viele dieses Gesetz nicht beachtet haben:

Weil die Aufsicht nicht funktionierte oder weil die meisten die Vorschriften für überzogen hielten? Anfang 2018 haben nach Angaben des Konzerns in Europa 282 Millionen Menschen, mehr als die Hälfte der Bevölkerung, jeden Tag *Facebook* genutzt, sich also gegen den Schutz ihrer *Privatsphäre* entschieden, in Deutschland nutzten 31 Millionen Menschen mindestens einmal im Monat dieses Angebot, die Nutzer der Dienste *WhatsApp* (34 Millionen täglich aktive deutsche Nutzer) und *Instagram* (17 Millionen deutsche Nutzer monatlich), die ebenfalls von diesem Konzern angeboten werden, noch gar nicht gerechnet. Wenn man noch die anderen sogenannten Sozialen Medien hinzunimmt, dann haben die meisten schon längst über dieses Gesetz abgestimmt. Dass in Umfragen viele sagen, sie würden diesen Plattformen nicht vertrauen, ändert nichts daran, dass sie sie trotzdem nutzen. Ein zeitgemäßer Datenschutz dürfte das nicht beklagen, sondern müsste das tatsächliche Verhalten als Ausgangspunkt nehmen, um Auswege aus dieser Widersprüchlichkeit anzubieten.

Auch wenn Bußgelder nach der neuen Verordnung deutlich höher ausfallen können, ist aus verschiedenen Gründen nicht damit zu rechnen, dass die Vollzugsdefizite europaweit wesentlich kleiner werden. Nicht nur das deutsche, sondern auch das europäische Schutzregime ist relativ ineffizient und ineffektiv. Die Lücke zwischen Norm und Wirklichkeit eröffnet vor allem Chancen für Kanzleien, die sich auf Abmahnungen spezialisiert haben. Das trifft besonders kleinere Betriebe, die mit den Vorschriften überfordert sind, während ausgerechnet die großen Datensammler mit großen Rechtsabteilungen Wettbewerbsvorteile bekommen. Dass die erweiterten Pflichten für Vereine, Verbände und Unternehmen zu einem besseren Schutz der *Privatsphäre* führen, ist nicht zu erwarten.

Die Debatte um einen zeitgemäßen Datenschutz krankt daran, dass immer wieder über abstrakte Prinzipien gestritten wird, aber kaum empirische Erkenntnisse über *Output*, *Outcome* und *Impact* unseres Schutzregimes vorliegen: Ist unsere *Privatsphäre* heute besser geschützt als 1970, als in Deutschland das erste Gesetz zu diesem Zweck verabschiedet wurde (historischer Längsschnitt)? Sollte das nicht der Fall sein, dann wären fast fünf Jahrzehnte Datenschutz keine Erfolgsgeschichte, sondern eine Geschichte der Illusionen. Ist die *Privatsphäre* der Deutschen heute *de facto* besser geschützt als die der Norweger, der Neuseeländer oder der Amerikaner (internationaler Querschnitt)? Wäre das nicht der Fall, dann müsste man klären, woran das liegt. Nur dann könnte der Gesetzgeber daraus lernen. *Wollen* die Deutschen wirklich überall informiert zustimmen oder zeigen sie mit ihrem Verhalten, dass ihnen im Zweifel anderes wichtiger ist? *Können* wir tatsächlich immer informiert zustimmen oder ist das im Zeitalter von *Big Data* oder des *Internet of Things* eine Vorstellung von gestern? Wer gar nicht ahnt, welche Daten sein *Smart Home* oder „intelligente Assistenten“ ständig an wen liefern, der kann seine *Privatsphäre* beim besten Willen nicht schützen. Nach dem amerikanischen Schutzregime dürfte jemand, der sich digitale „Assistenten“ wie *Alexa* ins Wohnzimmer stellt, das auch gar nicht erwarten. Notwendig wäre eine öffentliche Diskussion darüber, welchen Datenschutz die Bürger wirklich wollen.

Was die neuen Vorschriften bewirken, kann man erst in einigen Jahren seriös ermitteln. In der ersten Zeit haben sie vor allem Unruhe und Unsicherheit gebracht und bürokratischen Mehraufwand, weil jeder, der einen *Newsletter* bezieht, erneut

gefragt werden musste, ob er ihn weiterhin haben möchte, und das Ergebnis gespeichert und länger dokumentiert werden musste, als das bei der viel kritisierten Vorratsdatenspeicherung jemals gefordert worden ist, mit deren Hilfe Straftaten besser aufgeklärt werden sollten. Ob der volkswirtschaftliche Mehraufwand, der dadurch verursacht worden ist, tatsächlich durch einen besseren Schutz der *Privatsphäre* aufgewogen wird, ist noch nicht bewiesen. Nicht jede Aufregung, die entstanden ist, war tatsächlich begründet, aber dass sie überhaupt entstehen konnte, zeigte, dass die neue Rechtslage noch keine Rechtssicherheit gebracht hat.

Ein zeitgemäßer Datenschutz muss Lösungen finden im Spannungsfeld zwischen technologischen Innovationen und menschlichem Verhalten, die praktikabel sind und akzeptiert werden (Bull 2011). Rechte der Nutzer, die von den meisten ignoriert werden, nützen letztlich niemandem. Um besser zu wissen, was Datenschutz in Deutschland praktisch bedeutet, brauchen wir dringend eine „empirische Wende“ in der Debatte. Dazu gehört auch die Frage, ob eigentlich „Big Brother“ oder „Big Business“ im digitalen Zeitalter das größere Risiko für die Persönlichkeit und die *Privatsphäre*, aber auch für die Öffentlichkeit und die Demokratie darstellt. Dass einmal kommerzielle „Datenfresser“ wie *Alphabet (Google)*, *Amazon* oder *Facebook* (Kurz und Rieger 2011) mehr über jeden von uns wissen würden als die gewählte Regierung oder irgendwelche Behörden (vielleicht mit Ausnahme der amerikanischen *National Security Agency*) ahnte in den Anfängen der Debatte um Datenschutz niemand.

---

## 5 Perspektiven für Staat, Verwaltung und Politik

Formell mögen wir in Europa die strengsten Gesetze haben, aber faktisch dürfte der Schutz der *Privatsphäre* in Deutschland kaum besser sein als in etlichen anderen funktionierenden Demokratien, die weniger rigoros darauf setzen, die Erhebung, Speicherung und Verarbeitung von *personen-bezogenen Daten* zunächst einmal grundsätzlich zu verbieten. Dass das deutsche bzw. europäische Rechtsregime ein „Exportschlager“ sei, wird häufig behauptet, aber selten bewiesen. Belege dafür, dass sich Firmen, die Daten verwerten, aus diesem Grund bewusst in Europa ansiedeln, gibt es nicht; auch nicht dafür, dass Kunden europäische Dienstleister in Anspruch nehmen, (nur) weil diese diesem Rechtsregime unterliegen. *Facebook* hat zwar angekündigt, diese Vorschriften für seine europäischen Kunden zu beachten, aber noch vor Inkrafttreten der Verordnung 1,5 Milliarden außereuropäische Kundendaten, die bis dahin in Irland verarbeitet wurden, von dort abgezogen.

Was die Bürger von dem paternalistischen Schutzanspruch des Staates halten, der in diesem Rechtsregime sichtbar wird, kann man daran ablesen, dass die meisten den Allgemeinen Geschäftsbedingungen kommerzieller „Datenkraken“ unbesehen zustimmen, weil sie gerne deren Dienste nutzen möchten. Obwohl viele ihnen nicht vertrauen, wie Umfragen zeigen, nutzen sie dennoch sogenannte Soziale Medien wie *Facebook*, *Twitter* oder *Whatsapp*. Die begrenzte Wirksamkeit des gesetzlichen Datenschutzes röhrt auch daher, dass sich viele von denen, die eigentlich geschützt werden sollen, im Zweifel gegen diesen Schutz entscheiden. Das wirft die Frage auf,

ob es nicht klüger sein könnte, bestimmte Verwertungen von *personen-bezogenen Daten* zu verbieten, die eine Mehrheit eindeutig nicht will, und dieses Verbot mit spürbaren Strafen zu bewehren, statt die Nutzung solcher Daten generell zu untersagen, ohne dass sich jemand ernsthaft daran hält. Manches, was in den letzten Jahren als formaler Verstoß gegen geltendes Recht gerügt worden ist, hatte materiell für die *Privatsphäre* der Betroffenen kaum eine Bedeutung.

Die staatlichen Beauftragten für den Datenschutz haben sich über den Umweg Brüssel den Status eines Quasi-Verfassungsorgans erarbeitet, der demokratie- und staatstheoretisch nicht unproblematisch ist. Die sogenannte Artikel 29-Gruppe sollte eigentlich die Europäische Kommission nur beraten – was auch beinhaltet hätte, dass ihre Vorschläge verworfen werden –, hat aber die Chance, dass es praktisch keine institutionellen Gegenspieler gibt, dazu genutzt, Politik zu machen – nicht zuletzt in eigener Sache. Wenn praktisch allein Datenschützer bestimmen, was „richtiger“ Datenschutz ist und was nicht, kommt die notwendige Abwägung mit anderen Interessen zu kurz, die sonst auf allen Politikfeldern stattfindet. Niemand würde akzeptieren, wenn nur Verbraucherschützer definieren, was Verbraucherschutz sein soll, oder allein die Umweltschützer, was Umweltschutz ist. Sonst könnte man auch die Autobauer festlegen lassen, welche Schadstoffe ihre Diesel ausstoßen dürfen.

Dass nachgeordnete Behörden sich der Exekutive entziehen und bei der Legislative unterschlüpfen, wie das etwa dem „Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein“ gelungen ist, mag man noch hinnehmen, auch wenn Parlamente eigentlich nicht dafür geeignet sind, Behörden zu führen. Dass nachgeordnete Behörden von Ressorts einer Regierung keiner Fachaufsicht, sondern nur einer Dienstaufsicht unterliegen, ist ordnungspolitisch eine Fehlentscheidung. Beauftragte für den Datenschutz zu einer Art „fünfter Gewalt“ aufzuwerten, obwohl davon nichts im Grundgesetz steht, ist – bei allem Respekt vor der Wichtigkeit der *Privatsphäre* – ein Irrweg, der mit zu der Kluft zwischen Recht und Realität geführt hat, die auf diesem Politikfeld herrscht. Der europäische Gesetzgeber und die europäische Gerichtsbarkeit haben ihnen eine Unabhängigkeit zugeschrieben, die in den Verfassungen der Mitgliedstaaten nicht vorgesehen ist und die diese Behörden *de facto* dem System der *checks and balances* entzieht, das für Demokratien unerlässlich ist.

Das gegenwärtige Rechtsregime führt dazu, dass Staat und Verwaltung sich künstlich dümmer stellen, als sie das eigentlich sein müssten. Die Vorgabe, Daten nur „sparsam“ sammeln zu dürfen, hindert sie daran, umfassend Daten zu sammeln, um ihre Aufgaben besser erfüllen und um besser steuern zu können. Im digitalen Zeitalter ist Datensparsamkeit ein Anachronismus. Während in der Wirtschaft im „Internet der Dinge und der Dienste“ allenthalben mit *Big Data*, Künstlicher Intelligenz, *Machine Learning* und Robotern experimentiert wird, um Erfahrungen zu sammeln und neue Geschäftsmodelle zu entwickeln, spielt die Frage, was das alles für Staat und Verwaltung im 21. Jahrhundert bedeuten könnte, kaum eine Rolle. Ohne eine übergreifende Datenstrategie wird es aber weder eine „digitale Verwaltung“ noch *Smart Government* geben. Ein „schwacher Staat im Netz“ (Schallbruch 2018), der seine Bürger kaum noch schützen kann, kündigt indirekt das Versprechen auf, auf dem das staatliche Gewaltmonopol beruht.

Das Prinzip der Zweckbindung schließt aus, dass die eine Behörde weiß, über welche Informationen andere verfügen. Das eröffnet nicht nur dem Missbrauch staatlicher Leistungen Tür und Tor, weil ein Abgleich von Daten untereinander nicht zulässig ist, sondern erschwert es Staat und Verwaltung auch, bessere Dienstleistungen anzubieten. Den Bürger vorsorglich darauf hinweisen, dass sein Ausweis in einem halben Jahr abläuft, dürfen sie nur, wenn das Gesetz das ausdrücklich gestattet. Jubilaren zu einem runden Geburtstag gratulieren dürfen Bürgermeister auch nur, wenn deren Daten genau zu diesem Zweck gespeichert worden sind. Das alles widerspricht dem Motto „die Daten sollen laufen, nicht die Bürger“. Wenn sich daran nichts ändert, wird Deutschland beim *Electronic Government* im Vergleich mit anderen Nationen weiterhin im unteren Mittelfeld dümpeln. Die mangelnde Attraktivität staatlicher Angebote führt dazu, dass kommerzielle Unternehmen mehr und mehr staatliche Funktionen zu übernehmen versuchen.

Europa hat nur dann eine Chance, seine Grundsätze weltweit zu etablieren, wenn es mit einer Stimme spricht. Ob das in Zukunft besser gelingt als bisher, muss sich zeigen. Deutschland ist hier kein gutes Vorbild. Der einheitliche europäische Rechtsrahmen ändert nichts daran, dass bei uns ein Bundesbeauftragter und sechzehn Landesbeauftragte diese Normen unterschiedlich interpretieren können. Wer als Unternehmen seine Dienste bundesweit anbieten möchte, muss sich im Grunde bei allen absichern. Das führt auch in den Behörden zu unnötiger Doppel- und Dreifacharbeit und zu einem beträchtlichen Koordinierungsaufwand sowie insgesamt zu einer Zersplitterung von Ressourcen. Wer in einer globalen Datenökonomie Standards setzen und es mit den Giganten des *Internet* aufnehmen möchte, muss Kräfte bündeln, statt beim Schutz von Persönlichkeit und *Privatsphäre* Kleinstaaterei zu betreiben.

---

## Literatur

- acatech, Hrsg. 2013. *Privatheit im Internet. Chancen wahrnehmen, Risiken einschätzen, Vertrauen gestalten*. Berlin/Heidelberg: Springer Vieweg.
- Brin, David. 1999. *The transparent society. Will technology force us to choose between privacy and freedom?* Reading: Perseus.
- Buchmann, Johannes, Hrsg. 2012. *Internet Privacy. Eine multidisziplinäre Bestandsaufnahme*. Berlin/Heidelberg: Springer Vieweg.
- Buchmann, Johannes, Hrsg. 2013. *Internet privacy. Options for adequate realisation*. Berlin/Heidelberg: Springer Vieweg.
- Bull, Hans Peter. 2011. *Informationelle Selbstbestimmung. Vision oder Illusion? Datenschutz im Spannungsverhältnis von Freiheit und Sicherheit*, 2., aktual. Aufl. Tübingen: Mohr Siebeck.
- Bull, Hans Peter. 2017. Der „vollständig automatisiert erlassene“ Verwaltungsakt. Zur Begriffsbildung und rechtlichen Einhegung von „E-Government“. *Deutsches Verwaltungsblatt* 132(7): 409–417.
- Han, Byong-Chul. 2012. *Transparenzgesellschaft*. Berlin: Matthes & Seitz.
- Heller, Christian. 2011. *Post-Privacy. Prima leben ohne Privatsphäre*. München: C.H. Beck.
- Hermann, Christoph. 2010. *Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Entstehung und Perspektiven*. Frankfurt a. M.: Peter Lang.

- Kurz, Constanze, und Frank Rieger. 2011. *Die Datenfresser. Wie Internetfirmen und Staat sich unsere Daten einverleiben und wir die Kontrolle darüber wiedererlangen*. Frankfurt a. M.: Fischer.
- Martini, Mario, und David Nink. 2017. Wenn Maschinen entscheiden ... Vollautomatisierte Verwaltungsverfahren und der Persönlichkeitsschutz. *Neue Zeitschrift für Verwaltungsrecht – Extra* 36(10): 1–14.
- Schallbruch, Martin. 2018. *Schwacher Staat im Netz. Wie die Digitalisierung den Staat in Frage stellt*. Wiesbaden: Springer.
- Wewer, Götztrik. 1997. Vom Bürger zum Kunden? Beteiligungsmodelle und Verwaltungsreform. In *Politische Beteiligung und Bürgerengagement in Deutschland*, Hrsg. Ansgar Klein und Rainer Schmalz-Brunns, 448–488. Baden-Baden: Nomos.



# Cybersicherheit

Wolf J. Schünemann

## Inhalt

1 Klärung des Begriffs .....	200
2 Theoretische Grundlagen .....	203
3 Praktische Anwendung .....	205
4 Künftige Entwicklung .....	207
Literatur .....	208

## Zusammenfassung

Die Sicherheit informationstechnischer Systeme ist eine wesentliche Herausforderung moderner Verwaltung unter den Bedingungen der Digitalisierung. Der Beitrag legt die soziotechnischen Bedeutungsdimensionen der Cybersicherheitspolitik differenziert dar. Es geht also um das technische Kernverständnis von *IT-Sicherheit* ebenso wie um die mehr theoretisch als praktisch-empirisch zu unterscheidenden Dimensionen einer inneren Cybersicherheit und einer äußeren Cybersicherheit. Im Überblick über die theoretischen Stränge der aktuellen Debatte wird insbesondere der Ansatz der *Versicherheitlichung* (Sekuritisierung) vorgestellt. Ferner werden das chronische Attributionsproblem und die Verantwortung des Staates für die Cybersicherheit innerhalb des eigenen Territoriums sowie gegenüber anderen Staaten geschildert. Konkretisiert wird die Cybersicherheitspolitik am Beispiel Deutschlands.

## Schlüsselwörter

IT-Sicherheit · Kritische Infrastrukturen · Versicherheitlichung · Cyber Security · Attributionsproblem

---

W. J. Schünemann (✉)

Institut für Sozialwissenschaften, Universität Hildesheim, Hildesheim, Deutschland  
E-Mail: [wolf.schuenemann@uni-hildesheim.de](mailto:wolf.schuenemann@uni-hildesheim.de)

## 1 Klärung des Begriffs

Die Sicherheit informationstechnischer Systeme ist eine wesentliche Herausforderung moderner Verwaltung unter den Bedingungen der Digitalisierung. Sie ist Voraussetzung für einen effektiven und effizienten Einsatz von *E-Government*-Lösungen und notwendige Bedingung für die vertrauensvolle Nutzung entsprechender Angebote durch Bürger\*innen und Unternehmen. Darüber hinaus kommt dem Staat im Rahmen seiner Sicherheitsfunktion die essenzielle Verantwortung zu, Rahmenbedingungen und institutionelle Strukturen für sichere Transaktionen im Netz und den Schutz vor Cyberangriffen zu gewährleisten. Cybersicherheit ist somit als Kernaufgabe von Staat und Verwaltung erkannt und hat sich als Politikfeld etabliert. Es ist Teil des sog. *Internet-Governance-Makrokosmos*, der diverse Politikfelder vereint, die aus der Internetentwicklung heraus entstanden sind oder mit ihr eine deutliche Neudefinition erfahren haben.

Jede Betrachtung der sicherheitspolitischen Herausforderungen von Internet und Digitalisierung muss Ausgang nehmen vom technischen Kernverständnis der *IT-Sicherheit*. Dieses umfasst im Wesentlichen die Sicherung der Verfügbarkeit von IT-Systemen und -Infrastrukturen, ihre Integrität und Vertraulichkeit – *confidentiality*, *integrity* und *availability* bilden die sogenannte „*CIA triad*“, die üblicherweise als Kernzielkatalog der *IT-Sicherheit* aufgefasst wird – sowie die Resilienz (im Sinne von Widerstandsfähigkeit oder Ausfallsicherheit) der Systeme und Kommunikationswege (Singer und Friedman 2014, S. 35). Die Ziele der *IT-Sicherheit* können mit technischen und organisatorischen Mitteln, einschließlich umfassender Verhaltensregeln für Anwender\*innen erreicht werden. Der Zielerreichung stehen ökonomische Interessen, veraltete Systeme und die Sorglosigkeit oder Bequemlichkeit von Anwender\*innen entgegen. Zudem begünstigt die Komplexität von IT-Systemen nahezu unkalkulierbare Effekte bei der Integration verschiedener Soft- und Hardwarekomponenten. Angriffe auf IT-Systeme können über Lücken und Fehler im Quellcode verübt werden. Dringen Angreifer über solche Lücken in geschützte Systeme ein, spricht man von *Exploits* oder – wenn zuvor unentdeckt, nicht-veröffentlicht und/oder nicht behandelt – von *Zero-Day-Exploits*. Vielfach wird auch das unbedachte Verhalten der Anwender\*innen ausgenutzt, die etwa ungeprüft Dateianhänge an *E-Mails* öffnen, kritische Informationen selbst infolge von Irreführung preisgeben oder manipulierte Datenträger in ihre Systeme einführen (*social engineering*). Die grundlegenden Ziele von *Cyberangriffen* bestehen im Ausspähen, im Diebstahl, in der Veränderung bis hin zur Zerstörung von gespeicherten Informationen oder Programmen. Hierzu kann Schadsoftware zum Einsatz kommen. Die Anzahl sogenannter *malware* ist in den vergangenen Jahren erheblich gestiegen. Laut Angaben des Antivirus-Test-Instituts sowie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist die Anzahl bekannter Schadprogramme allein 2017 um über 120 Mio. angestiegen.

Über das technische Kernverständnis hinaus schließt das weite Begriffsfeld der Cybersicherheitspolitik ähnlich wie die Sicherheitspolitik als solche diverse Bedrohungsszenarien, Verwundbarkeiten und staatliche Handlungsrepertoires ein, die sich weniger anhand der missbrauchten Technologien als anhand des unterstellten An-

greifertyps, seiner Motivation, der Implikationen des Angriffs auf die nationale Sicherheit sowie nicht zuletzt der Zuständigkeiten innerhalb der staatlichen Verwaltung unterscheiden lassen. Obwohl territoriale Grenzen für die digitale Kommunikation prinzipiell überwindbar sind, ist die klassische – schon im Vorfeld der Digitalisierung problematisch gewordene – Trennung zwischen innerer und äußerer Sicherheit auch auf dem Feld der Cybersicherheitspolitik erkennbar. Wer Cybersicherheit im Sinne der inneren Sicherheit betrachtet, denkt an Verbrechensbekämpfung, an Aufklärung von und Abwehr gegen Angriffe mit kriminellen Interessen. Angriffe auf IT-Systeme, die wir diesem Feld zuordnen, bedrohen mittelbar Personen und Unternehmen und fügen diesen ökonomischen oder anderen Schaden zu. Hinsichtlich ihrer Erscheinungsform erfolgen sie vielfach nicht zielgerichtet, sondern attackieren Opfer in einer großen Masse von Anwendern (z. B. *Phishing*). Sicherheitsinteressen auf übergeordneter Ebene, insbesondere die nationale Sicherheit, sind in der Regel nicht bedroht. Besondere Formen, die die Unterscheidung offensichtlich herausfordern, sind das organisierte Verbrechen und die Wirtschaftsspionage. Werden Unternehmen und Einrichtungen attackiert, die wesentliche Infrastrukturleistungen für das Funktionieren moderner Gesellschaften erbringen (Energie, Verkehr, Kommunikation etc.), ist durchaus mit weiterreichenden Sicherheitsbedrohungen zu rechnen. So haben etwa die in den vergangenen Jahren gestiegen zu beobachtenden Fälle von *Ransomware* für Aufsehen gesorgt. Dabei nimmt Schadsoftware eine Verschlüsselung der Dateien auf dem Zielsystem vor, die nur mittels eines Schlüssels, der von den Angreifern gegen Lösegeld angeboten wird, rückgängig gemacht werden kann. Derartige Datenverluste haben in der Vergangenheit z. B. auch Patientendaten in Krankenhäusern betroffen oder die Funktionsfähigkeit vernetzter medizinischer Geräte beeinträchtigt und damit zu vorübergehenden Einschränkungen der medizinischen Versorgung geführt. Ruchbar gewordenen Vorfällen wird mit technischen, polizeilichen, juristischen und politischen Mitteln begegnet.

Gerade die letztgenannten Beispiele zeigen die Schwierigkeiten einer klassischen Grenzziehung zwischen innerer und äußerer Sicherheit an. Die Übergänge zum zweiten Typ, also einer Cybersicherheitspolitik als Problembereich im Feld der Außen- und Sicherheitspolitik, sind hier offensichtlich fließend. Die genannten Angriffe und Ausspähungen krimineller Natur haben vielfach einen auswärtigen Ursprung (d. h. Spuren, einschließlich falscher Fährten, führen ins Ausland). Umgekehrt fallen viele politisch motivierte, terroristische oder extremistische Cyberangriffe angesichts der eingesetzten Mittel und einer (wenngleich unsicheren) Attribution in diesen Graubereich. Die Spionage von politischen Zielen (z. B. *Bundestags-Hack*) und die teils niedrigschwellig-destruktiven Angriffe politisch motivierter *Hacker* werden vielfach Staaten zugeschrieben und auf politische Ziele, staatliche Interessen und Unterstützungsstrukturen zurückgeführt. Dabei sind die Angriffe dieses Typs, zumindest in ihrer gängigen Erscheinungsform, anders geartet, sie erfolgen nämlich zielgerichtet und sind auf eine gewisse Dauer angelegt (*Advanced Persistent Threats – APTs*). In der Regel erfordern sie einen weit höheren Aufwand und deuten auch deshalb auf öffentliche Stellen als Ursprung oder Finanzierungsquelle hin. Sie zielen gegebenenfalls auf die nationale Sicherheit, können diese zumindest gefährden.

Angriffen dieses Typs kann mit technischen und politischen Mitteln begegnet werden. Zum einen bauen viele Staaten und internationale Organisationen ihre Fähigkeiten in der Cyberverteidigung, aber auch offensive Fähigkeiten erkennbar aus. Außerdem verhandeln die Staaten der Weltgemeinschaft international über globale Standards im Sinne eines Cyberkriegsvölkerrechts (*ius ad bellum et in bello*). Allgemeine Probleme heutiger internationaler Ordnung werden durch asymmetrische Konfliktkonstellationen (im Extremfall Staaten vs. Hacker-Gruppen) sowie die schwierige bis unmögliche Attribution von Cyberangriffen verschärft.

Die in Wissenschaft, politischer Praxis und Gesellschaft verbreitete Rede vom „Cyberkrieg“ ist umstritten, denn die Bedeutungen des Kriegsbegriffs stehen in offensichtlicher Spannung zum geringen Maß menschlichen Leids, zu vergleichsweise geringen materiellen Schäden und weiterhin unklaren politischen Folgen von Cyberangriffen. Dass Angriffe auf IT-Systeme im Rahmen kriegerischer Aktivitäten im Sinne operationeller Kriegsführung eine Rolle spielen, ist hingegen Konsens. Am Einsatzziel, am Maß der mittelbaren Verwundbarkeit in der physischen Welt (sogenannter „kinetischer Effekt“), insbesondere Verwundbarkeit der *kritischen Infrastrukturen*, und nach anderen Kriterien lassen sich Cyberangriffe klassifizieren. Dazu wurden in der jüngeren Vergangenheit in der wissenschaftlichen Literatur Vorschläge zur Indexbildung vorgelegt (u. a. Steiger et al. 2018). Cyberangriffe mit nachgewiesenem kinetischen Effekt sind ausgesprochen selten. Das am häufigsten genannte Beispiel ist der sog. *Stuxnet*-Wurm, der mutmaßlich von den USA und Israel entwickelt und im Jahr 2010 gegen iranische Zentrifugen zur Urananreicherung eingesetzt wurde. Derartige Angriffe gelten als sehr anspruchsvoll und aufwändig.

Darüber hinaus sind in der jüngeren Vergangenheit abseits gewaltsamer Konfliktkonstellationen zunehmend propagandistische Aktivitäten zur Meinungsmanipulation als Bedrohungen der nationalen Sicherheit wahrgenommen worden. Politische bis hin zu militärischen Reaktionen werden diskutiert. Mit dieser Auslegung von Cybersicherheit verlässt das Feld die technischen Kriterien entsprechender Vorfälle, jedenfalls soweit Desinformation und Propaganda nicht durch das verbotene Eindringen in fremde Systeme oder Schadsoftware verbreitet werden.

Die aktuellen Bedrohungsperzeptionen von Desinformation und Propaganda und ihre Verarbeitung in vielen Staaten sowie auf der internationalen Ebene führen die seit den 1990er-Jahren erkennbare gesellschaftspolitische Aufladung von Cybersicherheit fort. Helen Nissenbaum (2005) unterscheidet Cybersicherheit („*cyber-security*“) dezidiert von der technischen *IT-Sicherheit* („*technical security*“). Dieser Beitrag greift diese Unterscheidung in seiner begrifflichen Differenzierung auf. Tatsächlich geht es Cybersicherheit im weitesten Sinne nicht mehr nur um Angriffe auf Computer(netzwerke) und deren potenzielle Gefährdung, sondern auch auch um den Jugend-, den Minderheitenschutz, die klassische Verbrechensbekämpfung und Terrorabwehr (auch Verhinderung von Rekrutierung, Sperren von Propagandavideos etc.). Diese Aufladung und Ausweitung der ursprünglichen *IT-Sicherheit* kann bemerkenswerte unintendierte Konsequenzen und paradoxe Effekte haben. So sind die in den zurückliegenden Jahren gesteigerten und öffentlich enthüllten staatlichen Maßnahmen der (Massen-)Überwachung von *Online*-Kommunikation durch Ge-

heimdienste und Ermittlungsbehörden, der verdachtsunabhängigen Sammlung und temporären Speicherung von Kommunikationsdaten (Vorratsdatenspeicherung) sowie gewisse Praktiken der *Online-Content*-Regulierung, also der Beschränkung des Zugangs zu *Online*-Angeboten oder Inhalten, wie sie vielfach auf Grundlage politischer Cybersicherheitskonzeptionen erfolgen, mit den eigentlichen Zielen der *IT-Sicherheit* inkompatibel. Deutlicher noch wird dieses spannungsvolle bis widersprüchliche Verhalten staatlicher Stellen beim Ankauf von Schwachstellen (*Exploits*) durch Geheimdienste und Ermittlungsbehörden, beim Einbau von Hinterturen (*Backdoors*) in *Hardware*, dem Einsatz von „Staatstrojanern“ oder im Hinblick auf die zögerliche Unterstützung flächendeckender Verschlüsselung.

---

## 2 Theoretische Grundlagen

Vor dem Hintergrund der genannten Auffälligkeiten und inhärenten Widersprüche der Cybersicherheitsdiskussion ist es nicht verwunderlich, dass das Feld der Sicherheitsforschung in den vergangenen Jahren eine Vielzahl von Forschungsarbeiten hervorgebracht hat, die die teils wesensfremde Aufladung des Begriffs, die Vermischung mit den Gegenständen allgemeiner Sicherheitspolitik, alarmistische Untertöne und weitreichende, mitunter paradoxe Effekte behandeln. So hat bereits der breit verwendete Ausdruck „Cyberkrieg“ früh entsprechende Kritik hervorgerufen und ist bis heute umstritten (Dunn Cavelty 2013; Rid 2012). Der aus der konstruktivistischen Theorie der wissenschaftlichen Disziplin der Internationalen Beziehungen stammende Ansatz der *Versicherheitlichung* (Kopenhagener Schule: *securitization*) findet bis heute regelmäßig Anwendung. Er ist geradezu zum dominanten Theorieparadigma in der Analyse staatlichen Verhaltens angesichts der Herausforderungen der Digitalisierung im Sicherheitsbereich geworden (Hansen und Nissenbaum 2009). Der auf der Sprechakttheorie basierende Ansatz geht davon aus, dass die Wahrnehmung eines Phänomens als Sicherheitsproblem auf einem performativen Sprechakt beruht, mit dem ein versicherheitlichender Akteur, z. B. ein Minister oder sonstiger Politiker, ein Problem zu einem Sicherheitsproblem, orientiert an einem Bezugsobjekt, z. B. der Nation, erhebt und dafür bei einem jeweils maßgeblichen Publikum Anerkennung findet. Dadurch können außergewöhnliche Maßnahmen, z. B. pfadabweichende sicherheitspolitische Maßnahmen bis hin zu Grundrechtsverletzungen, legitimiert werden.

Den Fragen der Bedrohungsperzeption nachgeordnet wird in der *Governance*-Forschung sowie politikberatenden Veröffentlichungen die Frage behandelt, wie der Staat seiner Sicherheitsfunktion, aber auch seiner Gewährleistungsfunktion im Hinblick auf verschiedene von Cyberangriffen bedrohte Individualrechte gerecht werden kann. Aufgrund der prinzipiellen Offenheit der Netzwerkkommunikation und der dezentralen Verwaltung der zugehörigen Infrastruktur ist ein rein staatlicher Regulierungsansatz technisch wie normativ (im Sinne liberaler Demokratie und Medienpolitik) ausgeschlossen. Stattdessen geht es notwendig um die Gestaltung eines Ansatzes der sogenannten *networked governance* mit einer Vielzahl relevanter *Stakeholder*, insbesondere den Betreibern von Telekommunikationsnetzwerken

sowie anderen *kritischen Infrastrukturen*. Mit der Definition der Rolle des Staates in den existenten bzw. zu schaffenden privat-öffentlichen Strukturen und der Durchsetzung staatlicher Kontrollrechte gegenüber privaten Akteuren ist ein wesentlicher Gegenstand der *Governance*-Forschung berührt. Dabei gelten als zentrale Herausforderungen die zurückhaltende Informationspraxis privater Unternehmen im Falle von informationssicherheitsrelevanten Zwischenfällen, der schwierige Wettbewerb zwischen öffentlichen Einrichtungen und Privatwirtschaft um geeignete Fachkräfte sowie die Gewährleistung der Vertraulichkeit klassifizierter Informationen in Kontexten privat-öffentlicher Zusammenarbeit. Wie weit sollen die Aufsichts- und Eingriffsrechte des Staates in die unternehmerische Freiheit reichen? Auf welche Sektoren sollen und können sich diese Rechte überhaupt erstrecken? Verfügt der öffentliche Sektor über die nötigen Ressourcen, um ausreichende Expertise innerhalb der öffentlichen Verwaltung (*In-house*-Ansatz) einzuhören bzw. durch Ausbildung herzustellen? Kann auf Modelle von Kooperation und *Outsourcing* zurückgegriffen werden, ohne neue Sicherheitsrisiken einzugehen?

Ein weiterer konzeptioneller Strang im Feld der Cybersicherheitsforschung wendet sich der chronischen Attributionsproblematik zu (Rid und Buchanan 2015). Die besonderen raumzeitlich entnommenen Wirkungsweisen von Cyberangriffen, kurzum ihr virtueller Charakter, machen eine sichere Zuschreibung der Täterschaft zulasten eines Akteurs ausgesprochen schwierig. Dies ist zweifellos ein Problem für die Verbrechensbekämpfung, die auf eine effektive Strafermittlung und die abschreckende Wirkung des Strafvollzugs angewiesen ist. Die Attributionsproblematik berührt aber die Präventionsfähigkeit und Reaktionsmöglichkeiten auf Angriffe mit (mutmaßlich) politischem Hintergrund wesentlich. Sie steigert den Eindruck potenzieller Verwundbarkeit, die Verunsicherung und die Konfliktanfälligkeit in den internationalen Beziehungen. Unsichere Attribution und die Möglichkeit plausiblen Abstreitens der Vorwürfe (*plausible deniability*) auf Seiten mutmaßlich Verantwortlicher reduzieren die Wirksamkeit von Abschreckung. Cyberangriffe hinterlassen zwar durchaus Spuren (etwa in Form von Metadaten oder Mustern der Programmierung), die geschulte IT-Forensiker auslesen können. Allerdings können diese Spuren vielfach manipuliert sein, so dass sich ähnlich wie mit den Systemlücken auch in dieser Beziehung ein Katz- und Maus-Spiel zwischen Tätern und Ermittlern ergibt, wobei es Ersteren möglich ist, falsche Fährten zu legen. Führen Spuren oder gar Belege ins Ausland, sind den Ermittlungsbehörden vielfach die Hände gebunden.

Das Attributionsproblem gehört zu den wesentlichen neuen Bedingungen, die die Anwendung klassischen Völkerrechts auf den Cyberraum erschweren. Gefördert durch das NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE), erarbeiteten führende Experten des internationalen Rechts das „*Tallinn Manual*“. 2017 wurde eine überarbeitete Version („*Tallinn Manual 2.0*“) veröffentlicht (Schmitt 2017). Die Überarbeitungen fokussierten insbesondere auf die Verantwortung der Staaten, die Sicherheit anderer Staaten gefährdende Angriffe, die von ihrem Territorium ausgehen, zu bekämpfen. Als Orientierung gilt in diesem Zusammenhang die *due diligence*-Norm, die auf die besonderen Bedingungen digitalisierter Angriffsformen sowie die prinzipielle Offenheit der Netzwerkkommunikation abzustimmen war. So wurde bewusst eine Beschränkung auf aktuell laufende Operatio-

---

nen vorgenommen und keine Pflicht zur Verantwortungserfüllung mittels präventiver oder präemptiver Maßnahmen formuliert. Denn die Verpflichtung der Staaten zu einer möglichst effektiven Ex-ante-Kontrolle auf dem Territorium befindlicher IT-Systeme oder gar durch das Territorium geleiteter Kommunikationsaktivität würde Überwachungs- und Kontrollarchitekturen erfordern, welche die Internetfreiheit gefährden würden.

---

### 3 Praktische Anwendung

Maßnahmen und Reaktionen im Sinne der *IT-Sicherheit* umfassen etwa die Identifizierung von Lücken und Fehlern und ihre Behebung. In diesem Fall wird die Lücke zumeist mittels eines zum *Download* bereitgestellten *Updates (patch)* geschlossen. Prophylaktischen Schutz gegen Cyberangriffe bieten *Firewalls* und Anti-Virenprogramme bis hin zu aufwändigeren *Intrusion Detection*-Systemen sowie zahlreiche organisatorische Maßnahmen wie etwa Zugangskontrollen zu kritischen Systemen, die physische und logische Trennung von anderen IT-Systemen und Netzwerken (*air gap*), die Überwachung des Anwender\*innenverhaltens und ausreichende Schulungsmaßnahmen. Auch die Transparenz über in der Vergangenheit erfolgte Angriffe trägt zur Steigerung der *IT-Sicherheit* bei. Für diesen Zweck sowie zur Aufklärung von Straftaten ist zudem der Nachvollzug getätigter Cyberangriffe im Sinne der IT-Forensik von erheblicher Bedeutung. Eine wachsende Industrie stellt Werkzeuge und Beratung zur *IT-Sicherheit* zur Verfügung. Angreifer und Verteidiger von IT-Systemen befinden sich in einem permanenten Katz-und-Maus-Spiel (Singer und Friedman 2014, S. 60). Denn IT-Systeme und *Software* enthalten immer Lücken und Fehler, insbesondere dann, wenn diese in einem kompetitiven Umfeld rasch zur Marktreife gebracht werden. Staat und Verwaltung können diese Prozesse vielgestaltig beeinflussen. Zum einen setzen und überwachen sie Regeln der angemessenen IT-Sicherheitspraxis von Unternehmen und Einzelanwender\*innen, in der Regel differenziert nach dem Geschäftsbereich und der Relevanz für das Funktionieren moderner Gesellschaften (*kritische Infrastrukturen*). Sie beteiligen sich an der Entwicklung und Zertifizierung von IT-Sicherheitsmodellen (IT-Grundschatz). Sie haben eine besondere Aufgabe im Schutz der eigenen, in der Regel besonders schützenswerten IT-Systeme und eine Vorbildrolle gegenüber anderen gesellschaftlichen Akteuren. Zudem sind staatliche Behörden in autoritativer und umfassender Weise an der Erhebung und Verarbeitung personenbezogener Daten beteiligt.

Die Sicherheit dieser besonders schützenswerten Datenbestände vor Ausspähung, Diebstahl oder Kompromittierung stellt den Überschneidungsbereich von *IT-Sicherheit* und Datenschutz dar. Auch der Datenschutz hat sich unter den Eindrücken der Digitalisierung dramatisch gewandelt. Die jüngst im Rahmen der EU-Datenschutzgrundverordnung (DSGVO: EU 2016/679) reformierten, im internationalen Vergleich strikten Regularien zum Schutz personenbezogener Daten binden neben den datenverarbeitenden Unternehmen auch die Akteure des öffentlichen Sektors und bewahren die Bürger\*innen als Grundrechts-träger\*innen vor der unerlaubten, nicht an den jeweiligen Zweck gebundenen und nicht kenntlich gemachten Sammlung, Über-

tragung und Verarbeitung personenbezogener Daten durch staatliche Behörden. Zuletzt kommt diesen eine wesentliche Rolle bei der Aufklärung von Sicherheitsbedrohungen sowie eine exklusive Kompetenz in der Strafverfolgung und Ermittlung von Straftaten zu. Die staatlichen Ermittlungsbehörden und Geheimdienste genießen in Bezug auf den Datenschutz Sonderbefugnisse in dem jeweiligen gesetzlichen Rahmen nach der ebenfalls reformierten EU-Rechtsetzung (EU-Richtlinie 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung).

In Deutschland und der EU ist auch der Rechtsrahmen zur Gewährleistung von *IT-Sicherheit* in den vergangenen Jahren erheblich ausgebaut und konkretisiert worden. Die wesentlichen Reformdokumente sind das IT-Sicherheitsgesetz von 2015 (ITSiG), die 2016 in Kraft getretene EU-Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union (NIS-Richtlinie: EU 2016/1148) sowie das zugehörige nationale Umsetzungsgesetz vom Juni 2017. Im Ergebnis haben sie die Befugnisse von Staat und Verwaltung innerhalb der relevanten privat-öffentlichen Akteursnetzwerke klarer definiert und ausgebaut, allerdings auf Grundlage eines differenzierten Ansatzes. So fokussieren die Regulierungsmaßnahmen auf sog. *kritische Infrastrukturen*, die für das Funktionieren moderner Gesellschaften notwendig sind (also die Bereiche Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen) und legen den entsprechenden Betreibern (in Deutschland nach Schätzungen etwa 2000 Unternehmen) besondere Sorgfalts- und Meldepflichten auf, die sanktionsbewehrt sind.

Das organisatorische Zentrum bildet das im Geschäftsbereich des Bundesinnenministeriums verortete, aber unabhängige Bundesamt für Sicherheit in der Informationstechnik (BSI). Seit seiner Gründung 1991 sind die Befugnisse des BSI erheblich ausgebaut worden. Zuletzt hat es mit den genannten Gesetzesreformen sowie dem Gesetz zur Stärkung der Sicherheit in der Informationstechnik (BSI-Gesetz) aus dem Jahr 2009 erweiterte Kompetenzen erhalten, die sich auch in einem Ausbau der Organisation (materiell und personell) niedergeschlagen hat. Das Amt beschäftigt über 930 Mitarbeiter\*innen in fünf Abteilungen (Stand Nov. 2018). Das BSI ist heute der zentrale IT-Sicherheitsdienstleister des Bundes, zudem Aufsichtsbehörde, staatliche Forschungs-, Entwicklungs- und Beratungseinrichtung sowie Prüf- und Zertifizierungsstelle für Betreiber und Unternehmen. Sowohl die Bundesbehörden (nach § 4 Abs. 3 BSI-Gesetz) als auch die Betreiber *kritischer Infrastrukturen* sind verpflichtet, cybersicherheitsrelevante Vorfälle beim BSI zu melden. Bei den Bundesbehörden steht die Abwehr von Schadprogrammen im Vordergrund. Das BSI verzeichnet im Durchschnitt monatlich 28.000 entsprechende *E-Mails* an Mailkonten der Bundesverwaltung. Seitens der Betreiber *kritischer Infrastrukturen* sind im entsprechenden Berichtszeitraum bis zum 31. Mai 2018 145 Meldungen von Cybersicherheitsvorfällen eingegangen (Lagebericht des BSI 2018). Das BSI beherbergt zudem das sog. „CERT-Bund“ (*Cyber Emergency Response Team* der Bundesverwaltung), also eine Einheit zur schnellen Reaktion auf IT-Sicherheitszwischenfälle für die Einrichtungen des Bundes sowie das Nationale Cyber-Abwehrzentrum (NCAZ). Als behördenüber-

greifendes Kooperationszentrum dient es dem Schutz vor Cyberangriffen auf IT-Infrastrukturen in Deutschland. Neben dem BSI schließt es im Kern auch den Verfassungsschutz und die Katastrophenhilfe ein. Zu den assoziierten Organisationen zählt ferner auch die Bundeswehr.

Mit dem Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr von Juli 2016 hat das Verteidigungsministerium seinerseits umfassende institutionelle Reformen in der Ministerialverwaltung sowie bei der Bundeswehr vorbereitet, die mittlerweile vollzogen worden sind (Bundesregierung 2016). Mit den Reformen sollen die deutschen Streitkräfte sich und ihre IT sowie in einem weiteren Aufgabenspektrum die deutsche Gesellschaft vor Gefahren aus dem Cyberraum schützen. Grundlegend wird der Cyber- und Informationsraum in seiner militärischen Dimension als eigenständiger Operationsraum wahrgenommen und definiert. Mit Blick auf die Strukturen in Armee und Verwaltung bedeutet das vor allem eine Zentralisierung von Zuständigkeiten und die Zusammenlegung von Ressourcen für ein breites Spektrum der Cyber- und IT-bezogenen Aufgaben. Dazu zählen sowohl die Cyber-Verteidigung als auch operative Fähigkeiten, die *IT-Sicherheit* der eigenen Systeme sowie die IT-Beschaffung. Im April 2017 (Erstbefähigung) ist bei der Bundeswehr ein neuer militärischer Organisationsbereich für den Cyber- und Informationsraum (CIR) mit einem Inspekteur an der Spitze eingerichtet worden. Im Bundesverteidigungsministerium war bereits zuvor die neue Abteilung Cyber/IT (CIT) unter Leitung eines sog. *Ressort-Chief Information Officer* etabliert worden.

Mit Blick auf die Bundeswehr ist der neue Organisationsbereich CIR als Teil der Streitkräfte ins Leben gerufen worden. Ihm sind die Verbände und Dienststellen der Bereiche Kommando Strategische Aufklärung, Kommando Informationstechnik und Zentrum für Geoinformationswesen unterstellt. Die bereits bestehende Gruppe für Computer-Netzwerk-Operationen (CNO) ist zu einem Zentrum für Cyberoperationen (Zentr CybOp) ausgebaut und mit 20 zusätzlichen Personalstellen versehen worden. Insgesamt wurden knapp 14.000 Dienstposten mit den bestehenden Aufgaben in den neuen Organisationsbereich verlagert. Unter Führung des Inspekteurs vollzieht das Kommando CIR (KdoCIR) mit Sitz in Bonn die zentralen Aufgaben für den Organisationsbereich.

---

## 4 Künftige Entwicklung

Die bisherigen Maßnahmen auf bundesdeutscher Ebene berühren nicht die Standards und kritischen Ressourcen der Internetkommunikation, also den *Internet-Governance-Mikrokosmos*, obwohl auch in diesem Bereich erhebliche Sicherheitsprobleme bestehen können (z. B. *Domain-Name-System* oder *Border-Gateway-Protocol* etc.). Hinsichtlich dieser kritischen Ressourcen des Internets bleibt es bislang bei einer staatsfernen Organisation. Allerdings sprechen die Entwicklungen auf dem Feld der Cybersicherheit für eine mittelfristige *Restitution von Staatlichkeit* in der Cybersicherheit und *Internet Governance*. Das zeigt sich insbesondere an der Anrufung staatlicher Stellen, an den Bedeutungszuwachsen des Staates im Sinne der inneren Sicherheitsfunktion wie auch seiner Sorgfaltspflicht im Hinblick auf das Agieren nichtstaatlicher Akteure auf seinem

Territorium, schließlich auch an den der eigentlichen *IT-Sicherheit* fremden Forderungen nach Bekämpfung von Manipulationen über Inhalte der Internetkommunikation. Schon heute wird im Kontrast zu den reduzierten staatlichen Kontrollmöglichkeiten im Kontext globalen Datenverkehrs und den chronischen Ungewissheiten bei der Attribution und Bewertung von Cyberangriffen der Staat in zentraler Akteursrolle (als Täter, Opfer oder gar in bilateralen Konfliktkonstellationen) wahrgenommen und in seiner Regulierungsfunktion angerufen. Dies führt notgedrungen zu einem Spannungsverhältnis. Staatliche Behörden werden die von ihnen verlangten Sicherheitsgarantien nur zum Preis zunehmender Kontrolle und Überwachung von Internetkommunikation und damit Einschränkungen der Internetfreiheit abgeben können. Je weiter der traditionelle Konsens der westlichen Welt im Sinne einer liberalen Weltordnung ins Wanken gerät, desto wahrscheinlicher wird die Auflösung der Spannung durch eine (re-)nationalisierte Netzpolitik. In der die Kernfunktionen des Staates berührenden Cybersicherheitspolitik liegt diese Entwicklung besonders nahe.

---

## Literatur

- Bundesamt für Sicherheit in der Informationstechnik (BSI). 2018. *Die Lage der IT-Sicherheit in Deutschland 2018*. Bonn. [https://www.bsi.bund.de/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf;jsessionid=85A3AD97B3119C8CB7331C0FD6A01B33.1\\_cid351?\\_\\_blob=publicationFile&v=5](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf;jsessionid=85A3AD97B3119C8CB7331C0FD6A01B33.1_cid351?__blob=publicationFile&v=5). Zugegriffen am 19.12.2019.
- Bundesregierung. 2016. *Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr*. Berlin. <https://www.bmvg.de/resource/blob/13708/015be272f8c0098f1537a491676bfc31/weissbuch2016-barrierefrei-data.pdf>. Zugegriffen am 19.12.2019.
- Dunn Cavelti, Myriam. 2013. Der Cyber-Krieg, der (so) nicht kommt. Erzählte Katastrophen als (Nicht)Wissenspraxis. In *Aufbruch ins Unversicherbare. Zum Katastrophendiskurs der Gegenwart*, Hrsg. Leon Hempel und Marie Bartels, 2. Aufl., 209–233. Bielefeld: transcript.
- Hansen, Lene, und Helen Nissenbaum. 2009. Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly* 53(4): 1155–1175. <https://doi.org/10.1111/j.1468-2478.2009.00572.x>.
- Nissenbaum, Helen. 2005. Where computer security meets national security. *Ethics and Information Technology* 7(2): 61–73. <https://doi.org/10.1007/s10676-005-4582-3>.
- Rid, Thomas. 2012. Cyber war will not take place. *Journal of Strategic Studies* 35(1): 5–32. <https://doi.org/10.1080/01402390.2011.608939>.
- Rid, Thomas, und Ben Buchanan. 2015. Attributing cyber attacks. *Journal of Strategic Studies* 38 (1–2): 4–37.
- Schmitt, Michael N., Hrsg. 2017. *Tallinn manual 2.0 on the international law applicable to cyber operations*, NATO Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press. <https://doi.org/10.1017/9781316822524>.
- Singer, P. W., und Allan Friedman. 2014. *Cybersecurity and cyberwar. What everyone needs to know*. Oxford: Oxford University Press.
- Steiger, Stefan, Sebastian Harnisch, Kerstin Zettl, und Johannes Lohmann. 2018. Conceptualising conflicts in cyberspace. *Journal of Cyber Policy* 3(1): 77–95. <https://doi.org/10.1080/23738871.2018.1453526>.



# Die datengesteuerte Verwaltung

Basanta E. P. Thapa

## Inhalt

1 Klärung des Begriffs .....	210
2 Konzeptionelle Grundlagen .....	212
3 Praktische Anwendungsfelder .....	215
4 Perspektiven für Staat und Verwaltung .....	216
Literatur .....	217

## Zusammenfassung

Neue Datentechnologien wie *Big Data Analytics*, Künstliche Intelligenz und das Internet der Dinge erlauben Datenerhebung und -auswertung in ungekannter Qualität und Dichte, mit neuen Möglichkeiten der Feingranularität, „Vermischung“ von Datenquellen und Mustererkennung durch Maschinenlernen. Dadurch eröffnen sich der öffentlichen Verwaltung fortgeschrittene Möglichkeiten zur umfassenden Beobachtung, Analyse, Vorhersage und Automatisierung von Verwaltungshandeln. Die globale Debatte, die sowohl in der Verwaltungspraxis als in der Wissenschaft geführt wird, ist von weitreichenden Versprechen und vehementer Kritik geprägt. Die datengesteuerte Verwaltung kann jedoch je nach gesellschaftspolitischer Orientierung unterschiedlich gestaltet werden.

## Schlüsselwörter

Big Data · Linked Data · Algorithmus · Künstliche Intelligenz · Verwaltungsautomatisierung

---

B. E. P. Thapa (✉)

Fraunhofer-Institut für offene Kommunikationssysteme, Kompetenzzentrum Öffentliche IT, Berlin, Deutschland

E-Mail: [basanta.thapa@fokus.fraunhofer.de](mailto:basanta.thapa@fokus.fraunhofer.de)

## 1 Klärung des Begriffs

Die datengesteuerte Verwaltung („*data-driven government*“) ist ein Verwaltungsreformleitbild, das im Diskurs um Informationstechnologie und Staat vorwiegend von Beratungs- und Technologieunternehmen propagiert wird, aber auch bereits von einzelnen Regierungen aufgegriffen wurde. So nennt der britische *Government Digital Service* „*data-driven government*“ als Ziel einer Teilvision für die Verwaltung des Vereinigten Königreiches im Jahr 2030, denn: „Better use of government data will change the world for business, for government itself, and for citizens“. Als Schlagwort bezeichnet datengesteuerte Verwaltung das administrative Veränderungspotential von digitaler Datenerhebung, -aufbewahrung und -auswertung, die unter Überschriften wie *Big Data*, Algorithmisierung und Künstlicher Intelligenz in den 2010er-Jahren signifikante technische Fortschritte gemacht haben (Pencheva et al. 2018; Giest 2017).

Grundsätzlich umfasst öffentliche Verwaltung bereits seit ihren Anfängen Statistik und Datenverarbeitung zur Entscheidungsunterstützung und -findung (Scott 1998): Inventar- und Steuerabgabelisten der öffentlichen Verwaltung zählen zu den ältesten Schriftzeugnissen der Menschheit. Die christliche Weihnachtsgeschichte nimmt erst durch eine kaiserliche Volkszählung ihren Lauf. Max Weber benennt „Herrschaft kraft Wissen“ als ein zentrales Wesensmerkmal der rationalen Bürokratie (Weber 1922). In der langen Geschichte der Datenverarbeitung in der öffentlichen Verwaltung, die spätestens seit Ende des 19. Jahrhunderts auch Lochkarten-Rechenmaschinen umfasste und in den 1960er und 1970ern zunehmend in den digitalen Datenbanken von *Mainframe*-Rechnern stattfand, bedeuten die technischen Innovationen des 21. Jahrhunderts einen gravierenden Qualitätssprung. Dieser geht vor allem auf drei Aspekte der „Datenrevolution“ zurück, die nicht von ihrem Wesen, wohl aber von dem nun möglichen Ausmaß her neu sind: *Feingranularität*, *Vermischung* und *Maschinenlernen*.

1. *Feingranularität* bezeichnet die Fähigkeit, aggregierte Datensätze bis auf die Ebene des Einzelfalls – beispielsweise einzelne Bürger\*innen mit ihren diversen Attributen – aufzulösen. Statistiken können also jederzeit in neue Kategorien zugeschnitten und Indikatoren anders kombiniert werden. Diese Gleichzeitigkeit von Makro- und Mikroblick eröffnet für Monitoring und Datenanalyse neue Möglichkeiten.
2. Die *Vermischung* von Daten („*linked data*“) bezeichnet das Verknüpfen von verschiedenen Datensätzen, insbesondere der einzelnen Objekte in den Datensätzen – in Verwaltungskontexten beispielsweise natürliche oder juristische Personen, Immobilien oder Kraftfahrzeuge. So ergibt sich aus verschiedenen Datenquellen ein umfassendes Bild einzelner Objekte bzw. die Möglichkeit, neue Faktoren in eine Analyse einzubeziehen. Die Granularität der Daten ist hierfür Voraussetzung.
3. *Maschinenlernen*: Feingranularität, Vermischung und hohes Datenvolumen führen zu einem Datenreichtum, der Analysemethoden jenseits der klassischen, auf Datenarmut ausgerichteten Inferenzstatistik ermöglicht. Je größer die ausgewertete Stichprobe im Verhältnis zur Grundgesamtheit ist, über die Aussagen getroffen

werden sollen, desto robuster sind die ermittelten statistischen Korrelationen gegen Zufallseffekte und andere Fehler. Einen paradigmatischen Wechsel bei der Datenauswertung stellt der Ansatz des Maschinenlernens dar, bei dem Kategorien und Kausalmodelle durch den Rechner aus den Daten heraus ermittelt und selbstlernend optimiert werden. Die Suche nach Ursachen und Zusammenhängen ist daher nicht länger auf den menschlichen Einfallsreichtum angewiesen, sondern kann automatisiert stattfinden.

Voraussetzung für den Einsatz der neuen Datentechnologien ist Datenreichtum, denn Feingranularität ist nur mit hochauflösten Datensätzen zu erreichen, Vermaschung bedarf verschiedener Datensätze zu verknüpfbaren Objekten, und Maschinenlernen wird erst bei hohen Fallzahlen sinnvoll anwendbar. Datenquellen für diesen Datenreichtum können nicht nur die verwaltungseigenen Datenbestände sein, sondern auch externe Datenbestände jenseits der Verwaltung (Thapa und Parycek 2018).

1. *Interne Datenbanken* der Verwaltung sind beispielsweise Register oder Akten. Diese sollten zur optimalen Auswertbarkeit maschinenlesbar, von der Datenstruktur her einheitlich und miteinander verknüpfbar aufbereitet werden. Aus diesem Grund überführen immer mehr Staaten zuvor dezentral und möglicherweise analog geführte Register in zentrale Datenbanken, etwa für Personen, Kraftfahrzeuge oder Immobilien. Für die Vermaschung spielen zudem einheitliche Objektidentifikationen, beispielsweise Personenkennzahlen, über die verschiedenen Register hinweg eine kritische Rolle.
2. *Externe Datenquellen* können – so ihre Nutzung durch die Verwaltung erlaubt ist – die Bestands- und Verfahrensdaten von privaten Dienstleistern sein, etwa von Finanzinstitutionen, Transportunternehmen, Telekommunikationsanbietern oder Plattformdienstleistern. Zusätzlich kann auch öffentlich zugängliche digitale Kommunikation, etwa in den sozialen Medien, herangezogen werden.

In Pilotprojekten in Indonesien und den Niederlanden haben *UN Global Pulse*, das *Big-Data*-Programm der Vereinten Nationen, und die niederländische Statistikbehörde soziale Medien bzw. Tageszeitungen mithilfe von *Natural Language Processing*, also der automatischen Analyse natürlichsprachlicher Texte, ausgewertet, um die Preisentwicklung von Grundnahrungsmitteln bzw. die Stimmung in der Wirtschaft (als Indikator für die konjunkturelle Entwicklung) in (Quasi-)Echtzeit zu ermitteln. Die daraus resultierenden Informationen sind zwar weniger zuverlässig als amtliche Erhebungen, ergänzen diese aber nutzbringend, da sie wesentlich schneller zur Verfügung stehen.

3. Mit *vernetzten Sensoren* und dem *Internet der Dinge* nimmt auch die digitale Vermessung der physischen Welt zu. Auch diese Daten könnten den Informationssystemen der öffentlichen Verwaltung zufließen und beispielsweise ein umfassendes digitales Abbild eines Stadtviertels erzeugen.

Ein Pilotprojekt in Bonn hat beispielsweise Glascontainer mit vernetzten Ultraschallsensoren ausgestattet, die den Füllstand melden und die Leerung so bedarfs- statt turnusgemäß organisieren, was Kosten spart und die Servicequalität erhöht. In zahlreichen Städten werden Videosysteme getestet, die Bewegungen von Fußgän-

ger\*innen erkennen und einordnen können, wie etwa Schlägereien oder Fluchtbewegungen, um im Bedarfsfall menschliche Aufmerksamkeit darauf zu lenken.

Insbesondere externe Quellen wie soziale Medien und das Internet der Dinge können Daten von hoher Aktualität liefern, zum Teil sogar in Echtzeit (das sogenannte „Nowcasting“). Diese Datenquellen sind daher eher für Frühwarnsysteme und zeitnahe Interventionen geeignet als staatliche Daten, die oft nur in weit auseinanderliegenden Intervallen aktualisiert werden. Allerdings erfordert gerade die schwankende Datenqualität externer Datenquellen in Behörden, die es zuvor gewohnt waren mit einer „amtlich beglaubigten Wahrheit“ zu arbeiten, ein Umdenken und Sensibilität für unterschiedlich belastbare Datengrundlagen.

---

## 2 Konzeptionelle Grundlagen

Ideeengeschichtlich lässt sich für das Leitbild der datengesteuerten Verwaltung eine Nähe zu Konzepten des wissenschaftlichen Managements durch „*management by numbers*“ im *New Public Management* (NPM) sowie zu kybernetischen und rationalistischen Aspekten der Planungseuphorie der 1960er- und 1970er-Jahre erkennen. Die datengesteuerte Verwaltung fügt sich auch nahtlos in den Trend des aus NPM und rationalistischer *Policy Analysis* hervorgehenden „*evidence-based policy-making*“ ein, also der Politikgestaltung auf empirisch-wissenschaftlicher Grundlage (siehe exemplarisch Esty und Rushing 2007). Der Glaube an die Messbarkeit, analytische Ergründbarkeit und schließlich die Steuerbarkeit der Gesellschaft, welcher im Rahmen des „*participatory turn*“ der 1980er und 1990er in Verruf geraten war, lebt mit dem Leitbild der datengesteuerten Verwaltung wieder auf. Es zehrt daher legitimatorisch von dominanten Meta-Narrativen der Aufklärung wie Rationalität und Positivismus. So wird kritisch von einer Ideologie des „*Dataismus*“ (Van Dijck 2014) gesprochen, nach der jedes Problem bei ausreichender Datenlage durch rationale Analyse gelöst werden kann.

Die datengesteuerte Verwaltung ist also keine vornehmlich technische Innovation, die sich automatisch aus dem Einsatz bestimmter Datentechnologien ergibt, sondern meint die sozialen Praxen, die aus diesen Technologien erwachsen (Ruppert et al. 2015). Die Breite der so eröffneten Möglichkeitsräume zeigt sich in der Literatur, die Visionen von Überwachungsdystopien bis zu Automatisierungsutopien aufspannt (Kling 1996). Auf der hoffnungsvollen Seite der Debatte lassen sich vier wesentliche Versprechen identifizieren:

1. Entlang des traditionellen Vektors des Versprechens technischer Innovationen „*faster, better, cheaper*“ werden insbesondere Effizienzgewinne durch automatisierte Verwaltungsprozesse bis hin zur autonomen Steuerung ganzer Politikfelder durch Künstliche Intelligenzen erwartet (Thapa und Parycek 2018). So sind in der Arbeits- und Sozialverwaltung individuell auf die Bürger\*innen zugeschnittene Maßnahmenbündel denkbar, die auf den analytisch ermittelten Erfahrungswerten aus hunderttausenden vorhergehenden Fällen beruhen. Die technische Verkehrs-

planung und -steuerung unterhalb der verkehrspolitischen Leitlinien Computerprogrammen zu überlassen, ist kein fernliegender Gedanke mehr und wird in Pilotprojekten auf der ganzen Welt bereits erprobt.

2. Die verbesserte Sensorik und die erweiterten Analysefähigkeiten der Verwaltung erlauben ein umsichtiges, *holistisches Regieren*, das auch komplexe Interaktionen verschiedener gesellschaftlicher Teilsysteme antizipieren kann. Diese Perspektive ist vor allem in Kontext des „Smart City“-Diskurses verbreitet. Klassische Beispiele sind die Interaktion zwischen Städtebau und Stadtclima oder Verkehrslenkung und Stadtclima. Auch das Echtzeitmonitoring des urbanen Umfelds, um beispielsweise Einsatz- oder Reinigungskräfte nach Bedarf zu lenken, ist ein bekanntes Szenario.
3. Ein weiteres Versprechen lautet: erhöhte *Responsivität* der Verwaltung für die Wünsche der Bürger\*innen. Diese können beispielsweise aus den sozialen Medien abgelesen werden (Chatfield und Reddick 2018). Verwaltungsintern kann durch die hohe Datendichte von Verfahrensdaten die Servicequalität leichter gesichert werden. Dies eröffnet einen direkten Kommunikations- und Legitimationskanal zwischen Bürger\*innen und Verwaltung. So kann die Verwaltung beispielsweise Unzufriedenheit mit den Öffnungszeiten oder Gebührenordnungen öffentlicher Einrichtungen frühzeitig aus entsprechenden Kommentaren auf Facebook oder Twitter erkennen und darauf reagieren. Auch die datengestützte Wahrnehmung von Mehrbedarfen der Bürger\*innen, beispielsweise bei öffentlichen Verkehrsmitteln oder Sozialleistungen, kann die Verwaltung zur Angebotsanpassung anregen, ohne dass diese Anliegen den klassischen Weg über die politischen Organe nehmen müssen.
4. Die hohe Dichte und Aktualität der *Monitoring*daten der Verwaltung eröffnet die Möglichkeit für „agiles“ Regieren im Sinne der agilen Softwareentwicklung (Mergel et al. 2018). Dies bedeutet eine hohe Iterationsfrequenz an Nachbesserungen, gemäß dem Motto „*Test early, test often*“, aber auch eine veränderte Aufgabenteilung zwischen Politik und Verwaltung. Bei Maßnahmen wie dem Baukindergeld könnte zum Beispiel bereits nach den ersten Implementierungsmonaten geprüft werden, welche Zielgruppen tatsächlich erreicht werden, und bei Verfehlung politisch gewünschter Zielgruppen nachgesteuert werden – wieder und wieder, bis ein zufriedenstellendes Maß erreicht ist. Diese Vorgehensweise ist auch geografisch aufteilbar. Beispielsweise könnten bundesweite Leistungen wie das Elterngeld in unterschiedlichen Bundesländern in verschiedene Varianten eingeführt werden. Aus den Monitoring-Daten der Implementation ließe sich vergleichsweise schnell ermitteln, welche Varianten die gesetzten familien- und arbeitspolitischen Ziele besonders gut erreichen.

Auf der eher kritischen Seite der Debatte findet sich eine Vielzahl unterschiedlicher Perspektiven, von denen hier vier angerissen werden:

1. Aus der Schule der *Surveillance Studies* speist sich die Kritik an der datengesteuerten Verwaltung als Überwachungssystem. Indem Verwaltungsdaten, Datenspuren bei Dienstleistern und im Internet sowie *Monitoring*-Daten aus vernetzten Sensoren

automatisiert zusammengezogen und auf verdächtige Aktivitäten hin ausgewertet werden, verändert sich auch die Art der Überwachung. Das ständige Überwachungspotenzial des Panoptikums wandelt sich zu einem „Panspektrum“, also tatsächlicher Dauerüberwachung mit Hilfe von Computerprogrammen (Braman 2006). Die Folge dieser Beobachtung kann unter anderem eine vorausseilende Selbstdisziplinierung zur Konformität sein. Zudem gibt es in Wirtschaft wie Verwaltung attraktive Einsatzzwecke von – auch personenbezogener – Beobachtung, so dass Systeme entstehen, die später leicht zu anderen Zwecken missbraucht werden können (Lyon 2014). Das bekannteste Beispiel bietet das chinesische Sozialkredit-System, das Kredit-, Vertrauens- und Glaubwürdigkeit aller Bürger\*innen abbilden und so Kreditvergabe, behördliche Angelegenheiten und Gerichtsverfahren beschleunigen soll. Neben Strafregister und Kredithistorie fließen auch persönliches Verhalten und Beziehungen in die Bewertung ein, so dass sich eine umfassende Beobachtung des individuellen Lebenswandels ergibt, die via Sozialkredit-Bewertung Auswirkung auf verschiedenste Lebensbereiche hat, von der Visumsvergabe bis zu den Karrierechancen.

2. Die begleitend zum Aufstieg der neuen Datentechnologien entstandene Disziplin der *Critical Data Studies* bringt mehrere Kritikpunkte an. So wird grundsätzlich die „hyperpositivistische“ Epistemologie datengesteuerter Organisation kritisiert, die für nicht-quantifizierbare Eigenschaften und Prozesse sowie schwache Signale weitgehend blind ist (Rieder und Simon 2018). Die Selektivität der datenbasierten Wahrnehmung führt unter anderem zum sogenannten „*data divide*“, der systematischen Unterrepräsentierung von Menschen, die weniger Datenspuren hinterlassen, weil sie beispielsweise keine Internetnutzer sind. Datensteuerung kann zudem systematische Diskriminierung zur Folge haben, wenn sich gesellschaftliche Ungleichheiten in den Daten spiegeln, mit denen etwa Entscheidungsalgorithmen trainiert werden. Ein bekanntes Beispiel hierfür ist der in den USA eingesetzte COMPAS-Algorithmus, der die Rückfälligkeitswahrscheinlichkeit von Strafgefangenen berechnet, um über ihre frühzeitige Entlassung zu entscheiden. Dieser Algorithmus hatte anhand der historischen Daten die Hautfarbe der Insassen als wichtige Variable identifiziert und Schwarzen daher systematisch eine höhere Rückfallwahrscheinlichkeit zugewiesen.
3. Ein Großteil der Kritik am kennzahlorientierten „*management by numbers*“ im öffentlichen Sektor trifft auch die datengesteuerte Verwaltung, etwa die strategische Ausrichtung des Verwaltungshandelns an bekannten Variablen und Leistungsindikatoren, statt einer Ausrichtung auf die eigentlichen Politikziele (Smith 1995). Auch der Kritikpunkt, dass Daten nicht unbedingt die Realität abbilden, und dort, wo sie es nicht tun, eher die Realität den Daten angepasst wird, lässt sich übertragen (Scott 1998).
4. Ein weiterer Kritikkomplex bezieht sich auf die möglichen Machtverschiebungen durch Datensteuerung der öffentlichen Verwaltung, insbesondere aus wissenspolitischer Perspektive (Thapa 2018). Danach besteht die Gefahr einer Monopolisierung von politikrelevantem Daten bzw. Wissen in Staatshand, so dass die Entscheidungen der Regierung kaum noch anzweifelbar sind. Zudem droht sich die Konkurrenz zwischen dem Erfahrungswissen von Verwaltungskräften und Bürger\*innen mit

datenbasierter Evidenz auszuweiten. In Wien etwa ersetzt ein zentrales, vermaschtes Monitoring- und Vorhersagesystem in der Energieraumplanung das umfangreiche Erfahrungswissen der Quartiersbetreuer\*innen, auf deren Einschätzungen die Energieraumplanung zuvor beruhte, wodurch aber deren umfangreiches lokales Wissen verloren geht. Nicht zuletzt droht durch die datengesteuerte Verwaltung als einer Form der evidenzbasierten Politikgestaltung eine Depolitisierung bzw. Technokratisierung, indem Wertfragen scheinbar in datenbasiert zu optimierende Sachfragen umgedeutet werden.

---

### 3 Praktische Anwendungsfelder

Die neuen Datentechnologien sind in Staat und Verwaltung im Wesentlichen für vier Zwecke interessant: *Beobachtung*, *Analyse*, *Vorhersage* und *Entscheiden*.

1. *Beobachtung* ist die Nutzung der verschiedenen Datenquellen, um gesellschaftliche Entwicklungen in Echtzeit festzustellen oder Informationen zu beschaffen, etwa für die Prüfung eines Antrags. Hier ergibt sich durch die höhere Aktualität und Datendichte ein Vorteil gegenüber früheren Praktiken.

*Beispiel „Did you feel it?“:* Die US-amerikanische Bundesbehörde für Geologie wertet Twitter-Meldungen im Kontext von Erdbeben aus, um ein möglichst aktuelles und – durch Mehrfachmeldungen verifiziertes – realistisches Bild der Schäden zu erhalten.

2. *Analyse* bezeichnet die Suche nach Ursachen und Kausalzusammenhängen von gesellschaftlichen Phänomenen, welche unter Datenreichtum und mithilfe von Maschinenlernen einfacher und in höherer Qualität möglich ist als früher. Die datengesteuerte Verwaltung ist somit auch eine evidenzbasierte Verwaltung, die ihre Aktivitäten nach empirischen Erkenntnissen ausrichtet und diese auch der Politik bereitstellt.

*Beispiel Epidemiologie:* Suchanfragen zu spezifischen Symptomen in Internet-Suchmaschinen werden vermascht mit Umweltdaten ausgewertet, um die Prävalenz ansteckender Krankheiten wie Grippe und Dengue zu ermitteln und den Gesundheitsbehörden so frühzeitig die Möglichkeit zur Intervention zu geben.

3. *Vorhersage* bezieht sich auf die Möglichkeit prädiktiver Analysen, also aus den Mustern in historischen Daten wahrscheinliche Entwicklungspfade zu extrapoliieren. Interessant ist dies insbesondere für die Politikberatung durch die Simulation der Auswirkungen unterschiedlicher politischer Maßnahmen, aber auch als Frühwarnsystem für das Auslösen individueller Verwaltungsinterventionen.

*Beispiel „Troubled Families“:* Ein Pilotprojekt im Rahmen des englischen Troubled Families-Sozialhilfe-Programms zieht Daten von Einsatzkräften, Bildungs- und Gesundheitseinrichtungen sowie Sozialversicherungen zusammen, um frühzeitig Verhaltensmuster zu erkennen, die auf den Eingriffsbedarf einer Familie durch die Sozialbehörden hinweisen. Entsprechend der beobachteten Muster werden Interventionsformen ausgewählt, die gemäß Datenlage in ähnlichen Fällen die höchste Erfolgswahrscheinlichkeit versprechen.

*Beispiel Arbeitsmarktservice Österreich:* Ab 2020 plant der österreichische Arbeitsmarktservice, die Kategorisierung von Arbeitssuchenden nach niedrigen, mittleren und hohen Arbeitsmarktchancen, die über die Beratungsintensität entscheidet, automatisiert durch einen Algorithmus auf Grundlage verschiedener Merkmale wie Arbeitslosigkeitshistorie, Ausbildung, Alter und Wohnort vornehmen zu lassen.

4. *Entscheiden* bezieht sich auf das Potenzial zur datenbasierten, automatisierten Entscheidungsfindung, insbesondere die automatisierte Erstellung von Bescheiden auf Grundlage von verwaltungsinternen wie -externen Datenquellen.

*Beispiel „Bewohner\*innenparkausweis“:* In der Stadt Frankfurt am Main beantragen Anwohner\*innen den Bewohner\*innenparkausweis *online*. Die Korrektheit von Wohnort und Fahrzeugkennzeichen werden automatisch über das Einwohnermelde- und Kraftfahrzeugregister geprüft. Kann die Software nun noch den Eingang der entsprechenden Gebühr in der Stadtkasse feststellen, wird der Bewohner\*innenparkausweis automatisch ausgestellt. Ein Jahr nach Einführung konnte das System bereits die Hälfte der Anträge vollautomatisch abwickeln.

*Beispiel „Umweltorientierte Verkehrssteuerung“:* In den Städten Braunschweig, Erfurt und Potsdam fließen Wetter-, Feinstaub- und Verkehrsdaten für eine intelligente Verkehrssteuerung zusammen. Diese reagiert beispielsweise auf erhöhtes Verkehrsaufkommen oder Feinstaubwerte mit angepasster Verkehrslenkung via Verkehrsleitsystemen, Ampelschaltungen und Routenempfehlungen in einer eigenen Mobilitäts-*App*.

Die Beispiele verdeutlichen: Über alle Politikfelder hinweg bieten sich zahllose Einsatzmöglichkeiten der neuen Datentechnologien. Wenig überraschend findet sich in Verwaltungsfeldern wie Verkehr und Umwelt, die auf eine lange Tradition technisch-empirischer Entscheidungsfindung zurückblicken, die höchste Experimentierbereitschaft. Da die zunehmende Verlagerung zu *Online*-Transaktionen und die Verbreitung von vernetzten Sensoren, z. B. in smarten Fahrzeugen, digitale Datenquellen für immer mehr Lebensbereiche eröffnet, ist eine Vervielfachung dieser Möglichkeiten absehbar.

---

## 4 Perspektiven für Staat und Verwaltung

In der Praxis lassen sich zwar bereits einzelne Anwendungen der neuen Datentechnologien in der öffentlichen Verwaltung finden, „datengesteuerte Verwaltung“ als ein kohärent gelebtes Verwaltungsparadigma ist jedoch noch kaum anzutreffen. Zunehmend werden jedoch die nötigen rechtlichen, organisatorischen und technischen Voraussetzungen geschaffen: *E-Government*-Gesetze, Onlinezugangsgesetz und Verwaltungsverfahrensgesetz haben einige wichtige Grundlagen für den Einsatz der neuen Datentechnologien in der Verwaltung geschaffen (Etscheid 2018). Die Einrichtung harmonisierter digitaler Register und die Einführung einer einheitlichen Personenkennung, um Bürger\*innen über diese Register hinweg sicher wiederfinden zu können,

steht bereits auf der deutschen politischen Agenda (McKinsey 2017). Mit den Anstrengungen im Bereich *Smart City* werden deutschlandweit in Städten und Gemeinden vernetzte Sensoren installiert, Datenplattformen zur Vermischung aufgebaut und Erfahrungen mit den verschiedenen Funktionen datengesteuerter Verwaltung gesammelt. Die ausreichende Rekrutierung von Fachkräften für IT für die öffentliche Verwaltung ist bereits seit einigen Jahren auf der verwaltungspolitischen Agenda. Andererseits stellen sich mit zunehmender Vehemenz grundlegende Gestaltungsfragen (Kolany-Raiser et al. 2018): Wie gestalten wir den Datenschutz in der datengesteuerten Verwaltung, wenn Datensparsamkeit (also nicht mehr Daten zu erheben, als für den Vorgang unbedingt nötig sind) und Zweckbindungsgebot (Daten nur für den ursprünglichen Erhebungszweck zu nutzen) der Logik der neuen Datentechnologie grundsätzlich zuwiderlaufen? Wem gehören die Daten in öffentlichen Registern und aus vernetzten Sensoren? Welche Rolle hat demokratische Willensbildung, wenn politische Fragen zunehmend als datenbasiert optimiert lösbar Sachfragen angegangen werden können? Welche institutionellen Arrangements heben die Qualitäts-, Kosten- und Komfortvorteile datengesteuerter Verwaltung, ohne gleichzeitig die Voraussetzungen für einen Überwachungsstaat zu schaffen? Bis zu welchem Punkt ist es akzeptabel, wenn Entscheidungen über Bürger\*innen automatisiert getroffen werden? Wie können Anforderungen an Transparenz und Nachvollziehbarkeit von Verwaltungshandeln bei algorithmischen Entscheidungen eingehalten werden?

Dies macht deutlich, dass die datengesteuerte Verwaltung keinen einzelnen technisch determinierten Entwicklungspfad besitzt, sondern diese neuen Datentechnologien hochgradig flexibel interpretierbar und einsetzbar sind. Dementsprechend ist die datengesteuerte Verwaltung ein politischer Gestaltungsraum, der von Land zu Land und von Gemeinde zu Gemeinde unterschiedlich umgesetzt werden kann. Welche Gestaltungswege in der datengesteuerten Verwaltung eingeschlagen werden und welche gesellschaftlich-politischen Fragen sich hierbei stellen, zählt in den nächsten Jahren zweifelsohne zu den spannenden Fragen der Verwaltungsforschung.

---

## Literatur

- Braman, Sandra. 2006. *Change of state: Information, policy, and power*. Cambridge: MIT Press.
- Chatfield, Akemi Takeoka, und Christopher G. Reddick. 2018. Customer agility and responsiveness through big data analytics for public value creation. A case study of Houston 311 on-demand services. *Government Information Quarterly* 35(2): 336–347.
- Esty, Daniel C., und Reece Rushing. 2007. *Governing by the numbers. The promise of data-driven policymaking in the information age*. Washington, DC: Center for American Progress.
- Etscheid, Jan. 2018. Automatisierungspotenziale in der Verwaltung. In *(Un)berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft*, Hrsg. Resa Mohabbat Kar, Basanta E. P. Thapa und Peter Parycek, 126–158. Berlin: Kompetenzzentrum Öffentliche IT.
- Giest, Sarah. 2017. Big data for policymaking: Fad or fasttrack? *Policy Sciences* 50:367–382.
- Kling, Rob. 1996. Hopes and horrors. Technological Utopianism and Anti-Utopianism in narratives of computerization. In *Computerization and controversy. Value conflicts and social choices*, Hrsg. Rob Kling, 40–58. San Diego: Morgan Kaufmann.
- Kolany-Raiser, Barbara, Reinhard Heil, Carsten Orwat, und Thomas Hoeren, Hrsg. 2018. *Big Data und Gesellschaft*. Wiesbaden: Springer VS.

- Lyon, David. 2014. Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society* 1(2): 1–13.
- McKinsey. 2017. *Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren*. Berlin: Nationaler Normenkontrollrat.
- Mergel, Ines, Yiwei Gong, und John Bertot. 2018. Agile government. Systematic literature review and future research. *Government Information Quarterly* 35(2): 291–298.
- Pencheva, Irina, Marc Esteve, und Slava J. Mikhaylov. 2018. Big data and AI – A transformational shift for government: So, what next for research? *Public Policy and Administration* 35:24.
- Rieder, Gernot, und Judith Simon. 2018. Vertrauen in Daten oder: Die politische Suche nach numerischen Beweisen und die Erkenntnisversprechen von Big Data. In *(Un)berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft*, Hrsg. Resa Mohabbat Kar, Basanta E. P. Thapa und Peter Parycek, 159–178. Berlin: Kompetenzzentrum Öffentliche IT.
- Ruppert, Evelyn, et al. 2015. *Socialising big data. From concept to practice, Centre for Research on Socio-cultural change working paper series 138*. Manchester: CRESC, The University of Manchester and the Open University.
- Scott, James C. 1998. *Seeing like a state. How certain schemes to improve the human condition have failed*. New Haven: Yale University Press.
- Smith, Peter. 1995. On the unintended consequences of publishing performance data in the public sector. *International Journal of Public Administration* 18(2–3): 277–310.
- Thapa, Basanta E. P. 2018. Vier wissenspolitische Herausforderungen einer datengetriebenen Verwaltung. In *(Un)berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft*, Hrsg. Resa Mohabbat Kar, Basanta E. P. Thapa und Peter Parycek, 268–293. Berlin: Kompetenzzentrum Öffentliche IT.
- Thapa, Basanta E. P., und Peter Parycek. 2018. Data Analytics in Politik und Verwaltung. In *(Un)berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft*, Hrsg. Resa Mohabbat Kar, Basanta E. P. Thapa und Peter Parycek, 40–75. Berlin: Kompetenzzentrum Öffentliche IT.
- Van Dijck, José. 2014. Datafication, dataism and dataveillance. Big data between scientific paradigm and ideology. *Surveillance and Society* 12(2): 197–208.
- Weber, Max. 1922. *Wirtschaft und Gesellschaft*. Tübingen: Mohr Siebeck.



---

# Digitale Ungleichheiten und digitale Spaltung

Norbert Kersting

## Inhalt

1 Klärung des Begriffs .....	220
2 Theoretische Grundlagen .....	222
3 Ausmaß und Struktur digitaler Ungleichheiten: Untersuchungsergebnisse .....	223
4 Perspektiven für Staat und Verwaltung .....	227
Literatur .....	229

---

## Zusammenfassung

Als digitale Spaltung werden ungleiche individuelle und gruppenspezifische Zugangschancen zu digitalen Informations- und Kommunikationstechnologien verstanden. Digitale Spaltung umfasst neben internationalen Unterschieden bezüglich des Digitalisierungsniveau auch regionale Ungleichheiten. Der Zugang zu digitaler Infrastruktur ist in Deutschland zum Teil noch rückständig, was sowohl temporär (bei stärkerer Nutzung) als auch regional (auf dem Land) deutlich wird. Neben den Zugangsmöglichkeiten als erstem Level der digitalen Spaltung sind als zweites Level die Kenntnisse und Kompetenzen der Bürger\*innen relevant. Diesbezügliche Disparitäten zeigen sich beim Vergleich zwischen Bevölkerungsgruppen wie Jugendlichen und Senioren, Männern und Frauen (Gender Gap), aber auch bei marginalisierter armer Bevölkerung, Gruppen mit Migrationshintergrund oder Menschen mit Behinderungen. Digitale Spaltung überlappt und verstärkt somit bestehende soziale und partizipative Ungleichheiten. Lösungsvorschläge stellen neben der Anerkennung der digitalen Infrastrukturzugänge als Teil staatlicher Daseinsvorsorge die digitale Gleichheit (Netzneutralität) in den Vordergrund. Zum anderen sollen gemischte (*blended*) Partizipations- und Bildungsangebote die notwendigen Kenntnisse vermitteln.

---

N. Kersting (✉)

Institut für Politikwissenschaft, Universität Münster, Münster, Deutschland

E-Mail: [norbert.kersting@uni-muenster.de](mailto:norbert.kersting@uni-muenster.de)

## Schlüsselwörter

Digitale Infrastruktur · Netzneutralität · Medienkompetenzen · Gender Gap · Politische Partizipation

## 1 Klärung des Begriffs

Mit dem Begriff digitale Spaltung werden die ungleichen Zugangsmöglichkeiten zu den digitalen Informations- und Kommunikationstechnologien beschrieben. Bevölkerungsgruppen können von deren Nutzung aufgrund mangelnder Infrastruktur und/oder fehlender individueller Ressourcen ausgeschlossen sein. Insofern wird auf einer ersten Ebene digitaler Spaltung (*First Level Digital Divide*, Makroebene) als mangelhafte Versorgung mit digitaler Infrastruktur (Norris 2001) und auf einer zweiten Ebene (*Second Level Digital Divide*, Mikroebene) als unterschiedlich ausgeprägte Medienkompetenzen definiert (Mossberger et al. 2008).

*First Level:* Digitalisierung bewirkt über eine Ausweitung der Nutzer\*innen als auch über größere Datenmengen neuer Onlinedienste höhere Ansprüche an die Infrastruktur. Aufgrund der starken Visualisierung von neuen Dienstleistungsplattform im *Internet* wie zum Beispiel *YouTube*, *Netflix* und *Zoom* sind größere und schnellere Datentransfers notwendig. Von zentraler Bedeutung ist dabei neben dem Durchfluss die Geschwindigkeit innerhalb der digitalen Infrastruktur. Bei starker Nutzung (wie z. B. der Covid-19-Pandemie) sind die Netze überlastet. Dabei wird in Deutschland flächendeckend eine mangelnde Versorgung der Haushalte mit schnellen Glasfaserzugängen deutlich, die zudem den ländlichen Raum ausgrenzt. Man kann neben der nationalen auch eine internationale Ungleichheit in Bezug auf die Digitalisierung feststellen. Auf der einen Seite zeigen sich im globalen Vergleich Länder, in denen das *Millennium Development Goal No. 8* zur Digitalisierung kaum oder nicht erreicht wurde und ein Großteil der Bevölkerung von diesen digitalen Netzen und Serviceleistungen ausgeschlossen ist (UN 2015, S. 83). Dabei wird bei den Indikatoren zwischen der Nutzung von Mobiltelefonen, *Personal Computern* sowie anderen Internet-Zugängen unterschieden. Hier wird eine führende Rolle der OECD-Länder konstatiert. Während traditionelle Informationstechnologien wie zum Beispiel Telefonleitungen hier deutlich weiterverbreitet sind als zum Beispiel in Asien, Lateinamerika oder Afrika, so galt dies auch für die Nutzung von Computern sowie von Internetanschlüssen. In Europa liegen dabei die skandinavischen Länder vor Mitteleuropa und diese wiederum vor den südlichen Ländern Europas. Gleiches galt für die Nutzung für Mobiltelefone, bei denen die Länder des Südens jedoch deutlich aufholten. In den Jahren seit 2000 zeigt sich dabei eine Tendenz, dass nicht allein die Verbreitung von *Personal Computern* ausschlaggebend ist. Aufgrund der weiten Verbreitung von Mobiltelefonen wurde insbesondere in einigen ostafrikanischen Ländern wie zum Beispiel Ruanda und Kenia ein Schwerpunkt auf die Entwicklung von mobilen Technologien gesetzt („mobile first“). Insofern wird Afrika der erste Post-PC-Kontinent sein, in denen wesentliche digitale Dienstleistungen über Mobiltelefone umgesetzt werden. Afrika ist in Bezug auf die Ein-

führung von mobilem *E-Banking* auch den OECD-Ländern deutlich voraus. In Europa und den USA wurde die *Mobile-First*-Strategie erst deutlich später aufgegriffen.

*Second Level:* Individuelle Ressourcen wie z. B. Medienkompetenzen umfassen digitale Kenntnisse, die das Mediennutzungsverhalten insbesondere bei politischer Beteiligung prägen. In Zusammenhang mit gesellschaftlicher Ungleichheit und sozialer Spaltung werden divergierende kognitive Ressourcen auch in Bezug auf die Kenntnisse der digitalen Medien deutlich (Dijk 2005). So unterscheiden sich diese Kenntnisse über innovative digitale Technologien in verschiedenen Milieus, in sozialen Gruppen wie auch in den unterschiedlichen Alterskohorten. Insofern gibt es eine Überlappung von sozialer (arm vs. reich), partizipativer (aktiv vs. passiv) und digitaler Spaltung. Deutschland liegt dabei in Bezug auf die Nutzung der sozialen Medien deutlich hinter anderen westlichen Industrienationen wie Frankreich und den USA zurück. Dennoch zeigt sich auch hier eine zunehmende Zahl deutscher Nutzer (ARD-ZDF 2017). Im deutschen Kontext wird deutlich, dass sich aber insbesondere die Multiplikatoren im politischen Bereich, wie zum Beispiel Journalisten und Politiker, in Deutschland stärker in den sozialen Medien wie zum Beispiel *Twitter* engagieren. 2016 besaßen ca. 40 Millionen Deutsche ein *Smartphone*. 33 Millionen Nutzern griffen auf *Messengerdienste* wie zum Beispiel *WhatsApp* zurück. Es existierten 24 Millionen *Facebook-Accounts*, aber nur etwa 4 Millionen *Twitter-Accounts*. Hierbei lässt sich jedoch nur begrenzt von der Anzahl der *Accounts* auf die möglichen Nutzungsmuster schließen, da viele dieser *Accounts* lediglich sporadisch oder gar nicht benutzt werden. So ist zu beachten, dass man entsprechend der 90-9-1 Regel davon ausgehen kann, dass mehr als 90 % aller Nutzer lediglich Informationen im Netz beobachten (*Lurkers*). Demgegenüber stehen etwa 9 %, die die neuen Medien sporadisch aktiv benutzen, und etwa 1 Prozent starke Nutzer (*Super Twitterroos*) (Roemmele 2012).

Die internationalen Entwicklungstrends orientieren sich weg vom PC hin zu mobilen Endgeräten wie zum Beispiel *Smartphones*, wobei noch Generationsunterschiede deutlich werden. Das *Smartphone* wird in Deutschland durchschnittlich täglich bis zu 89 Mal benutzt (Initiative D21 2018). Während die *Babyboomer* Generation (bis 1965) als digitale Immigranten sich erst in der Postadoleszenz mit der Digitalisierung befasste, sind die jüngeren Generationen deutlich früher hiervon betroffen. Die Generation X (bis 1980) hat bereits die Entwicklung der sozialen Medien in der Adoleszenz wahrgenommen. Dennoch ist diese Generation häufig – auch aufgrund stark materialistischer Ausrichtung – eher durch eine geringere politische Beteiligung charakterisiert. Waren lange Zeit die mittleren Bevölkerungsgruppen im Alter zwischen 30 und 50 Jahren die aktiven Träger sowohl des politischen als auch des sozialen Engagements, sind diese zunehmend durch ökonomische Bindungen und stärker familienorientierte Aktivitäten weniger politisch aktiv als noch in den davorliegenden Jahrzehnten (Kersting 2016a). Beim digitalen politischen Engagement werden sie mittlerweile bei den Wachstumszahlen von den *Babyboomer* und jungen Senioren übertroffen. Dieses geringere politische Engagement im Alter von 25–55 Jahren galt lange Zeit als Phänomen, das insbesondere Frauen betraf, die im mittleren Alter vor allem mit der Kindererziehung stark

beschäftigt waren. Mittlerweile zeigt sich bei beiden Geschlechtern in dieser Altersgruppe eine deutliche Abnahme politischen Engagements (Kersting 2016b), während die jüngeren Generationen sich weiterhin stark engagieren. Diese Generation X (1965–1980) ist zwar internetaffin, aber beruflich stark eingebunden, während die Generation Y (1990–2000) und die *Millennials* (seit 2000) bereits als *Digital Natives* gelten. Mit der Weiterentwicklung der Digitalisierung und der Dominanz des *Smartphones* sind sie bereits im vorpubertären Kindesalter digital sozialisiert.

---

## 2 Theoretische Grundlagen

Im Folgenden wird digitale Spaltung in Bezug auf politische *Online*-Partizipation und die Nutzung staatlicher Dienstleistungen analysiert. Digitale Aktivitäten sind nur sehr begrenzt politisches Engagement. Die Mehrzahl der Nutzungen digitaler Medien bezieht sich auf den ökonomischen und den Unterhaltungsbereich. Internetnutzer werden als *Shopper*, *Chatter* oder *Gamer* tituliert. Die Mehrzahl der Nutzung ist freizeitorientiert und unterhaltungsorientiert. Politische *Online*-Partizipation und *Online*-Verwaltungskontakte sind eher seltener.

Die *Gateway-These* behauptete daher ein wachsendes Engagement vormals inaktiver Bürger. Die *Substitutionsthese* sah dagegen in der Digitalisierung lediglich neue Kanäle für ohnehin bereits politisch Aktive. Hierdurch könnte sich die partizipative Spaltung eher vergrößern als verkleinern. Die übertriebenen Erwartungen der Vertreter der *Gateway*-These wurden vielfach enttäuscht, da politisches Engagement eher über Themen als über Kanäle forciert wird. Dennoch war die digitale Mobilisierungsfunktion wichtig. Die Substitutionsthese übersah, dass insbesondere die jüngeren Generationen der *Millennials* ohnehin digital sozialisiert wurde. Häufig sieht man bei den *Digital Natives* ein zweites, virtuelles Leben im Internet. Erste digitale politische Erfahrungen tragen zu späterer analoger *Offline*-Partizipation bei.

Bei der Analyse der gesellschaftlichen Gruppen, des politischen Engagements sowie der Nutzung von digitalen Medien lässt sich neben einer digitalen Spaltung auch eine soziale und eine partizipative Spaltung darstellen. Die *soziale* Spaltung basiert auf ungleichen Teilhabechancen von verschiedenen Gruppen, definiert nach Einkommen, Geschlecht, Alter und weiteren sozialen Charakteristika wie z. B. Migrationshintergrund. Die *partizipative* Spaltung unterscheidet politisch aktive und inaktive Gruppen. Letztere lassen sich in „politische Zyniker“ und „politisch apathische Bürger“ unterteilen (Kersting 2013). In der ersten Dekade des neuen Millenniums zeigte sich zunächst eine Reaktivierung der zynischen politischen Gruppen. Diese besitzen relativ hohe politische Kenntnisse, sehen aber ein Engagement im politischen System als nicht effektiv an. Aufgrund dieser geringen politischen externen *Efficacy*, also dem mangelnden Vertrauen in politische Einflussmöglichkeiten, engagierten sich diese Gruppen lange Zeit nicht. Mit der Protestwelle um Stuttgart 21 und einem neuen Engagement dieser häufig aus der Babyboomer-Generation rekrutierten Bevölkerungsgruppe kam es seit den 2010er-Jahren zu einer Re-Aktivierung dieser Gruppe als „Wutbürger“. Im Rahmen der Kritik an dem politischen Establishment und einer neuen, insbesondere rechtspopulistischen

Welle, zeigen sich zudem eine neue Aktivierung von Bevölkerungsgruppen, die lange Zeit eher als politisch apathisch angesehen wurden. Diese attestierten sich häufig eine geringe interne *Efficacy*, das heißt, sie sahen sich als nicht kompetent in Bezug auf politisches Engagement an. In dieser Gruppe kam es durch rechtspopulistischen Protest und durch die Entwicklung neuer politischer Parteien zu einer Reaktivierung.

Die Digitalisierung wurde lange Zeit als große Chance zur politischen Mobilisierung über Onlinekanäle angesehen (Norris 2001). Neue Öffentlichkeiten sollten die demokratischen Systeme revitalisieren. Dabei spielt *Online*-Partizipation eine besondere Rolle in der politischen Sozialisation von Jugendlichen, da sie den Einstieg in das politische Engagement beinhalten konnte. *Online*-Medien bewirken danach eine Mobilisierung und hieraus resultierend auch *Offline*-Engagement. Über *Online*-Partizipation in sozialen Netzwerken (*Facebook*, *Twitter*, *Instagram*) lassen sich neben dialogischen Instrumenten auch stark demonstrative Partizipationsformen realisieren. In diesem Zusammenhang ist die Entwicklung von Echokammern und Teil-Öffentlichkeiten, d. h. segmentierten Diskursarenen im Internet, von besonderer Bedeutung. Hier können auf der einen Seite die individuelle Identitätsfindung in einem etwas breiteren gesellschaftlichen Diskurs bewerkstelligt werden und dabei die Entwicklung von neuen politischen Gemeinschaften vorangetrieben werden. Problematisch ist aber, dass in diesem Bereich eine besondere Konzentration auf partikulare Einzelinteressen, eine geringe Reflexivität, eine Radikalisierung und oft eine stärkere Ausländerfeindlichkeit deutlich wird.

---

### **3 Ausmaß und Struktur digitaler Ungleichheiten: Untersuchungsergebnisse**

Im Folgenden wird zunächst die digitale Infrastruktur als erste Ebene der Digitalen Spaltung analysiert, bevor divergierende Kompetenzen verschiedene Bevölkerungsgruppen untersucht werden. Bei der Betrachtung unterschiedlicher sozialer Gruppen zeigen sich deutliche Ausgrenzungstendenzen und mangelnde digitale Inklusion. In den weiteren Abschnitten werden die Gruppen Jugendliche, Senioren, Menschen mit Migrationshintergrund und Menschen mit Behinderung näher analysiert. Weiterführende Analysen zu Gruppen wie z. B. prekäre oder arme Haushalte fehlen bislang.

#### **3.1 Zugangsmöglichkeiten und digitale Infrastruktur**

Der Breitbandatlas der Initiative D 21 sieht 2011 grundsätzlich zwei Drittel der Bevölkerung mit einem Zugang von mehr als 16 MBit/s. Bezüglich der Breitbandverfügbarkeit der Bundesländer wurden bereits damals Disparitäten deutlich. 2017 sind demnach nahezu alle Haushalte mit einer Geschwindigkeit von mindestens 6 MBit/s abgedeckt. Es zeigen sich ab einer Größe von mehr als 30 MBit/s regionale Disparitäten (BMVI 2017). Während Länder wie Bayern und Baden-Württemberg

über 84 % und in den Stadtstaaten sogar über 95 % mit dieser schnellen Technologie versorgt werden, liegen Länder wie zum Beispiel Mecklenburg-Vorpommern (67 %) oder Brandenburg (71 %), Sachsen (69 %) und Sachsen-Anhalt (60 %) zurück. Es zeigt sich somit eine Ungleichverteilung zwischen neuen und alten Bundesländern. Zudem sind diese Geschwindigkeiten nicht in Spitzenzeiten bei einer hohen Anzahl von Nutzern zu erreichen, da es sich zumeist nicht um Glasfasertechnologien handelt. Auch bei der Mobilfunk-LTE-Versorgung wird davon ausgegangen, dass grundsätzlich mehr als 96 % der Haushalte hiermit versorgt sind (BMVI 2017). Doch auch hier besteht in den strukturschwachen ländlichen Regionen sowie bei hoher Nutzung eine deutlich geringere Verfügbarkeit. Die Bandbreitenklassen werden weiterhin insbesondere durch DSL bzw. VDSL abgedeckt, d. h. es werden nur die Stadtteile und nicht die Haushalte über Glasfaseranschlüsse verbunden. Weitere Anbieter wie Kabel Deutschland oder Unitymedia besitzen deutlich geringere Geschwindigkeiten. Von besonderer Bedeutung ist auch die gewerbliche Breitband- bzw. Glasfaser-Verfügbarkeit. Diese liegt bei den Leitungen mit mehr als 50 Mbit/s bei allen Firmen in Gewerbegebieten deutlich höher (ca. 80 %), während Mischgebiete nur ca. 70 % dieser Geschwindigkeit erreichen. Obwohl diese regionalen Ungleichheiten beim Netzausbau existieren, gibt es bei der Infrastruktur keine Diskriminierung von Gruppen. Die Netze selbst erzeugen keine Bevorzugung einzelner Gruppen. Bislang besteht eine hohe Netzneutralität, das heißt, es werden grundsätzlich keine Arten von Datenübertragungen im Internet bevorzugt oder benachteiligt. Neben der Geschwindigkeit der digitalen Infrastruktur in Bezug auf den Datendurchsatz ist die Latenz (Reaktionszeit) von besonderer Bedeutung. Hier von hängen neue Möglichkeiten für Technologien wie zum Beispiel autonomes Fahren ab.

### 3.2 Jugendliche

Die jüngere Generation galt lange Zeit als politisch desinteressierte, beteiligungsferne und schwer erreichbare Gruppe, die aber stark durch die Digitalisierung beeinflusst werden kann. Insofern wurde der Digitalisierung und den neuen Kanälen im Internet eine besondere Rolle bei der Sozialisation zugewiesen. Über neue Informations- und Kommunikationstechnologien sollten insbesondere Jugendliche stärker an die Politik gebunden werden und mobilisiert werden. Auch die Angebote der kommunalen Verwaltungen sollten – so die Annahme – von dieser Gruppe stärker genutzt werden. Ein mangelndes politisches Engagement kann laut neuerer Untersuchungen wie zum Beispiel der vorletzten Shell Jugend-Studie (2015) nicht mehr festgestellt werden. Gleichzeitig wurde der Generation Y und den *Millennials* ein größeres politisches *Online*-Engagement attestiert. Die Jugendlichen unterscheiden sich diesbezüglich beim politischen Engagement kaum von älteren Kohorten wie den *Babyboomer*n. Es wird allerdings deutlich, dass es eine geringere feste Zuordnung zu politischen Parteien und zu sozialen Organisationen wie Kirchen gibt, die ein regelmäßiges Engagement beinhaltet. Jugendliche wie andere soziale Gruppen binden sich zunehmend nur sporadisch an neue soziale Bewegungen und Organisa-

tionen. Ihr Engagement bleibt stark auf einmalige „Events“ bezogen und ist auch aufgrund der Suche nach der eigenen Identität in deutlich höherem Maße expressiv (Kersting 2016b).

### 3.3 Senioren und *Silver Surfer*

In den 1980ern wurde Senioren im Pensionsalter ab 65 häufig ein politisches Disengagement attestiert. Auch die Internetnutzung in dieser Altersgruppe lag am Ende der 1990er lange Zeit deutlich zurück (Statistisches Bundesamt 2016, S. 78 ff.). Entsprechend damaliger (Dis-)Engagement-Theorien nahm nach dem 65. Lebensjahr das politische Engagement aufgrund mangelnder Ressourcen und vor allem auch aufgrund eines schlechteren Gesundheitszustandes ab. Dies hing – insbesondere in den älteren ärmeren Bevölkerungsgruppen in den ländlichen Regionen – mit einem niedrigeren Bildungsstand und mangelnden politischen Kenntnissen zusammen. Bei der *Babyboomer*-Generation zeigte sich dagegen bereits eine starke Politisierung, die mit einer erhöhten Lebenserwartung und grundsätzlich höherem Engagement im Alter korreliert. Ein hohes politisches Engagement – insbesondere gegen infrastrukturelle Großprojekte wie zum Beispiel Stuttgart 21 – hat zur Mobilisierung von älteren etablierten Mittelschichten geführt. Die Sitzblockade war nicht nur in der Mitte der Gesellschaft angekommen, sondern auch bei den Senioren. Senioren besitzen die für Partizipation notwendigen Zeitressourcen wie auch die kognitiven Ressourcen und oft auch die ökonomische Unabhängigkeit, um sich politisch stärker einzubringen. Dabei zeigt sich im linken Spektrum eine Reaktivierung der „politischen Zyniker“. Zudem wird auch in den letzten Jahren ein starker Protest im Bereich von migrationsfeindlichen rechtspopulistischen Gruppen deutlich. Hier existieren starke Anti-Establishment-Einstellungen. Befürchtungen eines Zerfalls der nationalen Identität und eines drohenden sozialen Abstiegs gelten als Ursachen für politisches Engagement.

In dieser älteren Altersgruppe zeigen sich aber in den letzten Jahren gravierende Veränderungen bei der *Online*-Partizipation. Dabei liegen die Ursachen insbesondere in zwei Faktoren. Auf der einen Seite ist die Kohorte der *Babyboomer* weitgehend in das Rentenalter aufgerückt und anderseits sind die technischen Möglichkeiten erweitert worden und somit Barrieren des digitalen Engagements für Ältere deutlich gesunken. Neuere *Laptops* und bedienungsfreundliche *Tablets* sind auf dem Markt. Dabei zeigte sich ein drastischer Anstieg der Internetnutzung. Neuere Zahlen zeigen, dass zwei Drittel der Nutzer der älteren Generation regelmäßig im Internet und zum Teil täglich *online* aktiv sind (Kersting 2015). Ein starker Fokus liegt auf Informationsbeschaffung über *Online*-Angebote der großen Zeitungen und Zeitschriften, die von zwei Dritteln der Nutzer frequentiert werden. Weniger als ein Drittel sind in sozialen Netzwerken wie zum Beispiel *Facebook* aktiv. Der Fokus liegt insbesondere auf sozialen und ökonomischen Aktivitäten und im Rahmen der Kommunikation mit den Familienmitgliedern vor allem auf *Messengerdiensten* wie zum Beispiel *WhatsApp*. Bisher unterschiedliche digitale Nutzungsverhalten gleichen sich heute langsam an, da bereits jetzt so genannte *Silver Surfer* die neue

Generation der Senioren darstellen und diese sich weniger über Ressourcenmangel (Zeit, Einkommen, Kenntnisse zu Digitalisierung, Computerkenntnisse etc.) charakterisieren. Erst im sehr hohen Alter beginnt das Disengagement und eine deutlich geringere Nutzung unterschiedlicher Kommunikationskanäle.

### **3.4 Digitale Geschlechterungleichheit und der Gender Gap**

Die digitale Spaltung spiegelt sich auch in der Geschlechterungleichheit in verschiedenen Bereichen wider. Frauen finden sich nicht nur seltener in den Führungsetagen der großen digitalen Konzerne. Sie sind außerdem in der Gruppe der Softwareentwickler unterrepräsentiert. Dies scheint damit zusammenzuhängen, dass die Technikaffinität bei vielen Frauen bislang weniger stark ausgeprägt ist als bei Männern (Langer 2012). Dabei zeigen sich sowohl geschlechtsbezogen unterschiedliches Nutzungsverhalten als auch Tendenzen einer Nivellierung dieser Unterschiede. Deutlich wird, dass grundsätzlich Frauen weniger Zeit zum *Surfen* und zum *Downloaden* aufwenden. Sie nutzen deutlich mehr Zeit für Informationsseiten und Diskussionsseiten im Bereich Kultur und Freizeit. Männer nutzten das *Internet* hingegen vermehrt für Video-Konsum. Dies gilt insbesondere für soziale Medien wie zum Beispiel *YouTube*. Gleichzeitig waren sie stärker in *Weblogs* und bei Kommentaren im *Internet* aktiv. Bei den Senioren sind Unterschiede zwischen Männern und Frauen offensichtlich. Während etwa drei Viertel der Männer zwischen 65 und 75 täglich aktiv *surfen*, tun dies nur etwas mehr als die Hälfte der Frauen. Auch bei Internetnutzern, die für die Entwicklung neuer *Software* eine besondere Rolle spielen, sind Frauen eher unterrepräsentiert. Typische Internetpioniere und *First User* sind männlich, zwischen 20 und 40 Jahre alt, beschäftigt, hochgebildet und nutzen das Internet sowohl für ökonomische Zwecke als auch zur Unterhaltung.

### **3.5 Digitale Integration und Migration**

Bevölkerungsgruppen mit Migrationshintergrund sind häufig sozial marginalisiert, aber auch Ziel diverser Integrationspolitiken. Dies macht sich besonders deutlich in der Gruppe der Flüchtlinge. Personen mit Migrationshintergrund und insbesondere Flüchtlinge besitzen in der Regel Mobiltelefone zur internen Kommunikation und als Medium der Information über das Heimatland. Während Flüchtlinge durch die Nutzung von *Messengerdiensten* und *E-Mail* sowohl den Kontakt zu ihren Familien in den Kriegs- und Krisenregionen herstellen, sind sie von der Nutzung digitaler Angebote in Deutschland oft bereits sprachlich ausgeschlossen. Die Internetseiten von deutschen Behörden sind vielfach nicht auf Englisch oder in anderen Sprachen verfügbar. Sie verwenden oft keine leicht verständliche Sprache. Weiterhin sind Bereiche wie *E-Learning* und Plattformen für den Spracherwerb kaum vorhanden bzw. oft nicht auf mobile Endgeräte zugeschnitten.

### 3.6 Behinderung und Exklusion

Die Gruppe der Menschen mit Behinderungen in Deutschland ist durch eine starke Heterogenität gekennzeichnet. Darauf reagiert ein breites Angebot im Bereich der Information und des Lernens. Für diese Bevölkerungsgruppe ist Barrierefreiheit von zentraler Bedeutung. Die Internetseiten von staatlichen Behörden auf lokaler, regionaler und nationaler Ebene als auch zivilgesellschaftliche und privatwirtschaftliche Angebote weisen eine derartige Barrierefreiheit und Formulierungen in leichter Sprache allerdings nur selten auf (Wei und Hindman 2011).

---

## 4 Perspektiven für Staat und Verwaltung

Die Strategien zur Auflösung der digitalen Spaltung auf der infrastrukturellen Ebene (*First Level Digital Divide* auf der Makroebene) und auf der individuellen Ressourcenebene (*Second Level Digital Divide* auf der Mikroebene) sind vielfältig. Auf dem ersten Level der infrastrukturellen Zugangsmöglichkeiten liegt der Hauptbedarf und eine wichtige Aufgabe in der Bereitstellung dieser Infrastruktur für die einzelnen Haushalte. Insofern geht es um den Einsatz von Glasfasertechnologie oder ähnlich schneller Infrastruktur in allen Regionen. Hierfür muss die digitale Infrastruktur als Teil der Daseinsvorsorge anerkannt werden. Digitale Bürgerrechte und digitale Souveränität können nur über das Recht auf gleiche Zugangsmöglichkeiten zu den digitalen Angeboten realisiert werden. Aufgrund vielfachen Marktversagens scheinen die notwendigen breiten Zugangsmöglichkeiten nur über eine staatliche Bereitstellung der Netzinfrastruktur bewerkstelligt werden zu können. In Deutschland hatten 2017 nahezu alle Bevölkerungsgruppen einen schnellen Internetzugang mit max. 25 Mbit/Sekunde (BMVI 2017). Dies gilt aber nicht in Spitzenzeiten und auch nicht flächendeckend. Es zeigen sich leichte Unterschiede bei den Bundesländern (Ost-West) und zwischen ländlichen und städtischen Regionen. Diese aggregierten Zahlen sind zum Teil irreführend, da diese Geschwindigkeit in Spitzenzeiten real nicht erreicht werden kann. Bei stärkerer Nutzung und insbesondere in Krisenzeiten wie bei der Covid-19 Pandemie sind die Netze überlastet. Hier ist die Nutzung von Breitbandtechnologien, die auf Glasfaservernetzung bei den Hausanschlüssen setzen, der zentrale Indikator, da diese einen hohen Datentransfer erlaubt. Die schnellen Glasfasertechnologien können bislang nur von wenigen Bevölkerungsgruppen genutzt werden. Seit 2017 setzt man flächendeckend auf diese Technologie und verzichtet auf den Ausbau von anderen, deutlich langsameren und begrenzten Zwischentechnologien.

Ältere internationale Lösungswege wie z. B. in Griechenland sahen unter anderem Telezentren, Multi-Zweck-Gemeinschaftszentren und Terminals in öffentlichen Gebäuden wie zum Beispiel in Büchereien oder Poststation vor. Mittlerweile wird diese Idee der digitalen Gemeinschaftserlebnisse wieder aufgegriffen. So bieten Vereine digitale Abteilungen im *E-Sport* an, in denen vor allem Jugendliche gemeinsam elektronische Sportarten praktizieren können. Gleichzeitig gründen sich vereinzelt multikulturelle Computer-Clubs, die zur Integration und indirekt zur Ausbildung

von Jugendlichen zumeist mit Migrationshintergrund beitragen. Die gemeinsame Nutzung von digitalen Infrastrukturen in Nachbarschaftszentren wie zum Beispiel Bibliotheken, aber auch digitale Plattformen ([nebenan.de](#)) dienen auch der Entwicklung von analogen nachbarschaftlichen Netzwerken und Gemeinschaft.

Digitalisierung hat zu einer verstärkten Individualisierung beigetragen. Digitale Enklaven und Informationsblasen in den sozialen Medien, die sich oft durch Dominanz von *Hate Speech* auszeichnen, prägen den sozialen wie politischen Diskurs. Die Aufgabe von politischen Verwaltungen und Parteien und anderen staatlichen wie zivilgesellschaftlichen Institutionen wird es zunehmend sein, diese segmentierten Arenen zu einer gemeinsamen Diskursarena zusammenzufügen, um ein gegenseitiges Verstehen zu ermöglichen. Der Abbau von digitaler Spaltung kann dabei zu Integration und Inklusion beitragen.

Dabei ist die Entwicklung von Instrumenten der Bürgerbeteiligung, die *Online-Partizipation* und *face-to-face*-Kommunikationen miteinander verbinden (*blended participation*), von besonderer Bedeutung. Hierüber könnten besondere Medienkompetenzen vermittelt werden, die zu neuen *Digital Skills*, aber auch zu einem neuen medialen Habitus und zur *Netiquette* beitragen. Die Nutzung von digitalen Technologien zur Vernetzung von Bürgern auf der lokalen Ebene, in der Nachbarschaft und in der Stadt muss im Rahmen einer *Smart City* einen hohen politischen Stellenwert besitzen. Hierüber lassen sich nicht nur neue nachhaltige Strategien und Plattformen einer *Sharing Economy* entwickeln, sondern auch neue Gemeinschaften, die zentrale Aufgaben im neuen Millennium wie zum Beispiel Seniorenbetreuung und Integration aufgreifen können.

Bei Jugendlichen ist sozialer Protest Teil der Identitätsfindung und der Jugendkultur. Neue *Online-* und *Offline-Partizipationsangebote* (*invited space*) der Politik und Verwaltung, der sozialen Bewegungen und der politischen Parteien können für Jugendliche attraktiv sein, wenn auch Bedürfnisse nach Expressivität und Identitätsuche beachtet und einbezogen werden. Dabei drängen Jugendliche auf eine Entwicklung selbstbestimmter, relativ autonomer Räume (*invented space*), um insbesondere Kontrollmechanismen und der Dominanz durch Hierarchien zu entfliehen. Insofern wird eine deutliche Hinwendung der Politik und Verwaltung an vermeintliche Bedürfnisse von Jugendlichen von diesen selbst als Anbiederung wahrgenommen und führt zu einer Gegenbewegung und Gegenöffentlichkeit, um sich gerade von diesem *invited space* abzugrenzen.

Multiple sozioökonomische und kulturelle Spaltungen der Gesellschaft wirken sich auch auf den Prozess der Digitalisierung der Gesellschaft aus. Zwar sind Strategien und Ansätze zur Auflösung speziell der digitalen Spaltung nötig. Eine langfristige Lösung der Probleme und ein gleichmäßiger digitaler Zugang können aber sicherlich nur über einen Abbau der sozioökonomischen Unterschiede erreicht werden. Der digitalen Spaltung auf der Makroebene als auch den mangelnden Medienkompetenzen auf der Mikroebene, die zu prekärer digitaler Souveränität beiträgt, kann zwar durch direkte Bildungsmaßnahmen entgegengewirkt werden, langfristig bedarf es aber auch einer Entwicklung in Richtung größerer sozioökonomischer Gleichheit.

## Literatur

- ARD-ZDF. 2017. *ARD/ZDF-Onlinestudie 2017*. <http://www.ard-zdf-onlinestudie.de/archiv-1997-2018/>.
- BMVI. 2017. *Aktuelle Breitbandverfügbarkeit in Deutschland. Erhebung des TÜV Rheinland im Auftrag vom BMVI*. Berlin: Bundesministerium für Verkehr und digitale Infrastruktur.
- Dijk, Jan A. G. M. van 2005. *The deepening divide. Inequality in the information society*. Thousand Oaks: Sage.
- Initiative D21. 2018. *D21 Digital index 2017/2018*. Berlin: Initiative D21 e.V.
- Kersting, Norbert. 2013. Online participation. From ‚invited‘ to ‚invented‘ spaces. *International Journal of Electronic Governance* 6(4): 270–280.
- Kersting, Norbert. 2015. Senioren und politische Online-Partizipation. Engagement und Disengagement der Silversurfer. *Zeitschrift für Politikberatung* 7(4): 160–172.
- Kersting, Norbert. 2016a. Politische Online-Beteiligung im internationalen Vergleich. Eine Revitalisierung politischer Beteiligung? *Zeitschrift für Vergleichende Politikwissenschaft* 10(2 Suppl): 91–113.
- Kersting, Norbert. 2016b. Onlinebeteiligung und Jugendliche. Expressiv und unabhängig? *Der Bürger im Staat* 66(4): 278–285.
- Langer, Christian. 2012. *Digitale Spaltung. Eine kritische Analyse*. Saarbrücken: Akademikerverlag.
- Mossberger, Karen, Caroline J. Tolbert, und Ramona S. McNeal. 2008. *Digital citizenship. The internet, society, and participation*. Cambridge, MA/London: The MIT Press.
- Norris, Pippa. 2001. *Digital divide. Civic engagement, information poverty, and the internet worldwide*. Cambridge: Cambridge University Press.
- Roemmele, Andrea. 2012. Electronic political campaigning. In *Electronic democracy*, Hrsg. Norbert Kersting, 103–124. Opladen: Barbara Budrich.
- Shell. 2015. *Shell Jugend Studie 2015*. <https://www.shell.de/ueber-uns/shell-jugendstudie.html#vanity-aHR0cHM6Ly93d3cuc2hbGwuZGUvanVnZW5kc3R1ZGll>. Zugegriffen am 02.05.2020.
- Statistisches Bundesamt. 2016. *Ältere Menschen in Deutschland und der EU*. Wiesbaden: Statistisches Bundesamt. <https://www.destatis.de/Migration/DE/Publikationen/Thematisch/Bevoelkerung/Bevoelkerungsstand/BroschuereAeltereMenschen.html>. Zugegriffen am 02.04.2020.
- UN. 2015. *Millenniums-Entwicklungsziele. Bericht 2015*. New York: Vereinte Nationen.
- Wei, Lu, und Douglas B. Hindman. 2011. Does the digital divide matter more? Comparing the effects of new media and old media use on the education-based knowledge gap. *Mass Communication and Society* 14(2): 216–235.



# Digitale Ethik

Göttrik Wewer

## Inhalt

1 Klärung der Begriffe .....	232
2 Konzeptionelle Grundlagen .....	234
3 Praktische Anwendungsfelder .....	235
4 Gesellschaftliche Auswirkungen .....	237
5 Perspektiven für Staat, Verwaltung und Politik .....	239
Literatur .....	240

## Zusammenfassung

Die Grundfragen der Moralphilosophie bleiben im digitalen Zeitalter die gleichen wie vorher, aber ein anderer Kontext, die Digitalisierung aller Lebensbereiche, erfordert womöglich ganz neue Antworten darauf. Eine **Digitale Ethik** soll nicht nur **Auswege aus moralischen Dilemmata** aufzeigen, vor denen Programmierer oder Internetnutzer stehen können, sondern auch **vernünftige Lösungen** für Situationen anbieten, in denen Fahrzeuge autonom funktionieren oder Maschinen miteinander kommunizieren. Da immer und überall auch moralische Fragen beantwortet werden müssen, eröffnet die Digitalisierung aller Lebensbereiche für eine Digitale Ethik nahezu unendliche Anwendungsfelder. Da sie noch in den Anfängen steckt, kann Digitale Ethik noch nicht Antworten auf alle Fragen geben, die durch *Big Data* und *Data Analytics*, Künstliche Intelligenz und maschinelles Lernen aufgeworfen werden. Wie sich die moralischen Maximen, an deren wir uns orientieren, und die sozialen Normen, was wir von anderen erwarten, aber auch die gesetzlichen Regelungen entwickeln, die daraus abgeleitet werden, ist noch offen.

---

G. Wewer (✉)

Lorenz-von-Stein-Institut für Verwaltungswissenschaften an der Christian-Albrechts-Universität zu Kiel, Kiel, Deutschland

E-Mail: [g.wewer@bvdp.de](mailto:g.wewer@bvdp.de)

## Schlüsselwörter

Moralphilosophie · Technikethik · Maschinenethik · Internetethik · **Hackerethik**

### 1 Klärung der Begriffe

Ethik ist eine Subdisziplin der *Philosophie*, die sich mit den moralischen Grundlagen menschlichen Handelns befasst. Eine Digitale Ethik (oder Digitalethik) wiederum ist jener Ausschnitt einer allgemeinen Moralphilosophie, der speziell die moralischen Fragen beleuchtet, die sich aus der umfassenden Datenverarbeitung unserer Tage ergeben. Sie versucht, moralische Dilemmata aufzuzeigen, die sich aus der Digitalisierung aller Lebensbereiche ergeben können, und Grundregeln zu entwickeln, wie man vernünftig damit umgehen kann. Ethik ist also die Disziplin, die solche Fragen zu beantworten versucht, *Moral* ihr Gegenstand.

Moral, Ethos oder Sitten einer Person, einer Gruppe oder einer Gesellschaft kann man (deskriptiv) beschreiben, also zeigen, wie diese faktisch handeln oder welches Verhalten in bestimmten Situationen allgemein erwartet wird, aber auch anhand ethischer Maximen als moralisch gut oder moralisch schlecht (normativ) bewerten, also erklären, welches Handeln aus welchen Gründen jeweils als vernünftig gelten kann. Auf einer Metaebene untersucht die Ethik die vielfältigen Voraussetzungen und logischen Konsequenzen moralischen Denkens, Sprechens und Handelns. Moralisches Handeln ist menschliches Handeln, da Tiere oder Maschinen kein hinreichendes Reflexionsvermögen besitzen, sondern ihren Instinkten folgen oder nach den Regeln funktionieren, die ihnen einprogrammiert worden sind.

Wirtschaftsethik, Technikethik, *Computerethik*, Informationsethik und ähnliche Arbeitsfelder der Philosophie gibt es schon seit längerer Zeit, während eine Digitale Ethik noch ein relativ neues Gebiet darstellt, das sich erst im digitalen Zeitalter entwickeln konnte. Der Beginn dieses Zeitalters wird für gewöhnlich auf das Jahr 2002 datiert, als erstmals in der Geschichte der Menschheit mehr Informationen digital gespeichert wurden als analog. Rafael Capurro zum Beispiel, einer der Pioniere auf diesem Gebiet, verwendet diesen Begriff nach eigenen Angaben seit 2009, also seit etwa zehn Jahren; sein Institut für Digitale Ethik an der Stuttgarter Hochschule für Medien hat 2014 die Arbeit aufgenommen (Capurro 2017, S. 11). Capurro ist außerdem Gründer des *International Center for Information Ethics* (ICIE), das 1999 aus der Taufe gehoben wurde, und Herausgeber der *International Review of Information Ethics* (IRIE), die seit 2004 erscheint, was darauf hindeutet, dass die Digitale Ethik ein noch sehr junger Zweig des philosophischen Nachdenkens ist, jedoch mit Wurzeln, die bis in die Antike zurückreichen. Digitale Ethik versteht Capurro im Sinne einer „kritischen Reflexion über das gute Leben in einer von der Digitalisierung geprägten Welt“ (Capurro 2017, S. 11). Manche sehen in Digitaler Ethik auch eine Erweiterung der allgemeinen Medienethik.

Wenn früher von **Computerethik** gesprochen wurde, dann meinte man nicht, dass Rechner moralisch handeln sollten, sondern meist eine Berufsethik für Informatiker, die nicht nur professionell arbeiten, sondern sich auch der gesellschaftlichen Auswirkungen dessen, was sie schufen, bewusst werden sollten. In diesem Sinne verabschiedete die deutsche Gesellschaft für Informatik (GI) 1994 „Ethische Leitlinien“ für ihre Mitglieder, die zehn Jahre später neu gefasst wurden. 2003 gründete sie eine Fachgruppe „Informatik und Ethik“, die sich kontinuierlich mit der moralischen Verantwortung der Profession beschäftigen soll. Dabei geht es um die Arbeit der Informatiker, die Nutzer ihrer Produkte und die Konstruktion der Systeme (*ethics by design*).

Hackerethik Wenn von **Internetethik** die Rede ist, dann geht es meist um Spielregeln, wie wir uns im Netz verhalten sollten („Netiquette“). Unter dem Stichwort „**Hackerethik**“ kursieren verschiedene Versionen von Prinzipien, an die sich möglichst alle halten sollen, die mit mehr oder minder guten Absichten in die Systeme anderer eindringen. Dazu gehört, Autoritäten zu misstrauen, Informationen allgemein verfügbar zu machen und das eigene Wissen zu teilen, etwa über Schwachstellen in einer Software. Nachdem einige Mitglieder den russischen Geheimdienst unterstützt hatten, entwickelte der Chaos Computer Club (CCC) eine eigene Version, die unter anderem die Punkte „mülle nicht in den Daten anderer Leute“ und „öffentliche Daten nützen, private Daten schützen“ enthielt ([www.ccc.de](http://www.ccc.de)). Das Einhalten solcher Grundsätze kann nicht erzwungen werden, sondern nur freiwillig erfolgen. Hacker, die dagegen verstößen, können aber in der Szene geächtet werden.

Wie in allen Disziplinen gibt es auch in der angewandten Ethik unterschiedliche Grundverständnisse, Ansätze und Konzepte, also nicht „die“ eine **Digitale Ethik**, über die sich alle einig sind. Eine grundlegende Unterscheidung, die auch in der praktischen Politik eine wichtige Rolle spielt, ist die zwischen *Gesinnungsethik* und *Verantwortungsethik*, die Max Weber in seinem Vortrag „Politik als Beruf“ 1919 entwickelt hat. Verantwortung übernimmt, wer sein Handeln an den Folgen ausrichtet, die es voraussichtlich auslöst, ungeachtet der Mittel, die dabei womöglich eingesetzt werden müssen. Gesinnung zeigt, wer nach bestimmten Prinzipien handelt, die als gut und richtig angesehen werden, unabhängig davon, was dieses Handeln womöglich bewirkt. Ähnlich gehen deontologische Handlungstheorien (von griech. *to deon* = die Pflicht) davon aus, dass man etwas tun soll, weil es „an sich“ richtig ist, und nicht etwa (nur), um ein bestimmtes Ziel zu erreichen, während konsequentialistische Handlungsanleitungen stets von den Folgen ausgehen, die eine bestimmte Handlung haben könnte. Zweckmäßig oder zielgerichtet handeln bedeutet, vom Ergebnis her zu denken. Da es oft nicht möglich ist, Lösungen zu finden, von denen alle profitieren, besagt eines der Prinzipien, sich am „größten Glück der größten Zahl“ (Jeremy Bentham) zu orientieren, also die Alternative zu wählen, die den meisten nützt (Utilitarismus). Die *Tugendethik* wiederum fragt allgemein danach, wie sich ein „guter Mensch“ in einer bestimmten Situation verhalten würde.

Der Rolle von Wissenschaft, Forschung und Entwicklung bei der Gestaltung technischer oder sozio-technischer Systeme widmen sich *Science and Technology Studies* (STS) bzw. eine spezielle *Techniksoziologie*, die ebenfalls normative Grundsätze für die handelnden Personen, Organisationen und Institutionen anbietet, ohne sich explizit als Ethik zu verstehen.

## 2 Konzeptionelle Grundlagen

Die **Fragen**, die eine Digitale Ethik zu beantworten hat, sind im Grunde **nicht neu** und die **moralischen Dilemmata**, die von ihr diskutiert werden, **unterscheiden sich nicht prinzipiell** von denen, die in der Ethik allgemein verhandelt werden. Zu klären ist aber, ob die **Antworten**, auf die man sich bisher verständigt hatte, für moralisches Handeln im digitalen Zeitalter **noch genügen**. Wenn sich durch die digitale Revolution der Kontext menschlichen Handelns radikal verändert, müssen womöglich auch neue Antworten auf alte Fragen gefunden werden. Methodisch und theoretisch unterscheidet sich die Digitale Ethik nicht von der allgemeinen Philosophie, wenn man davon absieht, dass *Data Science*, also die Forschung mit großen Datenmengen, auch dort allmählich einzieht.

Relativ neu ist, dass moralische Fragen nicht mehr nur bezogen allein auf menschliches Handeln verhandelt werden, sondern auch auf das Funktionieren von Maschinen. Daraus ist die neue Disziplin der *Maschinenethic* entstanden (Anderson und Anderson 2011; Bendel 2018), die als ein Zweig der Digitalen Ethik verstanden werden kann. **Lassen sich „moralische Maschinen“ konstruieren, die selbstständig zwischen richtig und falsch unterscheiden können**, indem sie menschliche Moralvorstellungen simulieren (Wallach und Allen 2009)?

Zwar werden *Software*, Maschinen und Roboter überwiegend noch von Menschen programmiert, aber wenn sie dank Künstlicher Intelligenz eigenständig „lernen“, je mehr Daten sie verarbeiten, dann werden sie **selbst zu „moralischen Agenten“**, weil sie nicht nur Steuerungsbefehle ausführen, die ihnen vorgegeben wurden, sondern womöglich Entscheidungen treffen, die ihre Schöpfer nicht vorhergesehen haben. Man muss nicht gleich befürchten, dass irgendwann die Maschinen die Menschen beherrschen, aber je autonomer diese Systeme arbeiten, desto dringender ist zu klären, **wer die Ergebnisse dieser Entscheidungen eigentlich verantwortet**: Der Roboter? Der Betreiber des Systems? Der Verkäufer? Oder der Programmierer?

Die Fragen, mit denen sich die Digitale Ethik beschäftigt, werden nicht einfacher, da es längst nicht mehr darum geht, ob *entweder* der Mensch *oder* die Maschine moralisch verantwortlich ist. In Mensch-Maschine-Systemen wirken beide zusammen, ohne dass immer eindeutig zu sagen wäre, wer an einem bestimmten Punkt was entschieden hat. Hätte der Mensch überhaupt erkennen können, dass etwas moralisch Fragwürdiges geschieht, und hätte er tatsächlich eingreifen können, um das zu verhindern? Hier geht es um Grundfragen von Autonomie und Freiheit.

Noch komplexer und komplizierter werden moralische Fragen, wenn Maschinen untereinander kommunizieren, um zum Beispiel eine Produktion zu steuern, **ohne dass Menschen noch unmittelbar beteiligt** sind, die „Entscheidungen“ dieser Maschinen aber nicht nur zu Fehlern führen, sondern auch Menschen schädigen können. Maschinen haben keine Moral; sie folgen stur den Regeln, die ihnen vorgegeben sind.

Die konzeptionellen Überlegungen, wie wir mit diesen Phänomenen umgehen sollen, stehen noch ganz am Anfang. Es gibt weder ein Lehrbuch der Digitalen Ethik, das alle Fragen mustergültig beantworten würde, noch ein Handbuch der Digitalen Ethik, das für Interessierte den Stand der Forschung umfassend aufbereiten

würde. Derzeit gibt es vor allem eine Fülle von Fragen, zu denen täglich neue hinzukommen, aber noch kaum Antworten, die als verbindlich angesehen werden könnten. Die moralischen Grundsätze, an denen wir uns im analogen Zeitalter orientiert haben, werden nicht obsolet, aber was sie in bestimmten Konstellationen heute bedeuten, ist nicht immer klar zu sagen. Erste Antworten reichen von Spielregeln, wie man sich im Internet verhalten sollte („Netiquette“), bis hin zu Entwürfen für einen „digitalen Kodex“ oder eine „Digitale Charta“, die Grundrechte oder Grundregeln definieren sollten, an die sich möglichst alle halten sollten, ohne dazu gesetzlich verpflichtet zu sein.

Wichtig ist die Erkenntnis, dass niemand den moralischen Dilemmata, die durch den ubiquitären Umgang mit Daten entstehen, ausweichen kann. Moralisch richtig oder falsch kann sich auch verhalten, wer in einer bestimmten Situation nichts macht. Unterstütze ich das Geschäftsmodell von *Amazon*, indem ich diese Plattform nutze, oder greife ich bewusst nicht darauf zurück, obwohl das vielleicht unbequemer ist und mehr kostet? Viele nutzen die sogenannten Sozialen Medien, obwohl sie ihnen nicht vertrauen, nur weil das alle machen und man dort präsent sein möchte. Das sind nur einige Beispiele dafür, warum eine Ethik für das digitale Zeitalter so wichtig ist. Mit der Berufung einer Datenethikkommission im Sommer 2018 hat die Bundesregierung signalisiert, dass sie die Bedeutung dieses Themas verstanden hat. In einigen Ländern (wie Hessen) gibt es ähnliche Gremien.

---

### 3 Praktische Anwendungsfelder

Wo es um Leben und Tod geht, treten immer auch moralische Fragen auf, die nur schwer zu beantworten sind. Deshalb hat beispielsweise die Bundesärztekammer 1994 beschlossen, eine Zentrale Kommission zur Wahrung ethischer Grundsätze in der Medizin und ihren Grenzgebieten („Zentrale Ethikkommission“) einzurichten, die seither zahlreiche Stellungnahmen herausgegeben hat, an denen sich Ärzte und Forscher orientieren können ([www.zentrale-ethikkommission.de](http://www.zentrale-ethikkommission.de)). Schon 1999 hat diese Kommission eine Stellungnahme zur „Verwendung patientenbezogener Daten für die Forschung“ vorgelegt, später etwa Leitlinien zur „Altersschätzung bei unbegleiteten Flüchtlingen“ (2016). Der Deutsche Ethikrat, 2001 als Nationaler Ethikrat gegründet und 2007 gesetzlich verankert, der Regierung, Parlament und Öffentlichkeit in bioethischen Fragen (in den sogenannten Lebenswissenschaften) beraten soll ([www.ethikrat.org](http://www.ethikrat.org)), hat unter anderem 2017 ein Positionspapier zu „Big Data und Gesundheit“ vorgelegt (Deutscher Ethikrat 2017).

Ähnlich einer Berufsethik für Programmierer sollen Ethikkommissionen an Hochschulen dafür sorgen, dass die Grundsätze guten wissenschaftlichen Arbeitens eingehalten werden, nicht nur, aber auch beim Umgang mit Daten. Für Ingenieure hat das *Institute of Electrical and Electronics Engineers* (IEEE), ein weltweiter Berufsverband, 2017 „Ethically Aligned Design“ erarbeitet: „A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems“ ([www.ieee.org](http://www.ieee.org)).

Auch der Staat lässt sich bei schwierigen Fragen, die kontrovers diskutiert werden, gerne von solchen Kommissionen beraten. Beispiele dafür sind die Ethikkommission für eine sichere Energieversorgung, die nach der Katastrophe von

Fukushima Vorschläge erarbeiten sollte, wie ein Atomausstieg in Deutschland gelingen könnte, oder auch die Ethikkommission „Automatisiertes und Vernetztes Fahren“, die das Bundesministerium für Verkehr und digitale Infrastruktur berufen hatte, um hier Leitlinien zu entwickeln. Zu den zwanzig Thesen, die diese Kommission formuliert hat, gehört die Regel, dass in gefährlichen Situationen der Schutz des Menschen höchste Priorität besitze gegenüber Tier- oder Sachschäden. Und: „Die Zulassung von automatisierten Systemen ist nur vertretbar, wenn sie im Vergleich zu menschlichen Fahrleistungen zumindest eine Verminderung von Schäden im Sinne einer positiven Risikobilanz verspricht“ (BMVI 2017, S. 10–11).

Da es heute kaum noch einen Bereich gibt, in dem Daten keine Rolle spielen, ist das Gebiet, um das sie sich kümmern soll, nahezu unbegrenzt. Anders gesagt: Digitale Ethik ist die Ethik des digitalen Zeitalters. Überall gefordert zu sein, und das bei einer rasanten technischen Entwicklung, erschwert aber auch den Überblick und die Synthese. Zudem ist durchaus strittig, ob Deutschland (oder Europa oder die Welt) überhaupt so etwas wie einen Digitalen Kodex braucht, also soziale Normen oder moralische Grundsätze für das digitale Zeitalter, die unsere rechtlichen Regeln ergänzen und stützen (DIVSI 2014). Der *European Data Protection Supervisor* zumindest ist, wie er in seiner Strategie für die Jahre 2015 bis 2019 betont hat, davon überzeugt, dass ein gesetzlicher Schutz der Privatsphäre allein nicht hinreicht, und hat deshalb eine *Ethics Advisory Group* gegründet: Bei vielen Themen, die mit Ethik zu tun hätten, ginge es auch um personen-bezogene Daten; die Aufsichtsbehörden seien häufig mit ethischen Fragen konfrontiert, die sich allein durch rechtliche Analyse nicht beantworten ließen ([www.edps.europa.eu](http://www.edps.europa.eu)).

Besonders gefordert ist eine Digitale Ethik auf allen Feldern, auf denen mit Algorithmen, Künstlicher Intelligenz, maschinellem Lernen (*Deep Learning*), Robotern und Maschine-Mensch-Systemen gearbeitet wird. Die Kategorien, an denen sie sich orientiert, sind immer die gleichen: Menschenwürde, Selbstbestimmung, Gleichbehandlung, Gerechtigkeit, Billigkeit (Fairness). Diese Wertekategorien bilden die Grundlage, auf der eine Digitale Ethik Leitlinien zu formulieren versucht für die Bewertung von Problemen einer datenbasierten Gesellschaftsentwicklung.

Es mag das Leben erleichtern, wenn wir „intelligente Assistenten“ durch Sprache steuern können, uns im Alltag zu helfen. Wenn diese Assistenten aber alles aufzeichnen, was wir sagen und tun, und diese Daten dann irgendwo in einer *Cloud* speichern, wo sie von Firmen genutzt werden können, ohne dass wir wissen wofür, dann stellen sich die Menschen praktisch einen Spion ins Wohnzimmer, für den sie auch noch Geld bezahlt haben. In welcher Form wäre ein *Smart Home*, obwohl es über kurz oder lang gläserne Bewohner schafft, moralisch noch zu rechtfertigen?

Während in deutschen Verwaltungen noch keine Roboter gesichtet wurden, sind sie aus Unternehmen nicht mehr wegzudenken. Das gilt nicht nur für die industrielle Fertigung („Industrie 4.0“), sondern auch in der Lagerhaltung und in der Logistik. Roboter kann man einsetzen, das Zimmer zu saugen oder den Rasen zu mähen, aber auch, um Touristen zu betreuen oder Menschen zu pflegen. Schwierig wird es immer dann, wenn beispielsweise Pflegeroboter nicht nur das tun, was man ihnen sagt, sondern auch gegen den Willen der Pflegeperson etwas an eine andere Stelle meldet.

Algorithmen spielen nicht nur beim *Predictive Policing* eine Rolle, sondern werden in amerikanischen Gefängnissen auch für Prognosen genutzt, ob Straftäter

rückfällig werden, also nicht entlassen werden sollten. Da es perfekte Systeme nicht gibt, sind diese Programme anfällig für Fehler, für Vorurteile, die in ihre Regeln eingeflossen sind, für Ungleichbehandlung und Diskriminierung. Auch Menschen, die über eine große Erfahrung verfügen, haben Vorurteile und machen Fehler. Wenn Software diese Fehler nicht potenzieren soll, dann müssen die Algorithmen transparent und ihre Ergebnisse überprüfbar sein. Nur dann lassen sich Fehler korrigieren. Wenn bekannt ist, wie das Programm arbeitet, haben es allerdings auch Straftäter leichter, sich so zu verhalten, dass sie eine günstige Prognose bekommen. Ähnliche Fragen stellen sich bei Gesichtserkennung, Videoüberwachung und anderen Instrumenten, die unsere Sicherheit erhöhen sollen, aber unsere Freiheit einschränken können.

Die österreichische Arbeitsverwaltung konzentriert sich auf Arbeitssuchende, die nach einem Algorithmus die größten Chancen haben, wieder Arbeit zu finden. Ist das konsequent und effizient, weil sich dadurch nicht nur die Zahlen verbessern, sondern auch relativ viele Arbeit finden, oder unfair gegenüber denen, deren Daten weniger positiv erscheinen, die aber auch dringend einen Job benötigen? Ist es richtig, mit den einfachen Fällen anzufangen, oder müsste man sich nicht umgekehrt besonders um diejenigen kümmern, die schwerer zu vermitteln sind? Und wie wäre es zu bewerten, wenn der Algorithmus Menschen diskriminiert, die eigentlich relativ einfache Arbeit finden könnten, wenn man sie dabei unterstützt?

Drohnen können dazu genutzt werden, in schwierigem Gelände Pakete zuzustellen, aber auch dazu, Stadionbesucher zu beobachten oder Demonstrationen zu überwachen. Sie können auch eingesetzt werden, um tatsächliche oder vermeintliche Gegner gezielt zu töten. Von da ist es nicht mehr weit bis zu „Killer Robotern“, die menschliche Soldaten in Kriegen ersetzen oder bei Kampfeinsätzen unterstützen. „Intelligente Raketen“, die bewegliche Ziele, auf die sie programmiert worden sind, unbirrt verfolgen, bis sie sie getroffen haben, sind schon länger im Einsatz.

Letztlich geht es aber um mehr als nur um Algorithmen, Roboter und maschinelles Lernen. „Wir brauchen so etwas wie eine Ethik der Digitalisierung“, hat Bundespräsident Frank-Walter Steinmeier 2018 auf dem 21. Bundeskongress des Deutschen Gewerkschaftsbundes (DGB) gesagt, da die technische Entwicklung die nächste große Bewährungsprobe des Sozialstaates markiere. Eine Digitale Ethik sei aber nicht nur wegen der vielen technischen Innovationen notwendig, die im digitalen Zeitalter unser Leben und Arbeiten verändern, sondern noch aus einem anderen Grund: Weil sich Zukunftsangst, wo immer sie vorhanden sei, nicht in Demokratieskepsis verwandeln dürfe ([www.bundespraesident.de](http://www.bundespraesident.de)).

---

## 4 Gesellschaftliche Auswirkungen

Wenn technische Errungenschaften das Leben und den Alltag leichter machen, indem sie uns lästige Tätigkeiten abnehmen, wird das niemand bedauern. Zum moralischen Problem werden „lernende“ Programme und Maschinen erst dann, wenn sie nicht „neutral“ bleiben, sondern Menschen oder Gruppen diskriminieren, also Macht ausüben, sich von menschlicher Einflussnahme emanzipieren, also ein „Eigenleben“ entwickeln, das nicht hilfreich, sondern ärgerlich ist, oder Entschei-

dungen vornehmen, die wir mehrheitlich ablehnen, aber nicht mehr korrigieren können, sie also letztlich die Richtung bestimmen, in der sich die Gesellschaft verändert. Dann hätten wir nicht nur die Kontrolle verloren, sondern auch die Demokratie.

Programme und Maschinen lernen zwar dazu, wenn man ihnen das eingepflanzt hat, aber die Regeln, nach denen das geschieht, sind ihnen – zumindest anfangs – von Menschen vorgegeben worden. Auch „lernende Maschinen“ sind Menschenwerk. Damit sie das bleiben, versucht die Digitale Ethik Prinzipien zu entwickeln, die bei ihrer Konstruktion und im Alltagsbetrieb beachtet werden sollten. Das zentrale Problem des digitalen Kapitalismus sei es, sagen manche, dass einige wenige Reiche darüber befinden, wie ganz viele Arme ihre Haut (ihre Daten) zu Markten tragen müssen. Das ist nicht nur eine politische, sondern auch eine moralische Frage.

Wenn eine Digitale Ethik Antworten auf solche Fragen liefern soll, die etwas bewirken, dann müssten diese Antworten bekannt sein, allgemein überzeugen und überwiegend beachtet werden. Das ist sicherlich (noch?) nicht der Fall. Ob die „Zehn Gebote der Digitalen Ethik“, die für eine Beratungsplattform von Jugendlichen für Jugendliche entwickelt worden sind, daran etwas ändern? „Messe Deinen Wert nicht an Likes und Posts“, lautet das 8. Gebot; „schalte hin und wieder ab und gönne Dir auch mal eine Auszeit“, empfiehlt das 10. Gebot ([www.digitale-ethik.de](http://www.digitale-ethik.de)).

Die Initiative D21 hat eine Dialogreihe „Denkimpulse zur Digitalen Ethik“ gestartet, die das Thema aufbereiten soll. Die Stiftung Datenschutz hat dazu eine Broschüre „Grundlagen der digitalen Ethik – eine normative Orientierung in der vernetzten Welt“ (Stiftung Datenschutz 2017) vorgelegt. Nicht nur Unternehmen haben das Thema für sich entdeckt (Hasselbalch und Tranberg 2016), auch der Bayerische IT-Sicherheitscluster, ein Verein, hat ein „Ethik-Manifest“ formuliert. Da Technologie selbst keine Ethik kennt, müsse man an Leitlinien arbeiten. Mindestens solange in der digitalen Welt keine verlässlichen gesetzlichen Regelungen gelten würden, sollte man sich an moralischen Normen und Werten orientieren. Von Forschern erwartet die Europäische Union, dass heute jedes Förderprojekt Arbeitspakete enthält, die sich mit den ethischen, rechtlichen und sozialen Auswirkungen der jeweils zu entwickelnden Technik beschäftigen. Das Bundesministerium für Bildung und Forschung (BMBF) verfährt ähnlich.

Was diese Aktivitäten, so begrüßenswert sie sind, tatsächlich bewirken im Sinne von *Output, Outcome* und *Impact*, ist unklar. Wer wissen möchte, wie die Deutschen bestimmte digitale Angebote moralisch beurteilen, kann sie befragen, sollte sich damit aber nicht begnügen, sondern beobachten, wie sie sich im Alltag verhalten, weil das häufig im Widerspruch zu dem steht, was sie sagen. Wenn das nichts kostet, bequem ist und einen Mehrwert verspricht, werden gern auch Angebote genutzt, die unter ethischen Gesichtspunkten als anrüchig gelten. Obwohl zum Beispiel viele den sogenannten Sozialen Medien nicht vertrauen, wie Umfragen belegen, nutzen die meisten sie dennoch (*Privacy Paradox*). Die Allgemeinen Geschäftsbedingungen, durch die sich kommerzielle Datensammler jegliche Nutzung der persönlichen Angaben zugestehen lassen, werden in der Regel nicht gelesen, sondern ihnen wird einfach zugestimmt. Wählen kann man ohnehin nicht, nur völlig auf das Angebot verzichten („friß oder stirb“); da kann man sich die Lektüre vieler Seiten, die nicht

einfach zu verstehen sind, auch gleich schenken. Ob moralisches Handeln im digitalen Zeitalter insgesamt besser oder schlechter wird – siehe *Hate Speech* und *Fake News* –, ist eine Frage, die noch nicht hinreichend beantwortet ist. Das gilt auch für die Frage, was eine Digitale Ethik in diesem Kontext bewirken kann.

---

## 5 Perspektiven für Staat, Verwaltung und Politik

Da technologische Entwicklungen in der „Risikogesellschaft“ (Ulrich Beck) immer öfter in moralische Dilemmata führen, sind Politik, Staat und Verwaltung gefordert, die Nutzung von Künstlicher Intelligenz, maschinellem Lernen und Robotern im Interesse des Gemeinwohls zu regulieren, wenn gegen Grundsätze eines „guten Lebens“ verstoßen werden sollte. Eine Digitale Ethik kann solche Normen unterstützen, wenn sie von vielen gelebt wird, aber sie kann moralisches Handeln nicht erzwingen. Wenn es nicht als ethische Pflicht angesehen wird, sich an staatliche Gesetze zu halten, dann laufen diese leer. Maschinen kann man nicht moralisch verpflichten, sondern nur entsprechend programmieren. Ethische Grundsätze können dabei hilfreich sein. Eine Vorsortierung der Opfer nach persönlichen Merkmalen wie Alter oder Geschlecht im Falle eines Unfalls sei zwar unzulässig, lautet eine der zwanzig Thesen jener Kommission, die sich mit dem autonomen Fahren beschäftigt hat, aber eine Voreinstellung des Fahrzeugs, Schäden von Personen generell möglichst gering zu halten, könne durchaus vertreten werden. Dass Menschen intuitiv besser reagieren, ist keineswegs gesagt: In den meisten Fällen dürfte es die klügste Lösung sein, bei einer drohenden Kollision das Auto in die Leitplanke oder an eine Hauswand zu lenken, weil der Fahrer von allen Beteiligten am besten geschützt ist, statt sich zwischen Rentnern, die auf dem Bürgersteig stehen, und Kindern, die daneben spielen, zu entscheiden.

Politik, Staat und Verwaltung sind aber nicht nur gefordert, die Nutzung moderner Technologien nach moralischen Grundsätzen zu regulieren, sondern sie müssen sich auch fragen, wie sie die Möglichkeiten, die diese Technologien eröffnen, selbst ausschöpfen können, um im Interesse der Bürger besser zu werden. Dass die Bundesregierung, eine Landesregierung oder eine Stadtregierung darüber nachdenkt, ist nicht einmal in Ansätzen zu erkennen. Dienstleistungen auch elektronisch anzubieten (*Electronic Government*), ist nicht das Gleiche, wie die Potenziale der Digitalisierung für eine bessere staatliche Aufgabenerledigung zu nutzen.

Wenn in manchen Hotels heute schon Roboter die Gäste begrüßen und einchecken, dann ist zumindest nicht ausgeschlossen, sie auch am Empfang von Behörden einzusetzen. Wenn juristische Stellungnahmen inzwischen von „lernender“ *Software* geschrieben werden (*Legal Tech*), dann spricht nichts dagegen, solche Lösungen auch für amtliche Bescheide zu entwickeln, zumal auch dann ein Sachbearbeiter sich das Produkt immer noch angucken muss. Würde es nicht die Gerichte enorm entlasten, wenn Entwürfe für Urteile dank Künstlicher Intelligenz entstehen? Hätte das Bundesamt für Migration und Flüchtlinge auf dem Höhepunkt der Zuwanderungswelle ein entsprechendes Programm gehabt, dann hätte es Anträge nicht nur wesentlich schneller bescheiden können, sondern vermutlich auch eine geringere Fehlerquote erreicht als bei den hastig angelernten Mitarbeitern. Immerhin verfügt

die Behörde über die technische Möglichkeit, arabische Dialekte automatisiert zu überprüfen, um feststellen zu können, ob ein Antragsteller wirklich aus der Gegend stammt, aus der er geflüchtet sein will.

Wenn Staat und Verwaltung keine eigene Digitalisierungsstrategie entwickeln, dann werden sie noch weiter hinter Wirtschaft und Gesellschaft zurückfallen, als sie das heute schon sind. Was das für ihre Legitimation und Akzeptanz bedeuten könnte (Schallbruch 2018), ist nicht präzise zu benennen. Wenn Staat und Verwaltung jedoch ganz bewusst auf Datenmanagement, Algorithmen, Künstliche Intelligenz, maschinelles Lernen, Robotereinsatz und ähnliches mehr setzen, um besser steuern und um ihre Leistungen steigern zu können, dann müssen sie für sich selbst alle jene moralischen Fragen beantworten, vor denen bisher nur die anderen stehen.

---

## Literatur

- Anderson, Michael, und Susan Leigh Anderson, Hrsg. 2011. *Machine ethics*. Cambridge: Cambridge University Press.
- Bekey, George A., Keith Abney, und Patrick Lin. 2011. *Robot ethics: The ethical and social implications of robotics*. Cambridge: MIT Press.
- Bendel, Oliver. 2018. Überlegungen zur Disziplin der Maschinenethik. *Aus Politik und Zeitgeschichte* 68(6–8): 34–38.
- BMVI, Hrsg. 2017. *Ethik-Kommission Automatisiertes und Vernetztes Fahren. Bericht*. Berlin: Bundesministerium für Verkehr und digitale Infrastruktur. [www.bmvi.de](http://www.bmvi.de).
- Capurro, Rafael. 2017. Digitalisierung als ethische Herausforderung (Interview). In *3TH1CS. Die Ethik der digitalen Zeit*, Hrsg. Philipp Otto und Eike Gräf, 10–17. Berlin: iRights.Media.
- Deutscher Ethikrat. 2017. *Big Data und Gesundheit. Datensouveränität als informationelle Freiheitsgestaltung. Stellungnahme*. Berlin: Deutscher Ethikrat. [www.ethikrat.org](http://www.ethikrat.org).
- DIVSI, Hrsg. 2014. *Braucht Deutschland einen Digitalen Kodex?* Hamburg: Deutsches Institut für Vertrauen und Sicherheit im Internet.
- Eberl, Ulrich. 2018. Was ist Künstliche Intelligenz – was kann sie leisten? *Aus Politik und Zeitgeschichte* 68(6–8): 8–14.
- Floridi, Luciano. 2013. *The ethics of information*. Oxford: University Press.
- Grunwald, Armin, Hrsg. 2013. *Handbuch Technikethik*. Stuttgart: Metzler.
- Grunwald, Armin. 2019. *Der unterlegene Mensch. Die Zukunft der Menschheit im Angesicht von Algorithmen, Künstlicher Intelligenz und Robotern*. München: riva.
- Hasselbalch, Gry, und Pernille Tranberg. 2016. *Data ethics – The new competitive advantage*. Copenhagen: Publishare.
- Nida-Rümelin, Julian, und Nathalie Weidenfeld. 2018. *Digitaler Humanismus. Eine Ethik für das Zeitalter der Künstlichen Intelligenz*, 3. Aufl. München: Piper.
- O’Neil, Cathy. 2016. *Weapons of math destruction: How big data increases inequality and threatens democracy*. New York: Crown.
- Ramge, Thomas. 2018. *Mensch und Maschine. Wie Künstliche Intelligenz und Roboter unser Leben verändern*. Stuttgart: Reclam.
- Schallbruch, Martin. 2018. *Schwacher Staat im Netz. Wie die Digitalisierung den Staat in Frage stellt*. Wiesbaden: Springer VS.
- Stiftung Datenschutz, Hrsg. 2017. *Grundlagen der digitalen Ethik – eine normative Orientierung in der vernetzten Welt*. Leipzig: Stiftung Datenschutz.
- Wallach, Wendell, und Colin Allen. 2009. *Moral machines. Teaching robots right from wrong*. Oxford: Oxford University Press.



---

# Digitale Souveränität

Julia Pohle

## Inhalt

1 Begriffsklärung .....	242
2 Theoretisch-historische Entwicklung .....	243
3 Stand der Debatte in Deutschland .....	245
4 Umsetzungsstand und Auswirkungen .....	249
5 Herausforderungen für Staat und Verwaltung .....	251
Literatur .....	252

---

## Zusammenfassung

Die Forderung nach „digitaler Souveränität“ entspricht dem Wunsch nach Selbstbestimmung im digitalen Zeitalter – des Staates, von Unternehmen und von Bürger\*innen. In der aktuellen Debatte wird der Begriff jedoch meist einseitig ausgelegt und seine verschiedenen Dimensionen – die staatliche, die wirtschaftliche und die individuelle – werden nur unscharf voneinander abgegrenzt. Die Unschärfe des Konzepts und die Unsicherheit über die Aufgaben, die Staat und Verwaltung beim Streben nach digitaler Souveränität übernehmen sollen, verhindern eine kohärente Strategie, wie individuelle, ökonomische und staatliche Selbstbestimmung im digitalen Zeitalter bewahrt werden kann.

---

## Schlüsselwörter

Digitalpolitik · Demokratie · Selbstbestimmung · Vernetzung · Sicherheit

---

J. Pohle (✉)

Politik der Digitalisierung, Wissenschaftszentrum Berlin für Sozialforschung, Berlin, Deutschland  
E-Mail: [julia.pohle@wzb.eu](mailto:julia.pohle@wzb.eu)

## 1 Begriffsklärung

Das Konzept der „digitalen Souveränität“ hat sich in den letzten Jahren zu einem Schlüsselbegriff in der Debatte um die Digitalisierung entwickelt. Spätestens seit 2013 findet es als Kurzformel für das Streben nach mehr Eigenständigkeit und Selbstbestimmung in der digitalen Welt regelmäßig Eingang in Strategie- und Positionspapiere der deutschen Regierungspolitik sowie in Stellungnahmen wirtschaftlicher und gesellschaftlicher Akteure. Jedoch wird das Konzept bisher mit unterschiedlichsten Interpretationen und Assoziationen verknüpft und fast ausschließlich präskriptiv-normativ verwendet. Es drückt damit weniger konkrete Vorhaben als vielmehr die Hoffnung aus, dass Staaten, Organisationen und Individuen die Herausforderungen der stetig an Bedeutung gewinnenden digitalen Vernetzung zu bewältigen vermögen.

Unabhängig von seiner Verwendung im digitalen Kontext bezieht sich der Begriff der Souveränität auf die Fähigkeit, selbstbestimmt und frei von Fremdherrschaft agieren zu können. Aus dem Französischen (*souveraineté*) ins Deutsche gelangt, leitet sich der Souveränitätsbegriff vom lateinischen Wort *superanus* ab, was „darüber befindlich“ oder „überlegen“ bedeutet. Stark geprägt wurde das traditionelle Verständnis von Souveränität im 16. Jahrhundert durch den Staatstheoretiker Jean Bodin und seiner Idee, dass es im Staat dem Herrscher – dem Souverän – obliege, letzte Entscheidungen zu treffen (Letztentscheidungsbefugnis) und das Gewaltmonopol innezuhaben. Im 18. Jahrhundert läutete der Aufklärer Jean-Jacques Rousseau einen radikalen Wandel im Verständnis des Begriffs von der Fürsten- zur Volkssouveränität ein. Einhergehend mit der Entwicklung moderner Demokratien setzte sich die Idee durch, dass das Volk in seiner Gesamtheit Träger der höchsten Staatsgewalt sei, diese jedoch einem Herrscher oder einer gewählten Regierung zur Ausübung überlassen könne.

Formend für ein modernes Verständnis von Souveränität ist zudem die Begriffsauslegung der Rechtswissenschaft, in welcher der Souveränitätsbegriff für die Selbstbestimmungsfähigkeit eines Rechtssubjekts steht. Diese zeichnet sich durch Eigenständigkeit und Unabhängigkeit aus und stellt damit einen Gegensatz zu Fremdbestimmung dar. Im Staats- und Völkerrecht bedeutet Souveränität die Unabhängigkeit eines Staates gegenüber anderen (Souveränität nach außen) sowie die selbstbestimmte staatliche Gestaltung im Inneren (Souveränität nach innen). Souveränität ist somit ein Konzept, das eng mit der Idee des territorial begrenzten Nationalstaates verbunden ist: Ein Staat gilt als souverän, wenn er im Verhältnis zu anderen Staaten politisch, wirtschaftlich und gesellschaftlich weitestgehend unabhängig agieren kann.

In Demokratien ist der Begriff der Souveränität zudem mit dem Prinzip der Rechtsstaatlichkeit verbunden. Die Souveränität eines Staates besteht auch in der Sicherung der Selbstbestimmungsfähigkeit seiner Bürger\*innen mit ihren unveräußerlichen Rechten. Sie dient damit auch dem Zweck, jedem Menschen zu ermöglichen, in seinen persönlichen Rechten respektiert zu werden und eigenverantwortlich zu handeln. Die Rahmenbedingungen dafür zu garantieren wird als Aufgabe des Staates angesehen, nicht zuletzt angesichts der Herausforderungen der Digitalisierung.

Die Spezifizierung „digital“ im Konzept der „digitalen Souveränität“ bezieht sich folglich weniger auf das Adjektiv, das im Gegensatz zu „analog“ die Charakte-

risierung durch den Einsatz von Computertechnologien beschreibt. Vielmehr verweist sie auf den gesamtgesellschaftlichen Transformationsprozess der Digitalisierung, der sich neben der allumfassenden Nutzung von Computertechnologie vor allem durch zwei zusammenhängende Entwicklungen auszeichnet: der Verbreitung und Nutzung digitaler Vernetzungstechnologie und der starken Zunahme von digitalen Datensammlungen und grenzüberschreitenden Datenströmen.

Ein Souveränitätsbegriff, der zu eng mit der Idee eines territorial begrenzten Nationalstaates verbunden ist, erscheint angesichts dieser Entwicklungen in den Augen vieler überholt (Friedrichsen und Bisa 2016). Verstärkt durch die allgemeine Globalisierung führt die zunehmende digitale Vernetzung mit ihren Datenströmen dazu, dass Abhängigkeiten und Verflechtungen der Staaten untereinander ansteigen und Staaten noch weniger als zuvor selbstbestimmt und unabhängig agieren können. Die Digitalisierung wird daher als Herausforderung für die wirtschaftliche, politische und rechtliche Selbstbestimmung von Nationalstaaten, aber auch für die ihrer Bürger\*innen angesehen.

Der Ruf nach digitaler Souveränität lässt sich auf dieser Grundlage als Wunsch nach mehr Handlungs- und Gestaltungsfreiheit verstehen, um den Prozess der digitalen Transformation mitzugestalten und im digitalen Raum selbstbestimmt handeln zu können. Eine solche Idee von digitaler Souveränität lässt sich nicht nur auf den Staat beziehen, sondern auch auf einzelne Bürger\*innen oder Unternehmen. Daher verstehen manche unter digitaler Souveränität auch schlicht die Fähigkeit von Individuen sowie von staatlichen oder wirtschaftlichen Institutionen, selbstbestimmt digitale Technologien zu nutzen und ihre jeweiligen Rollen in Zeiten der Digitalisierung selbstständig und sicher ausüben zu können.

---

## 2 Theoretisch-historische Entwicklung

Die Frage, wie sich nationalstaatliche Souveränität und digitale Vernetzungstechnologien gegenüberstehen, ist nicht neu. Der Technikwissenschaftler Milton Mueller bemerkt einen radikalen Wandel der Verwendung des Souveränitätsbegriffs in Bezug auf den digitalen Raum in den letzten drei Jahrzehnten: von der Auffassung, der *Cyberspace* selbst sei souverän und solle von staatlichem Einfluss unabhängig bleiben, hin zu der Forderung, das Internet und seine digitalen Angebote seien der Logik territorialer Staatlichkeit und Entscheidungsbefugnis unterzuordnen (Mueller 2015, S. 68).

Tatsächlich unterstellten viele Studien bis weit in die 1990er-Jahre eine Inkompatibilität zwischen der Idee der nationalstaatlichen Souveränität und dem Internet als zunehmend dominanter Vernetzungstechnologie. Vertreter\*innen des sogenannten „Cyber-Exzptionalismus“ sahen das Internet als neuartigen virtuellen Raum an, der als einzigartig und unregulierbar galt. Herkömmliche Herrschaftsformen und staatliche Regulierung hätten dort keinen Platz und würden die quasi-evolutionäre Entwicklung des Internets nur stören (Misterek 2017, S. 5). Unter Bezugnahme auf die technische Architektur des Internets, die eine dezentrale und nicht-hierarchische Ordnungsform darstellt, forderten sie, den virtuellen Raum als eigenständiges Hoheitsgebiet der Internetgemeinde zu behandeln (Hofmann 2005, S. 16). Die Ablehnung

staatlicher Regulierung beruhte darüber hinaus auf der Neuheit, dass im Internet alle Datenflüsse grenzüberschreitend stattfinden und fortwährend viele verschiedene Rechtsräume durchlaufen. Aufgrund der vielfältigen Möglichkeiten, Datenverbindungen herzustellen, wurde der virtuelle Raum als frei von zentralen Eingriffs- oder Regulationsmöglichkeiten und weitgehend als vom geografischen Raum unabhängig angesehen. Folglich unterliege er keiner nationalstaatlichen Souveränität und Rechts-hoheit im herkömmlichen Sinne.

Um die Jahrtausendwende verstärkte sich weltweit die Auffassung, dass angesichts der zunehmenden weltweiten Vernetzung Ordnungsbildung und Koordination nötig seien. Gemeinsame Normen, Regeln und Prozeduren zur Gestaltung des Internets sollten jedoch weiterhin mit möglichst geringer staatlicher Einmischung entwickelt werden, da national unterschiedliche Zielvorstellungen der Weiterentwicklung des globalen Phänomens Internet nur im Wege ständen. Unter dem Oberbegriff „*Internet Governance*“ setzte sich die Ansicht durch, dass diese Koordinationsaufgabe vielmehr in die Hand einer internationalen *Multistakeholder*-Gemeinschaft aus privaten Akteur\*innen und technischen Eliten zu legen sei (Hofmann 2005, Thiel 2014, S. 223). Bis heute hält sich bei vielen die Meinung, dass sich das Internet nicht national einhegen lasse, da ein größerer Einfluss souveräner Staaten aufgrund ihrer konkurrierenden Interessen zur Fragmentierung des Internets entlang nationaler Grenzen und Rechtsräume führe (Mueller 2015). Daher, so diese Ansicht, könne das Internet – wenn überhaupt – nur durch globale Abstimmung im *Multistakeholder*-Verfahren koordiniert werden.

Trotz dieser allgemeinen Skepsis gegenüber staatlicher Einmischung werden seit Mitte der 2000er-Jahre vermehrt die Beziehungen zwischen digitalen Technologien, wirtschaftlichen Dynamiken und politischen Interessen souveräner Staaten in den Blick genommen. Die digitale Vernetzung wird dabei weiterhin als Herausforderung, jedoch nicht mehr unbedingt als Hindernis nationalstaatlicher Souveränitätsausübung wahrgenommen (Thiel 2014, S. 233 f.). Vielmehr wird anerkannt, dass bestimmte Formen staatlicher Regulierung nicht nur geeignete Mittel zur Regulierung, Rechtsetzung und Ordnungsbildung in Bezug auf digitale Kommunikation und Informationsflüsse darstellen können, sondern auch schon seit längerem stattfinden und somit die Entwicklung des Internets und seiner Dienste beeinflussen. Grund für diesen Perspektivenwechsel ist nicht zuletzt die zunehmende Kritik an mangelnden demokratischen Werten in der Regelsetzung durch den freien Markt und in Entscheidungsprozessen, die von Expert\*innen dominiert werden, sowie eine Rückbesinnung auf Normensetzung von durch Volkssouveränität legitimierten Institutionen.

Das zunehmende regulierende Eingreifen von Staaten zeigt, dass der oft vorhergesagte Bedeutungsverlust nationaler Grenzen aufgrund von digitaler Vernetzung nicht eingetreten ist. Obwohl sich die Anwendungsschicht des Internets nicht immer lokalisieren lässt, ist die digitale Infrastruktur dennoch stark in der physischen Realität verankert. Ihre Nutzer\*innen sind stets einem konkreten geografischen Standort zuzuordnen (Misterek 2017, S. 15). Sowohl autoritäre als auch demokratische Staaten nutzen diesen Umstand zur Überwachung und Zensur des Kommunikations- und Datenaustauschs, z. B. um Diffamierungen und regierungskritische Stimmen zu unterdrücken oder um geistiges Eigentum zu schützen. Gleichzeitig versuchen einige Staaten verstärkt zu regeln, wie Unternehmen und ausländische

Geheimdienste digitale Daten sammeln, analysieren und weitergeben können. Entsprechende Maßnahmen gelten jedoch stets nur für Nutzer\*innen und Anbieter digitaler Dienste und Technologien im jeweiligen Land. Daher lassen sich zunehmend verschiedene Teilräume im digitalen Raum unterscheiden, in denen unterschiedliche Rechtsnormen gelten und mit unterschiedlichem Erfolg durchgesetzt werden, z. B. zum Schutz von Persönlichkeitsrechten oder der freien Meinungsäußerung (Misterek 2017, S. 14).

Der Begriff Souveränität hat in Bezug auf die Digitalisierung seit den Enthüllungen des ehemaligen CIA-Mitarbeiters Edward Snowden im Sommer 2013 über die massenhaften Überwachungstätigkeiten ausländischer Geheimdienste neu an Konjunktur gewonnen (Schaar 2015). Als Reaktion auf die gefühlte digitale Übermacht US-amerikanischer Geheimdienste und Technologiekonzerne forderten Politiker\*innen und gesellschaftliche Akteur\*innen unter anderem in Deutschland, Frankreich und auf europäischer Ebene, die Souveränität der europäischen Staaten im digitalen Raum zu stärken. Im Gegensatz zu Russland und China, die unter dem Schlagwort der „Cyber-Souveränität“ eine rein national- und zwischenstaatliche Kontrolle und Regulierung des Internets fordern, lässt sich in der aktuellen Diskussion in Deutschland derweil eine Abkehr vom traditionellen Verständnis des Souveränitätsbegriffs feststellen. Digitale Souveränität (auch „technische Souveränität“) wird als die Voraussetzung dargestellt, den Prozess der digitalen Transformation mitgestalten und im digitalen Raum selbstbestimmt handeln zu können, ohne dabei auf die Nutzung von Technologien und Anbietern im Ausland verzichten zu müssen. Dabei wird häufig nicht nur die Souveränität des demokratischen Staates betont, sondern auch die der Bürger\*innen als individuelle Nutzer\*innen bzw. als Konsument\*innen digitaler Dienste.

In den Mittelpunkt rückt folglich nicht nur die kollektive Souveränität als Handlungs- und Gestaltungsfähigkeit des Staates und der Wirtschaft, sondern auch die individuelle Souveränität, verstanden als die Autonomie und selbstbestimmte Handlungsfähigkeit des Individuums in einer vernetzten Welt. Diese wird oft auch als „digitale Selbstbestimmung“ bezeichnet und mit den Konzepten der „Datensouveränität“ und der „informationellen Selbstbestimmung“ in Verbindung gebracht (Mertz et al. 2016). Obwohl sich die staatliche, wirtschaftliche und individuelle Dimension digitaler Souveränität in vielerlei Hinsicht wechselseitig bedingen und teilweise überlappen, hat die Verwirklichung digitaler Selbstbestimmung von Individuen und Unternehmen andere Voraussetzungen als die eines Staates. Sie zu schaffen und zu bewahren, stellt Staat und Verwaltung damit auch vor andere Herausforderungen.

---

### 3 Stand der Debatte in Deutschland

In der aktuellen Debatte in Deutschland (Stand März 2019) werden die staatliche, wirtschaftliche und individuelle Ebene von digitaler Souveränität sowie die jeweils damit verbundenen Aufgaben für Staat und Verwaltung nicht deutlich voneinander abgegrenzt. Zudem wird das Schlagwort der digitalen Souveränität vorrangig präskriptiv-normativ verwendet, indem zumeist Handlungsempfehlungen formuliert und seltener existierende Aufgabenfelder benannt werden.

### 3.1 Staatliche Dimension

In der Diskussion um die digitale Souveränität des Staates Deutschland dominieren sicherheitspolitische Aufgaben. Unter dem Einfluss der öffentlichen Reaktion auf die Snowden-Enthüllung kündigte der Koalitionsvertrag zwischen CDU, CSU und SPD im Dezember 2013 verschiedene Maßnahmen zur Rückgewinnung der technologischen Souveränität an. Diese sollten in der Förderung vertrauenswürdiger IT-Produkte und des Einsatzes nationaler IT-Sicherheitstechnologien bestehen. Gleichzeitig stellte die damalige Bundesregierung weitere technische Möglichkeiten der Überwachungsabwehr in Aussicht, wie den Ausbau der Kapazitäten zur Cyberabwehr des Bundesamts für Sicherheit in der Informationstechnik (BSI). Ein ähnlicher Maßnahmenkatalog zum Ausbau sicherheitspolitischer Kompetenzen findet sich in der „Digitalen Agenda 2014–2017“, mit der die Regierungskoalition die Grundsätze ihrer Digitalpolitik formulierte und für deren Umsetzung das Innen-, das Wirtschafts- und das Verkehrsressort gemeinsam Verantwortung zeichneten, und im Koalitionsvertrag von CDU, CSU und SPD aus dem März 2018. Letzterer sieht unter anderem die Einrichtung einer Innovationsagentur und eines IT-Sicherheitsfonds zum Schutz sicherheitsrelevanter Schlüsseltechnologien vor.

Das von der Bundesregierung geplante Aufgabenspektrum zur Sicherung der digitalen Souveränität des eigenen Staates ist somit größtenteils technischer Natur und bezieht sich auf den Schutz der digitalen Infrastruktur und der technischen Stärkung des Datenschutzes im digitalen Raum in Deutschland und Europa, z. B. durch eine umfassendere Verschlüsselung von Kommunikationsflüssen und die verpflichtende Speicherung von Daten auf europäischem Boden. Das skizzierte Handlungsrepertoire umfasst dennoch nicht-technische Aufgaben wie die aktualisierten Bedingungen für den Kauf von *Software* durch öffentliche Stellen oder die effiziente Umsetzung der Europäischen Datenschutzgrundverordnung (DSGVO).

Entsprechend ihrer sicherheitspolitischen Ausrichtung liegt die Verantwortlichkeit für die meisten der Maßnahmen zur staatlichen Souveränitätssicherung beim Bundesministerium des Innern (BMI) und zunehmend auch beim Bundesministerium der Verteidigung (BMVg). Das Innenministerium war unter anderem federführend für die Ausarbeitung des „Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme“ (kurz: IT-Sicherheitsgesetz), das 2015 in Kraft getreten ist und die Betreiber kritischer Infrastrukturen wie Energie, Wasser, Gesundheit oder Telekommunikation verpflichtet, die IT-Sicherheit ihrer Netze zu erhöhen. Praktische Unterstützung erhält das Innenministerium zudem vom BSI, dessen Aufgabe die präventive Förderung der Informations- und Cybersicherheit in Staat, Wirtschaft und Gesellschaft ist.

### 3.2 Wirtschaftliche Dimension

Sicherheitspolitische Aufgaben der Souveränitätssicherung Deutschlands haben oft einen wirtschaftlichen Bezug, da sie einerseits die IT-Infrastruktur und die Daten deutscher Unternehmen schützen und andererseits die Wettbewerbsfähigkeit und techni-

sche Unabhängigkeit des Wirtschafts- und Technologiestandorts Deutschlands fördern sollen. Darauf hinaus werden seit 2013 explizit wirtschaftspolitische Maßnahmen diskutiert, die der gefühlten Abhängigkeit von US-amerikanischen Digitalunternehmen und der mangelnden Innovationsfähigkeit Deutschlands und Europas entgegenwirken sollen. Entsprechend bezeichnete das Bundesministerium für Wirtschaft und Energie (BMWi) die Sicherung digitaler Souveränität als die Herausforderung, in „allen wichtigen Bereichen der digitalen Ökonomie [...] Standards zu setzen, Marktführerschaft zu erreichen [...]“ und gleichzeitig „die soziale Marktwirtschaft sowie die Entscheidungsgewalt des Verbrauchers über seine Daten zu schützen“ (BMWi 2015a).

Im Positionspapier „Leitplanken Digitaler Souveränität“ übersetzte eine Fokusgruppe des Nationalen IT-Gipfels diese Sicht in konkrete wirtschaftsstrategische Handlungsempfehlungen. Neben leistungsfähiger und sicherer Infrastruktur beziehen sich die Maßnahmen vor allem auf den Aufbau von Schlüsselkompetenzen und -technologien in den Bereichen der *Software*- und *Hardware*-Entwicklung, der *Cybersecurity* von *Big Data* und *Smart Data* sowie *Cloud*-Diensten. Ergänzend sollte Deutschland durch Innovationsförderung und den digitalen Binnenmarkt in Europa einen kompetitiven Wirtschafts- und innovativen Gestaltungsräum schaffen, der nicht von den Risiken technologischer Entwicklungen, sondern von ihren Chancen dominiert werde (BMWi 2015b, S. 5). Verschiedene Wirtschaftsverbände haben ähnliche Handlungsempfehlungen formuliert, wie beispielsweise der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM), der zudem fordert, die Gründung von *Start-ups* im IT-Bereich zu erleichtern (BITKOM 2015, S. 16).

Viele der genannten Handlungsempfehlungen hat das Ministerium 2016 in seine „Digitale Strategie 2025“ aufgenommen. Danach sei es Teil des digitalpolitischen Aufgabenspektrums des Wirtschaftsministeriums, die Datensicherheit und die „Datensouveränität“ nachhaltig und effektiv zu stärken; letzteres bedeute, dass „Daten gegen Missbrauch geschützt sind [und] Nutzer und Verbraucher [...] souveräne Entscheidungen über die Verwendung ihrer Daten treffen können“ (BMWi 2016, S. 33). Neben sicherheitspolitischen Aufgaben, die vom Innenministerium abgedeckt werden, versucht das Wirtschaftsministerium, Datensouveränität durch die „grenzüberschreitende Anwendung der elektronischen Identifizierung, der qualifizierten elektronischen Signatur, des elektronischen Siegels für Unternehmen und Behörden sowie andere elektronische Vertrauensdienste“ und eine Datenschutzzertifizierung für Cloud-Dienste zu erreichen (BMWi 2016, S. 35).

Im „Aktionsprogramm Digitalisierung“ aus demselben Jahr kündigte das Wirtschaftsministerium als Teil seiner Digitalstrategie die Einrichtung eines *Monitoring*-Prozesses zur digitalen Souveränität an. Ein Ausfluss dieses Monitorings ist das 2017 vorgelegte Gutachten „Kompetenzen für eine digitale Souveränität“, dessen Handlungsempfehlungen sich neben dem Staat als regulierende Instanz auch an andere Akteure richten. Dazu bringt das Gutachten neuartige Forderungen auf und empfiehlt beispielsweise, Arbeitnehmer\*innen und Kund\*innen, Hilfsmittel an die Hand zu geben, mit denen sie informiertere Entscheidungen treffen können; dies könne z. B. durch das anvisierte Gütesiegel für digitale Produkte oder kundenfreundlicher gestaltete Datenschutzerklärungen und allgemeinen Geschäftsbedingungen mit standardisierten Textelementen und Symboliken erreicht werden (BMWi 2017, S. 72).

Viele der Empfehlungen, die auf die Sicherung der digitalen Souveränität des Wirtschafts- und Industriestandortes Deutschland abzielen, enthalten Komponenten, welche die Digitalkompetenz der deutschen Verbraucher\*innen betreffen. Der Branchenverband BITKOM fasst diese Aspekte unter den Begriff „Anwendersouveränität“ zusammen: Während „Anbietersouveränität“ in der selbstbestimmten Herstellung digitaler Technologien, Dienste und Plattformen besteht, versetze Anwendersouveränität Unternehmen und Kund\*innen in die Lage, diese selbstbestimmt einzusetzen (BITKOM 2015, S. 13). Zur Gewährleistung dieser Souveränität fordert BITKOM, das deutsche Bildungswesen um ein „digitales Bildungsideal“ zu erweitern, Informatik- und Englischkenntnisse bereits frühzeitig in der Schule zu unterrichten und langfristig die Fähigkeit zum selbstbestimmten Einsatz digitaler Technologien in allen Gruppen, Schichten und Altersklassen der Gesellschaft hinweg zu fördern (BITKOM 2015, S. 17).

### 3.3 Individuelle Dimension

Die Forderungen nach mehr Digitalkompetenz legen offen, dass die wirtschaftliche und die individuelle Dimension der digitalen Souveränität starke Überschneidungen aufweisen. Dass die Souveränität der Individuen in ihrer Rolle als Verbraucher\*innen von digitalen Diensten zu schützen sei, wurde indes schon lange vor Beginn der politischen Debatte in Europa um digitale Souveränität betont. Bereits die „Charta Verbrauchersouveränität in der digitalen Welt“ des Bundesministeriums für Ernährung, Landwirtschaft und Verbraucherschutz aus dem Jahre 2007 enthielt Kernprinzipien für eine verbraucherfreundliche Gestaltung der digitalen Produkte und Dienste (BMELV 2007). Neben IT-Sicherheit als Garant für das Recht auf „informationelle Selbstbestimmung“ empfahl das Dokument, Verbraucher\*innen aller sozialen Schichten und Altersgruppen durch Komplexitätsreduzierung Zugang zu digitalen Inhalten zu geben.

Heute steht beim Schutz digitaler Verbrauchersouveränität weniger der physische Zugang im Mittelpunkt als vielmehr die Möglichkeiten und Kompetenzen der Bürger\*innen, digitale Technologien und Inhalte sinn- und verantwortungsvoll sowie selbstbestimmt zu nutzen. 2017 definierte der Sachverständigenrat für Verbraucherfragen (SVRV) digitale Souveränität als „Handlungsfähigkeit und Entscheidungsfreiheit der Verbraucher, in der Digitalen Welt in verschiedenen Rollen zu agieren, nämlich als Marktteilnehmer, als Konsumentenbürger einer Gesellschaft sowie als ‚Prosumer‘ in sozialen Netzwerken“ (SVRV 2017, S. 3). Neben Empfehlungen zum digitalen Kompetenzaufbau durch medienpädagogische Angebote macht das Gutachten Vorschläge zur Regulierung digitaler Dienste wie z. B. die Verknappung Allgemeiner Geschäftsbedingungen und die verpflichtende Offenlegung von Algorithmen, um ihre Konformität mit dem geltenden Recht prüfen zu können.

Neben der Überlappung der individuellen und wirtschaftlichen Dimensionen digitaler Souveränität, wo individuelle Nutzer\*innen vorwiegend als Konsument\*innen digitaler Produkte wahrgenommen werden, lässt sich auch eine Verqui-

ckung mit der staatlichen Dimension feststellen. So wird in der Diskussion sicherheitspolitischer Aspekte der selbstbestimmte Umgang mit digitalen Diensten und Technologien als Voraussetzung für die mündige, digital-souveräne Bürger\*in dargestellt. 2013 definierte eine Studie des IT-Planungsrates – des politischen Steuerungsgremiums von Bund und Ländern zur IT-Koordination – digitale Souveränität als die Fähigkeit, digitale Medien sinnvoll bei der Suche, Beurteilung und Verwendung von Informationen einzusetzen, kompetent mit den eigenen Daten umzugehen und sowohl Chancen als auch Risiken der Nutzung digitaler Dienste wahrzunehmen (IT-Planungsrat 2013, S. 34). Medienkompetenz wird folglich als Grundlage eines souveränen Handelns in der digitalen Welt angesehen und sollte daher als Kernkompetenz in schulische Lehrpläne aufgenommen und von Unternehmen an ihre Mitarbeiter\*innen vermittelt werden. Dieselbe Kompetenz sollte zudem auch in der Politik aufgebaut werden, damit „digital souveräne Politiker in der Lage sind, Digitalisierungspolitik jeweils auf Höhe der Zeit bewerten und gestalten zu können“ (IT-Planungsrat 2013, S. 10).

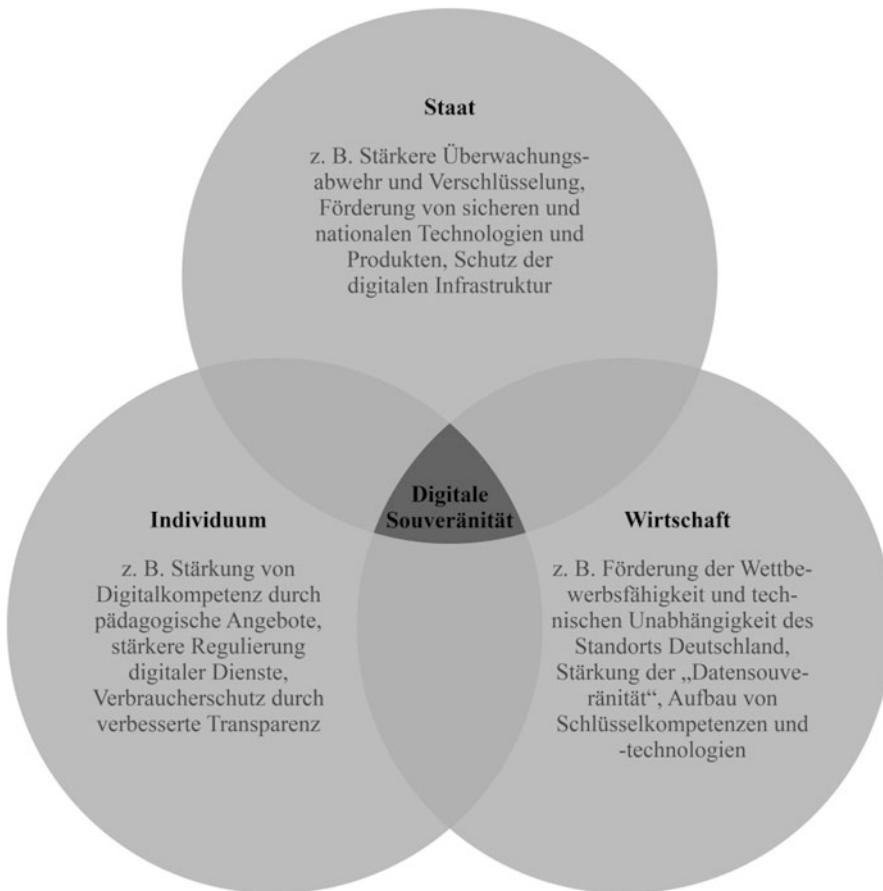
Bemerkenswert an der Studie des IT-Planungsrates ist, dass sie die Verantwortung und Pflicht, sich die zur digitalen Souveränität nötige Digitalkompetenz anzueignen, bei jeder Bürger\*in selbst sieht. Damit weicht sie sowohl deutlich von der Verbraucherschutz-Perspektive ab als auch von Positionen, welche die wirtschaftliche und staatliche Dimension der digitalen Souveränität hervorheben. Diese führen die individuelle Souveränität im Umgang mit der digitalen Welt vielmehr auf notwendige äußere Bedingungen zurück, bestehend in technischen und wirtschaftlichen Angeboten und regulatorischen Rahmenbedingungen. Denn nur wenn auf der kollektiven Ebene die notwendigen Voraussetzungen geschaffen werden, kann jede Einzelne selbstbestimmt darüber entscheiden, wie sie mit den Herausforderungen und Möglichkeiten der Digitalisierung umgehen möchte (Abb. 1).

---

## 4 Umsetzungsstand und Auswirkungen

Neben der Bedingtheit der drei Dimensionen digitaler Souveränität – staatlich, wirtschaftlich und individuell – ist es vor allem aufgrund der vorrangig präskriptiv-normative Verwendung des Konzepts schwierig, die Auswirkungen der politischen Debatte über digitale Souveränität zu evaluieren. So wird der Begriff nur selten zur Beschreibung eines Ist-Zustandes verwendet, sondern drückt vielmehr den Wunsch nach einer Situation aus, in der Staat, Unternehmen und Bürger\*innen in die Lage versetzt werden, selbstbestimmt mit den Chancen und Risiken der digitalen Vernetzung umzugehen. Entsprechend wird die tatsächliche Umsetzung der von Politik, Unternehmen und Zivilgesellschaft seit 2013 vorgebrachten Handlungsempfehlungen zur Souveränitätssicherung nur selten thematisiert und lässt sich somit schwer von anderen digitalpolitischen Maßnahmen abgrenzen.

Bei der Umsetzung scheint dem Ausbau von Schlüsselkompetenzen im Hinblick auf alle drei Dimensionen digitaler Souveränität Vorrang gegeben zu werden (Stand März 2019). Im staatlichen Bereich steht dabei vor allem die Erhöhung von Cybersicherheit im Vordergrund. Während das oft geforderte Gütesiegel für IT-Sicherheit



**Abb. 1** Dimensionen digitaler Souveränität. (Quelle: Eigene Darstellung)

noch auf sich warten lässt, wurden zum Beispiel im April 2017 vom Innenministerium die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) und vom Verteidigungsministerium das Kommando Cyber- und Informationsraum (CIR) gegründet. Im konkreten Bezug zur Debatte um digitale Souveränität steht zudem die Planung der dem BMI und BMVg zugeordneten Agentur für Innovation in der Cybersicherheit (Cyberagentur), die ambitionierte Cybersicherheits-Technologien mit strategischen Vorteilen für die innere und äußere Sicherheit entwickeln und für den Bedarf der Bundeswehr bis zur Einsatzreife bringen sollen. Als Nebeneffekt soll die Agentur zudem nationale und europäische Technologien und Expertensysteme stärken und damit die Technologiesouveränität Deutschlands und Europas sicherstellen (BMVg 2018).

Im wirtschaftlichen Bereich dient der Kompetenzaufbau vorrangig der Innovationsförderung und der Stärkung des deutschen Wirtschaftsstandorts. So versucht das Wirtschaftsministerium durch die Einrichtung verschiedener „Forschungs- und

Entwicklungsprojekte mit Leuchtturmcharakter“ die Entwicklung intelligenter Datenprodukte, -systeme und -dienste sowie datenbasierter Geschäftsmodelle voranzutreiben und das Vertrauen deutscher Unternehmen in *Cloud*-Lösungen durch das Förderprogramm „*Trusted Clouds*“ zu stärken (BMWi 2019). Auch auf europäischer Ebene sollen zudem Initiativen wie die vom BSI mitentwickelte eIDAS-Verordnung vom Juli 2016 für einen EU-weiten einheitlichen Rechtsrahmen für Vertrauensdienste wie elektronische Signaturen, Siegel und Zustelldienste und damit für sichere digitale Transaktionen sorgen.

Zur Stärkung der digitalen Selbstbestimmungsfähigkeit auf individueller Ebene baut die derzeitige Bundesregierung ebenfalls primär auf eine Förderung von Kenntnissen im Umgang mit Digitaltechnik. Während Vorschläge zur Regulierung digitaler Dienste, wie sie unter anderem vom Sachverständigenrat für Verbraucherfragen vorgebracht wurden, auf nationaler Ebene noch nicht umgesetzt wurden, floss viel Anstrengung in die Einigung zum „DigitalPakt Schule“ im Frühjahr 2019. Dieser zielt darauf ab, die Ausstattung der Schulen mit digitaler Technik und die entsprechende Qualifikation des Lehrpersonals zu verbessern und durch den verantwortungsvollen Umgang mit digitalen Lerninfrastrukturen die Medienkompetenz der Schüler\*innen, und damit langfristig auch ihre Chancen auf dem Arbeitsmarkt, zu fördern.

Mit dem Kompetenzaufbau im Bereich der Cybersicherheit, der Datenwirtschaft und im Umgang mit digitaler Technik verfolgen die bisherigen Fördermaßnahmen mittel- und langfristige Ziele, über deren Erreichen sich bisher keine Aussage treffen lässt. Bisher gibt es keine Erkenntnisse darüber, inwiefern die geforderten oder angekündigten Schritte tatsächlich zur Stärkung der digitalen Souveränität beizutragen vermögen. Gleichzeitig deuten wiederholt auftretende Vorfälle wie Hackerangriffe auf den Bundestag im Jahr 2015 und 2016 sowie der Diebstahl persönlicher Daten von rund tausend Politiker\*innen Ende 2018 darauf hin, dass weiterhin große Herausforderungen für die digitale Selbstbestimmungsfähigkeit in Deutschland und Europa bestehen.

---

## 5 Herausforderungen für Staat und Verwaltung

Die Analyse der deutschen Debatte um digitale Souveränität und ihrer Auswirkungen zeigt, dass sich eine starke wirtschafts- und sicherheitspolitische Sichtweise auf die digitale Souveränität in der Politik durchsetzt. Die Handlungsempfehlungen und neubegründeten Kompetenzen zielen vorwiegend auf die Sicherung einer zukunftsfähigen digitalen Infrastruktur und die Wettbewerbsfähigkeit der deutschen Wirtschaft und Industrie ab. Im Hinblick auf die digitale Souveränität von Individuen dominiert die Perspektive des Verbraucherschutzes, welche die Bürger\*innen primär als Konsument\*innen digitaler Dienste und Technologien wahrnimmt. Diese Sichtweise birgt jedoch das Risiko, das Streben nach digitaler Souveränität auf eine reine Wirtschafts- und Sicherheitsstrategie zu verengen und den komplexen Fragen nach der Handlungs- und Selbstbestimmungsfähigkeit jedes Einzelnen und des Staates als der Gesamtheit aller Bürger\*innen in Zeiten der

Digitalisierung nicht gerecht werden zu können. Damit alle wichtigen Aspekte ausreichend Aufmerksamkeit erhalten, bedarf es einer kohärenten Strategie, in der die drei Dimensionen digitaler Souveränität zwar klar differenziert, aber gleichzeitig gemeinsam betrachtet werden. Die Integration aller existierenden und zu ergänzenden Handlungsempfehlungen in eine solche umfassende Strategie stellt eine der größten Herausforderung in Bezug auf digitale Souveränität dar.

Eine weitere schwierige Aufgabe, der Staat und Verwaltung in den nächsten Jahren gegenüberstehen, ist die Umsetzung ihrer eigenen ambitionierten Ziele. Indem sie digitale Souveränität immer wieder in Aussicht stellen, suggerieren politische Akteur\*innen, Lösungsvorschläge bereitzuhalten, um die Sicherheit und Selbstbestimmung von Bürger\*innen, der heimischen Wirtschaft und des Staates in Zeiten der Digitalisierung gewährleisten zu können. Die praktische Umsetzung dieser Vorschläge zielt jedoch auf langfristige Lösungen ab; ihre tatsächliche Wirkkraft ist daher kaum absehbar. Damit besteht die Gefahr, dass die Politik und Unternehmen die Stärkung der digitalen Souveränität zwar in Aussicht stellen, gleichzeitig aber nicht für die kurz- und mittelfristig benötigte Sicherung der IT-Infrastruktur und der Entscheidungsfreiheit der Kund\*innen und Bürger\*innen einstehen können. Notwendig ist folglich nicht nur die entschlossene Umsetzung von Maßnahmen mit kurz-, mittel- und langfristigen Auswirkungen, sondern auch die kontinuierliche Evaluierung und potenzielle Korrektur des bisher eingeschlagenen Kurses.

---

## Literatur

- BITKOM. 2015. Digitale Souveränität. Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa. Berlin. [https://www.bitkom.org/sites/default/files/pdf/Presse/An\\_haenge-an-PIs/2015/05-Mai/BITKOM-Position-Digitale-Souveraenitaet1.pdf](https://www.bitkom.org/sites/default/files/pdf/Presse/An_haenge-an-PIs/2015/05-Mai/BITKOM-Position-Digitale-Souveraenitaet1.pdf). Zugegriffen im März 2019.
- BMELV (Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz). 2007. Charta Verbrauchersouveränität in der Digitalen Welt. Berlin. [https://www.vzbv.de/sites/default/files/\\_mediapics/chartha\\_digitale\\_welt\\_1532007.pdf](https://www.vzbv.de/sites/default/files/_mediapics/chartha_digitale_welt_1532007.pdf). Zugegriffen im März 2019.
- BMVg (Bundesministerium der Verteidigung). 2018. Technologiesouveränität erlangen – die neue Cyberagentur. Berlin. <https://www.bmvg.de/de/aktuelles/technologiesouveraenitaet-erlangen-die-neue-cyberagentur-27996>. Zugegriffen im März 2019.
- BMWi (Bundesministeriums für Wirtschaft und Energie). 2015a. Gabriel: CeBIT 2015 wichtige Wegmarke für Umsetzung der Digitalen Agenda. Pressemitteilung. Berlin. <https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2015/20150316-gabriel-cebit-2015-wichtige-wegmarke-fuer-umsetzung-der-digitalen-agenda.html>. Zugegriffen im März 2019.
- BMWi. 2015b. Leitplanken Digitaler Souveränität. Berlin: Nationaler IT-Gipfel. [https://www.de.digital/DIGITAL/Redaktion/DE/Downloads/it-gipfel-2015-leitplanken-digitaler-souveraenitaet.pdf?\\_\\_blob=publicationFile&v=1](https://www.de.digital/DIGITAL/Redaktion/DE/Downloads/it-gipfel-2015-leitplanken-digitaler-souveraenitaet.pdf?__blob=publicationFile&v=1). Zugegriffen im März 2019.
- BMWi. 2016. Digitale Strategie 2025. Berlin. [https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-strategie-2025.pdf?\\_\\_blob=publicationFile&v=8](https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-strategie-2025.pdf?__blob=publicationFile&v=8). Zugegriffen im März 2019.
- BMWi. 2017. Kompetenzen für eine digitale Souveränität. Berlin. [https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/kompetenzen-fuer-eine-digitale-souveraenitaet.pdf?\\_\\_blob=publicationFile&v=14](https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/kompetenzen-fuer-eine-digitale-souveraenitaet.pdf?__blob=publicationFile&v=14). Zugegriffen im März 2019.

- BMWi. 2019. Den digitalen Wandel gestalten. Berlin. <https://www.bmwi.de/Redaktion/DE/Dossier/digitalisierung.html>. Zugegriffen im März 2019.
- Friedrichsen, Mike, und Peter-Jan Bisa, Hrsg. 2016. *Digitale Souveränität: Vertrauen in der Netzwerkgesellschaft*. Wiesbaden: Springer VS.
- Hofmann, Jeanette. 2005. Internet Governance. Zwischen staatlicher Autorität und privater Koordination. *Internationale Politik und Gesellschaft* 3:10–29.
- IT-Planungsrat. 2013. Zukunftspfade Digitales Deutschland 2020. Berlin: TNS Infratest. <http://www.medienpolitik.net/wp-content/uploads/2014/01/zukunftspfade-digitales-deutschland-2020.pdf>. Zugegriffen im März 2019.
- Mertz, Marcel, Marc Jannes, Anna Schloemann, Enza Manderscheid, Christian Rietz, und Christiane Woopen. 2016. *Digitale Selbstbestimmung*. Köln: CERES.
- Misterek, Fokko. 2017. Digitale Souveränität. Technikutopien und Gestaltungsansprüche demokratischer Politik. MPIfG Discussion Paper 17/11. Köln: Max-Planck-Institut für Gesellschaftsforschung.
- Mueller, Milton. 2015. Gibt es Souveränität im Cyberspace? *Journal of Self-Regulation and Regulation* 1:65–80.
- Schaar, Peter. 2015. Globale Überwachung und digitale Souveränität. *Zeitschrift für Außen- und Sicherheitspolitik* 8(4): 447–459.
- SVRV (Sachverständigenrat für Verbraucherfragen). 2017. Digitale Souveränität. Gutachten des Sachverständigenrats für Verbraucherfragen. Berlin. [http://www.svr-verbraucherfragen.de/wp-content/uploads/Gutachten\\_Digitale\\_Souver%C3%A4nit%C3%A4t\\_.pdf](http://www.svr-verbraucherfragen.de/wp-content/uploads/Gutachten_Digitale_Souver%C3%A4nit%C3%A4t_.pdf). Zugegriffen im März 2019.
- Thiel, Thorsten. 2014. Internet und Souveränität. In *Der Begriff der Souveränität in der Transnationalen Konstellation*, Hrsg. Christian Volk und Friederike Kuntz, 215–239. Baden-Baden: Nomos.



# Dateneigentum

Frank Nullmeier

## Inhalt

1 Klärung der Begriffe .....	256
2 Konzeptionelle Grundlagen .....	257
3 Praktische Anwendungsfelder .....	260
4 Gesellschaftliche Auswirkungen .....	261
5 Perspektiven für Staat, Verwaltung und Politik .....	262
Literatur .....	264

## Zusammenfassung

Angesichts der Bedeutung von Daten für die aktuelle und zukünftige Marktentwicklung wäre zu erwarten, dass Daten heute einen rechtlich geklärten Status besitzen. Das ist aber nicht der Fall: Datenschutz bezieht sich nur auf personenbezogene Daten. Einem besonderen Schutz unterliegen auch Ergebnisse schöpferischer Aktivitäten, die unter dem Begriff „Geistiges Eigentum“ gefasst und über Urheberrechte geschützt werden. Aber das klassische Rechtsinstitut, das Eigentumsrecht, greift bei Daten gerade nicht. Denn Eigentum bezieht sich nur auf „Sachen“ und Sachen müssen Körperlichkeit besitzen, eine Eigenschaft, die zwar Datenträgern, aber nicht Daten zugeschrieben werden kann. Angesichts der gegenwärtigen Rechtslage wird in Wissenschaft und Politik diskutiert, ob es in Zukunft ein Dateneigentum („data ownership“) geben sollte. Unter Dateneigentum wird dabei eine gesetzliche Regelung verstanden, die die vollständige Kontrolle (einschließlich des Erwerbs, der Nutzung: Erstellung, Bearbeitung, Modifikation, Auswertung, sowie des Teilens, der Zugriffsbeschränkung, der Überlassung an Dritte) über ein einzelnes Datenelement oder einen Datensatz einem Rechtssubjekt zuschreibt. Die Mehrheit der Diskussionsbeiträge tendiert

---

F. Nullmeier (✉)  
SOCIUM Forschungszentrum Ungleichheit und Sozialpolitik, Universität Bremen, Bremen, Deutschland  
E-Mail: [frank.nullmeier@uni-bremen.de](mailto:frank.nullmeier@uni-bremen.de)

aktuell dazu, ein solches Dateneigentum nicht als Förderung, sondern als gravierendes Hindernis der wirtschaftlichen Entfaltung einer datenbasierten Ökonomie zu verstehen. Besonders viele Daten werden in Zukunft beim autonomen Fahren anfallen. In der Debatte über diese neue Form der Mobilität wird deutlich, dass Haftungsfragen und die Konkurrenz der beteiligten Unternehmen rechtliche Regelungen ähnlich einem Dateneigentum verlangen könnten.

---

### Schlüsselwörter

Datenrechte · Informationelle Selbstbestimmung · Vertragsfreiheit · Geistiges Eigentum · Datenzugang

---

## 1 Klärung der Begriffe

Digitalisierung erzeugt in riesigem Umfang Daten, sie sind Produkt, Nebenprodukt und pure prozessuale Erscheinungsform von digitalisierten Vorgängen. Diese Universalität des Aufkommens von Daten und ihrer breiten Nutzbarkeit macht die Frage höchst relevant, welchen rechtlichen Status Daten haben. Sind sie Privateigentum und wenn ja, in wessen Hand? Die Frage des Dateneigentums ist weitreichender als die des Datenschutzes, der in seiner jetzigen Gestaltung auf der Unterscheidung nicht personenbezogener und personenbezogener Daten beruht und sich allein auf Regelungen für letztere bezieht. Die Frage, was Daten rechtlich gesehen sind, erstreckt sich dagegen auf alle Formen von Daten, auch jene, die ohne unmittelbare Beteiligung von Personen, z. B. im Austausch zwischen Firmen (B2B) oder im ‚Internet der Dinge‘ zwischen Maschinen, als digitale Kommunikation von Artefakten anfallen. Eine primäre Aufgabe eines Staates, noch vor jeder Sozial- und Interventionsstaatlichkeit, besteht darin, einen Rechtsrahmen für die wirtschaftlichen und sozialen Prozesse in einem Land zu setzen. Das Eigentumsrecht steht dabei aufgrund seiner Bedeutung für alle wirtschaftlichen Vorgänge und aufgrund seiner Zentralstellung im Privatrecht im Vordergrund. Man könnte daher erwarten, dass ein Dateneigentumsrecht eine bedeutsame Rolle in der Digitalisierungspolitik besitzt.

Unter Dateneigentum („data ownership“) sind gesetzliche Rechte zu verstehen, die die vollständige Kontrolle über ein einzelnes Datenelement oder einen Datensatz einem Rechtssubjekt zuschreiben. Ein derartiges Recht enthält Regelungen, die die jeweiligen Eigentümer\*innen von Datenbeständen bestimmen sowie die von Dateneigentümer\*innen legal einsetzbaren Formen des Erwerbs, der Nutzung (Erstellung, Bearbeitung, Modifikation, Auswertung), des Teilens und der Zugriffsbeschränkung. Das Dateneigentum umfasst auch die Rechte der Eigentümer\*innen, diese Rechte an Dritte abzutreten oder Teile dieser Rechte Dritten zu überlassen.

In diesem Sinne eines umfassenden Eigentumsrechts existiert aktuell in der deutschen Rechtsordnung kein Dateneigentum. Die *aktuelle Rechtslage* in Deutschland kennt aber auch keinen generellen freien Zugang zu Daten. Das geltende Recht wird (a) von Bestimmungen zum Sacheigentum im BGB sowie (b) von Regelungen zum geistigen Eigentum bestimmt, die sich als Teil des Immaterialgüterrechts

insbesondere im Urheberrechtsgesetz finden (vgl. als Überblicke Jöns 2016; Schütze et al. 2018; BMVI 2018; Stiftung Datenschutz 2019).

- a) Die Eigentumsrechte im BGB beziehen sich nur auf „Sachen“. Das Sachgüterrecht verlangt aber, dass eine Sache Körperlichkeit besitzt (§ 90 BGB). Diese Körperlichkeit kann für Daten jedoch nicht aufgezeigt werden. Auch wenn sie ohne eine Bindung an eine physikalische Entität (Datenträger) nicht bestehen können, so sind sie doch beliebig vervielfältigbar und damit auf etlichen physikalischen Trägern reproduzierbar, so dass sie keine physikalische Einmaligkeit besitzen, ein Kennzeichen von Körperlichkeit. Die Bindung des privatrechtlichen Begriffs der „Sache“ an Körperlichkeit lässt die Anwendung des eigentumsrechtlich primären Ansatzpunktes des § 903 Satz 1 BGB, der erlaubt, mit einer Sache „nach Belieben“ verfahren zu können und Dritte auszuschließen – deshalb wird häufig von einem „absoluten“ Eigentumsrecht oder einem „Ausschließlichkeitsrecht“ gesprochen – auf Daten nicht zu. Dagegen ist der Datenträger ein physikalisches Objekt, mithin mit der Eigenschaft der Körperlichkeit versehen. Datenträger können entsprechend als Sacheigentum behandelt werden. Eingriffe in die physikalische Struktur eines Datenträgers oder Manipulationen auf einem Datenträger sind entsprechend strafbar. Da Daten mit einem Datenträger nicht strikt verknüpft sind und gleichzeitig auf mehreren Datenträgern gespeichert werden können, ist von dem Eigentumscharakter der Datenträger nicht auf ein Eigentum an den Daten zu schließen.
- b) Einem besonderen Schutz unterliegen im sogenannten Immaterialgüterrecht Ergebnisse schöpferischer Aktivitäten unter dem Begriff „Geistiges Eigentum“ („Intellectual Property“). Hier sind die Regelungen des Urheberrechts ausschlaggebend, das derzeit im Zentrum digitalpolitischer Auseinandersetzungen steht. Diese Konflikte werden hier aber nicht behandelt, da das Urheberrecht nur eigentumsrechtliche Regeln für einen Sonderbereich der Daten schafft, unter Dateneigentum aber eine generalisierte Zuweisung von Eigentumsrechten an Daten verhandelt wird. In dem für privatrechtlich verfasste Gesellschaften zentralen Bereich des Eigentumsrechts gibt es für alle Entitäten, die nicht als geistige Schöpfungen gelten können, mithin keinerlei grundlegende eigentumsrechtliche Regelungen.

---

## 2 Konzeptionelle Grundlagen

Zur Klärung der Frage, ob es ein allgemeines Dateneigentum geben oder nicht geben sollte, sind zunächst die Kriterien zu benennen, die zur Anwendung gebracht werden können. Die Lückenlosigkeit und Kohärenz eines Rechtssystems stellen zwei Kriterien dar, die zur Klärung der Frage, ob es ein generelles oder ein nach Bereichen spezifiziertes Dateneigentum geben soll, sicherlich einschlägig sind. Aus der Tatsache, dass im Rechtssystem eine Thematik nicht geregelt ist, folgt aber für die meisten Juristen\*innen nicht die Notwendigkeit einer gesetzgeberischen Initiative, um diese Lücke zu schließen. Rechtssicherheit und die Klärung von Interessenkonflikten

durch Recht können ebenso als Kriterien für eine Antwort auf die Frage herangezogen werden, ob es ein allgemeines Recht an den eigenen Daten geben sollte. Je größeren Wert Daten für Unternehmen und Individuen gewinnen, durchaus auch in einem vermögensrechtlichen Sinn, desto wichtiger wird eine rechtliche Klärung. Eine große Rolle in den akademischen wie politischen Diskussionen spielen wirtschaftliche Überlegungen: So werden die Ermöglichung von innovativen Geschäftsmodellen, die Handelbarkeit, der breite Zugang zu Daten und die Wettbewerbsfähigkeit der europäischen Wirtschaft als Maßstäbe einer deutschen und europäischen Datenrechtsordnung eingefordert. Vor dem Hintergrund dieser Kriterien halten die meisten Autor\*innen die bisherige Rechtslage ohne Dateneigentum für angemessener, da eine dateneigentumsrechtliche Regelung die Transaktionskosten deutlich erhöhen und die Expansion der Digitalwirtschaft behindern würde (vgl. u. a. Jöns 2016; Smart-Data-Begleitforschung 2017; Stiftung Datenschutz 2019; Scassa 2018). Auch die Unternehmen selbst sind an einer Klärung der Eigentumsfragen nicht interessiert. Eine von der Beratungsfirma Deloitte für die EU-Kommission angefertigte „Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability“ (European Commission 2018) kommt aufgrund der Auswertung der Problemlagen von Firmen, die aktiv Digitalisierung betreiben, zu dem Ergebnis, dass sowohl die Zugangs- als auch die Haftungsproblematik als primäres Hindernis weiterer Expansion auf digitalen Märkten angesehen werden. Fragen der Dateneigentümer\*innenschaft gelten dagegen als zweitrangig. Die Kombination aus tatsächlicher Verfügung über Daten ohne Eigentumsrecht und vertragsrechtlich frei gestaltbarem Handel von Daten erscheint unter wirtschaftspolitischen Gesichtspunkten als überlegen gegenüber einem expliziten Eigentumsrecht an Daten, unabhängig von der Frage, wem dieses Recht dann zukommen würde.

Jenseits dieser wirtschaftspolitischen Kriterien kann aber auch die Theorie der Güter aus der Wirtschaftswissenschaft herangezogen werden, um eine systematische Antwort zur Frage der eigentumsrechtlichen Behandlung von Daten zu bekommen: Als private Güter werden nur solche Güter angesehen, bei denen Rivalität des Konsums besteht und Ausschließbarkeit anderer vom Konsum dieser Güter gegeben ist. Bei Daten liegt jedoch Nicht-Rivalität vor, sie können zugleich von einer größeren Zahl an Nutzern verwendet werden und werden dabei nicht ‚verbraucht‘ (Jöns 2016). Das würde dafür sprechen, Daten als öffentliche Güter anzusehen. Da es aber möglich ist, andere mit nur geringen Kosten von ihrer Nutzung auszuschließen, eignet sich diese Zuordnung nicht. Angesichts der immer größer werdenden Datens Mengen und der immer leichter werdenden Möglichkeiten, neue Daten zu generieren, käme auch eine Zuordnung der Daten zur Gruppe der freien Güter (z. B. Luft) in Betracht. Dann wäre aber anzunehmen, dass der wirtschaftliche Bedarf immer geringer ist als die zur Verfügung stehende Menge an Daten – was nicht der Fall ist. Daten sind daher weder freie noch öffentliche Güter noch reine private Güter. Da Nicht-Rivalität, aber leichte Ausschließbarkeit gegeben sind, kann man am ehesten von einem „Klubgut“ sprechen. Für diese Güterart ist sowohl Privateigentum als auch öffentliche Bereitstellung denkbar. Die ökonomische Theorie liefert hier also keinen Schlüssel für eine klare eigentumsrechtliche Position.

Da weder diese Bestimmungsversuche noch das Sachenrecht oder das Recht geistigen Eigentums eine hinreichende Grundlage für eine Klärung des Eigentumscharakters von Daten ergeben haben, sind in der rechtswissenschaftlichen Literatur sowie in einigen Gutachten und Verbandsstellungnahmen auch weitere Rechtsgebiete als Ausgangspunkt einer juristischen Verortung von Daten vorgeschlagen und geprüft worden:

- a) Strafrecht: Das deutsche Strafrecht macht keine Unterschiede zwischen personenbezogenen und nicht-personenbezogenen Daten und bestimmt in § 303a, dass mit einer Freiheitsstrafe bis zu zwei Jahren oder einer Geldstrafe bedacht wird, wer rechtswidrig Daten, „die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden“ (§ 202a Abs. 2 StGB), löscht, unterdrückt, unbrauchbar macht oder verändert. In diesen Regelungen hat der Rechtswissenschaftler Thomas Hoeren einen Ansatzpunkt für ein allgemeines Dateneigentum finden wollen, weil eine strafrechtliche Verfolgung eine klare Zuordnung der Daten (und nicht nur des Datenträgers) zu einem Verfügungsberechtigten verlangt (Hoeren 2013).
- b) Wettbewerbsrecht: Im Gesetz gegen den unlauteren Wettbewerb (UWG) werden Betriebs- und Geschäftsgesheimnisse gegen den Bruch der Vertraulichkeit geschützt. Hier sind aber nur Unternehmen geschützt. Zudem ist nur ein Teil aller anfallenden Daten als Betriebs- oder Geschäftsgesheimnis anzusehen, auch wenn dem Betriebsinhaber rechtlich ein großer Spielraum in der Definition der Betriebsgeheimnisse eingeräumt wird.

Aus der Beschreibung der Rechtslage sind kaum Ansatzpunkte für eine Weiterentwicklung des Rechts zu gewinnen, die Anwendung der genannten normativen Kriterien führt zu keinen eindeutigen Ergebnissen. Der Jurist Karl-Heinz Fezer hat daher als Alternative zu einem klassischen Eigentum an Daten mit individuellen Übertragungsrechten und der derzeitigen Rechtssituation stärker demokratietheoretisch argumentierend ein Bürgerrecht an verhaltensgenerierten Daten vorgeschlagen, das von der Zivilgesellschaft repräsentativ und nicht individuell wahrgenommen wird. Die individuellen Dateneigentumsrechte werden nach seinem Vorschlag gesichert von einer Datenagentur, die mit den Unternehmen über Schutz- und Verwertungsrechte etc. verhandelt und die vermögensrechtliche Position der Bürger in einem Datensondervermögen bündelt, aus dem digitale (Weiter-)Bildung, Sicherheit und Infrastruktur finanziert werden (Fezer 2018). Damit wird die Verfügung über Daten kollektiviert und durch einen neuen öffentlichen Träger vermittelt. Im politischen Raum haben derartige Vorschläge bisher keine Resonanz gefunden.

Einen anderen Ansatz zur Beantwortung der Frage, ob es ein Dateneigentum geben sollte, liefert der Rekurs auf Interessen. Unternehmen sind vorrangig an der Verfügbarkeit und Nutzbarkeit von Daten für das Betreiben von neuen Geschäftsmodellen interessiert, aber auch an der Handelbarkeit von Daten als weiterem Verwertungsweg neben der Nutzung für das eigene Geschäft. Solange Besitz an Daten besteht, der nicht bestritten wird und der gegen Diebstahl, Verrat geschützt ist, ist ein umfassendes Eigentumsrecht keine zentrale Frage. Daher neigen die eher wirt-

schaftsnahen Beiträge einschließlich der Stellungnahmen der Branchenverbände dazu, keine Eigentumsrechte an Daten zu schaffen. Der gegenwärtige ungeregelte Zustand wird präferiert. In juristischer Diktion muss dann aber verneint werden können, dass es einen rechtlichen Schutzbedarf gibt. Durch die freie Dateneneignung werden aber stärkere Akteure bevorzugt, es findet kein Interessenausgleich zwischen großen und kleinen Unternehmen statt, mithin könnte im Schutz der kleineren Unternehmen eine rechtlich kaum zu verneinende Aufgabe liegen. Im Rechtssystem sind es die Rechtsanwälte, die von einer gesetzlich ungeregelten Situation deutlich profitieren. Da alles vertragsrechtlich gelöst werden muss, bildet Expertise für Vertragsgestaltung ein wichtiges Geschäftsmodell. Aus Sicht der Bürger\*innen und Kund\*innen ist dagegen der Schutz gegen missbräuchliche Nutzung der Daten und die Sicherung ihrer informationellen Selbstbestimmung entscheidend. In der Bundesregierung ist bisher allein das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) an einer Regelung des Dateneigentums interessiert. Die EU stellt die Förderung einer europäischen Digitalökonomie in den Vordergrund, um in der Konkurrenz mit den weltweit führenden amerikanischen Unternehmen bestehen zu können, und will alle Erschwernisse dafür beseitigen, zudem ein gemeinsames Recht für den europäischen Binnenmarkt sichern. Mit der Verordnung vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der EU wird ein einheitlicher Rechtsrahmen angemahnt, der alle Formen von Handelshemmnissen beseitigt. Eigentumsrechte werden hier nicht als Lösungsform erwähnt (EU 2018).

---

### 3 Praktische Anwendungsfelder

Impulse in Richtung Dateneigentum gehen weniger von den abstrakten Überlegungen zur konsistenten Gestaltung des Rechtssystems aus, sondern resultieren aus konkreten Anwendungsproblemen, die insbesondere im Bereich der Einführung neuer Mobilitätsformen entstehen. Die beim autonomen Fahren anfallenden Daten sind äußerst vielgestaltig, sie können sich auf den Verkehr, auf den Zustand des Fahrzeugs, das Verhalten des Fahrenden (und auch der Mitfahrenden) oder auch die Straßenverhältnisse und das Wetter beziehen. Entsprechend unterschiedliche Interessen an den Daten können auftreten. Daher sind im Bereich der Mobilitätspolitik aktuell die weitreichendsten Überlegungen in Richtung einer allgemeinen Eigentumsregelung für Daten entstanden: In einem Gutachten für das Bundesministerium für Verkehr und digitale Infrastruktur aus dem Jahre 2018 („Eigentumsordnung“ für Mobilitätsdaten? Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive“, BMVI 2018) wird die Erzeugung von Daten zum zentralen Ansatzpunkt in der Konstruktion eines Dateneigentumsrecht: Die Eigentumsrechte sollten sich, so das Gutachten, nach den Leistungsanteilen an der Erstellung der Daten richten. Es wird entsprechend nach dem „Verdienst“ bzw. der „Leistung“ gefragt, die seitens bestimmter Akteure in einen Datenerstellungsvorgang eingehen. Um die relativen Anteile als Grundlage der Zuweisung von Eigentumsrechten genauer bestimmen zu können, wird die Datenerzeugung zerlegt in jenen Teil, der seitens eines Nutzers

erbracht wird, und jenen, der durch die Bereitstellung der Datenerfassung in einer Technologie gegeben ist. Dabei wird nur in den seltensten Fällen von Mobilitätsdaten die Datenbereitstellung durch den Nutzer das Übergewicht besitzen, so dass die Eigentumsrechte ganz überwiegend auf Seiten der Softwarebereitsteller bzw. derjenigen Produzenten liegen werden, die die Software im Rahmen eines Produktes bereitstellen – im Falle der Mobilitätsdaten also die Autohersteller bzw. ihre Zulieferer.

Konflikte können auch bei Gesundheitsdaten auftreten, doch ist dort der Personenbezug der Daten so hoch, dass zunächst die Regelungen der Datenschutz-Grundverordnung greifen. Erst wenn sich deren Wirkungslosigkeit erweisen würde, ist auch mit Impulsen für ein allgemeines Dateneigentum aus diesem Anwendungsfeld zu rechnen.

---

## 4 Gesellschaftliche Auswirkungen

Die tatsächlichen Auswirkungen einer fragmentierten Regulation von Daten ohne generelles Dateneigentum *und* ohne Sicherung eines offenen Datenzuganges bestehen darin, dass die faktische Datenverfügung zur entscheidenden Größe wird. Da der Inhaber der Datenträger eigentumsrechtlich geschützt ist, ist die Verfügung des Dateninhabers über die Inhalte der Daten nur den oben aufgeführten speziellen Regelungen unterworfen. Darüber hinaus gilt allein die Vertragsfreiheit.

Die Besonderheit der aktuellen Rechtslage liegt darin, dass Handelbarkeit gerade dadurch erzeugt wird, dass auf explizite Eigentumsrechte verzichtet wird. Wie ist aber Handelbarkeit ohne Eigentumsrecht überhaupt möglich? Schließlich ist das Kaufen und Verkaufen nach Belieben ein Kernelement des Eigentumsrechts. Die Nicht-Rivalität im Konsum gestattet es jedoch, die Daten gleich mehrfach zu verkaufen. Damit ein solcher Handel entsteht, muss eine Ausschließlichkeit der Verfügung über das handelbare Gut, die Daten, auf Seiten eines Handelspartners existieren, und eine Nachfrage nach diesen Daten von der Seite eines anderen Handelspartners, der aber keinen Zugang zu den Daten hat. Es besteht mithin eine ausschließliche Verfügung über die Daten bei einem Akteur, die aber nicht als Eigentum gefasst wird. Diese Verfügung beruht aktuell darauf, dass ein Akteur über das Eigentum an den Datenträgern mitsamt den Daten verfügt. Dadurch werden die Daten zwar nicht sein Eigentum, gelangen aber in seinen ausschließlichen *Besitz*. Die Datenerhebung bleibt gebunden an einen Datenträger, an dem Eigentum besteht. Die Daten, die keinen Eigentumscharakter haben, befinden sich aber im Besitz der Eigentümer\*innen des Datenträgers. Die aktuelle Rechtssituation könnte daher mit Bezug auf die Unterscheidung von Besitz als tatsächlichem Innehaben einer Sache und Eigentum als einem umfassenden Rechtstitel an einer Sache als *Datenbesitzrecht* bezeichneten werden (vgl. Pierson 2013, 2016).

Diese Rechtslage überlässt jenseits personenbezogener Daten und schöpferischer Produkte weithin alles vertraglichen Abmachungen. Damit ist der wirtschaftlichen Dispositionsfähigkeit von Unternehmen, die Daten erzeugen oder erheben, die Entwicklung von datengetriebenen Geschäftsmodellen überlassen. Das wird auch

solange als gewollter Effekt rechtlicher Zurückhaltung verstanden, wie digitale Geschäftsmodelle entstehen, die mit dem bisherigen Weg deutscher Wirtschaftspolitik konformgehen. Dort, wo die Datensammlung aber bei ausländischen Firmen mit quasi-monopolistischer Reichweite liegt, erscheint im Zuge nationaler Wettbewerbsstrategien und industrie-politischer Ansätze die Übermacht bestimmter Unternehmen zunehmend als ökonomisches und politisches Problem. Das Vertragsrecht begünstigt bestehende Asymmetrien und ist durchaus auch ein Weg, diese Ungleichgewichte zu befestigen und auszubauen. Die internationale Konkurrenz auf Märkten wie der Automobilbranche, die für Deutschland als fundamental wichtig angesehen werden, lassen daher nach Konzepten einer Industriepolitik suchen, den starken amerikanischen (oder auch chinesischen) Firmen nicht das Feld zu überlassen. Industriepolitik und auch das Wettbewerbsrecht scheint damit ein Regulierungsfeld zu werden, das zunehmend für die digitale Ökonomie Bedeutung erhält. Das Entstehen von Datenmonopolen oder -oligopolen, die die Möglichkeit, neue digitale Geschäftsmodelle zu etablieren, erheblich erschweren, könnte auch unabhängig von der nationalen Bindung von Unternehmen die Wettbewerbsregulierung auf den Plan rufen. Auch die Innere Sicherheit kann angesichts der Verbindung von *Big Data*-Firmen mit ihren nationalen Geheimdiensten als Regulierungsanker verwendet werden. Dies trägt zwar nicht zu einer Politik eines generellen Dateneigentums bei, erhöht aber die Regulierungsintensität gegenüber dem bisher sehr freien Spiel der Marktkräfte.

---

## 5 Perspektiven für Staat, Verwaltung und Politik

Auch die Befürworter einer Bewahrung und moderaten Weiterentwicklung der derzeitigen Rechtsregeln halten es für nicht unwahrscheinlich, dass es zusätzlich zu diesen Fragen des Wettbewerbes und der inneren Sicherheit in Zukunft nicht immer zu einvernehmlichen vertraglichen Regelungen (z. B. auf dem Gebiet des autonomen Fahrens) kommt, sondern Konflikte sich so zuspitzen, dass eine Klärung durch Gerichte oder den Gesetzgeber verlangt wird. Interessenkonflikte können daher unterschiedliche Rechtsauffassungen erzeugen, die auch gerichtlich unterschiedliche Lösungen finden. Wenn dadurch die Rechtsunsicherheit wächst, sind legislative Eingriffe zu erwarten, aber wohl eher auf einzelnen Rechtsgebieten. Angesichts der divergierenden wirtschaftlichen Interessen und der in den vielen Anwendungsfeldern recht unterschiedlichen Konstellationen ist eine einfache Einbeziehung der Daten in das Eigentumsrecht qua Umformulierung des § 90 BGB (*Sachen und Daten*) oder eine ähnliche Regelung auf mittlere Frist nicht zu erwarten.

Einen Vorschlag, der in der Öffentlichkeit Aufsehen erregt hat, hat der Friedenpreisträger des Deutschen Buchhandels, Jaron Lanier, mit seiner Forderung gemacht, dass „in einer Welt der digitalen Würde ... jeder einzelne Mensch der kommerzielle Eigentümer aller seiner Daten, die sich aus seiner Situation oder seinem Verhalten ermitteln lassen“, sein sollte (Lanier 2014, S. 46). Wenn die Daten den Kunden gehören, müssen die Unternehmen, die sie nutzen wollen, dafür zahlen. Das ist das Gegenteil einer konsequenten *Open Data*-Politik. Diese verlangt die

kostenfreie Zugänglichkeit aller Daten für alle. Dies stößt aber sowohl bei personenbezogenen Daten wegen der informationellen Selbstbestimmung als auch bei nicht-personenbezogenen Daten wegen der Betriebs- und Geschäftsgeheimnisse auf klare Grenzen, trägt aber auch dazu bei, das Urheberrecht für schöpferische Produkte aufzuheben. In Laniers Szenario eines durchgehenden Dateneigentums würde dagegen für jedes einzelne Datum feststehen, wer der Dateneigentümer bzw. die Dateneigentümerin ist. Es würde freie Handelbarkeit mit allen Konsequenzen bestehen. Teil jeder digitalen Kommunikation müsste entsprechend ein Vertrag über die Nutzung, Abtretung etc. der in dieser Kommunikation enthaltenen Daten sein. Gegenüber dem eigentlichen Zweck der Nutzung digitaler Medien: Kommunikation mit Freunden, Erwerb eines Buches, Buchung einer Reise, Fahren eines autonomen Fahrzeuges würde der Datenentstehung und -verwendung eine eigene rechtliche Dimension zukommen. Es ist aber unwahrscheinlich, dass diese Dimension Unabhängigkeit gegenüber dem eigentlichen Zweck gewinnen kann. Wenn man ein Buch erwirbt, wird die Datendimension Unterteil eines Gesamtvertrages sein, in dem der Buchpreis zu entrichten ist. Zwar kann dies – z. B. für Zwecke der Versteuerung – ausgewiesen werden, aber es ist anzunehmen, dass die Einnahmen für Datennutzung, die etwa einem Käufer eines Buches auf einer Plattform entstehen (Datenüberlassungseinnahmen) nur einen Bruchteil der Gesamtkosten ausmachen werden. Zudem müsste zusätzlich zum Eigentumsrecht an Daten eine Kontrahierungspflicht gesetzlich eingeführt werden, damit das Einkaufen auf einer Plattform auch für jene möglich wird, die ihre Daten nicht verkaufen, d.h. zur Nutzung der Plattform überlassen wollen. Ohne die Kontrahierungspflicht, so würden einige Autoren es sehen wollen, entspräche diese komplizierte eigentumsrechtliche Situation bereits dem, was wir heute sehen: Daten gegen kostenfreie Kommunikationsleistungen bzw. gegen kostengünstige Kaufmöglichkeiten. Im Verhältnis der Unternehmen zueinander z. B. bei B2B-Geschäften oder beim autonomen Fahren mit der Vielzahl der beteiligten Firmen kann die Entstehung einer eigenen, rechtlich geschützten Dimension der Dateneigentümer\*innenschaft dann problemlos als Teil der Verhandlungen zwischen den Firmen bewältigt werden, sofern nur Firmen als Dateninhaber auftreten. Sobald die Fahrer\*innen des Autos als (Teil-)Rechteinhaber auftreten sollten, ergibt sich die oben bereits beschriebene Situation, dass nur bei Kontrahierungzwang für Personen, die ihre Daten nicht abgeben oder fremdnutzen lassen wollen, ein Vorteil für die Kund\*innen entsteht. Erst die Sicherung der Möglichkeit der Datenrückhaltung, der Verkaufs- oder Nutzungsweigerung seitens der Kund\*innen durch eine Regelung wie einen Kontrahierungzwang verändert die realen Machtverhältnisse, ansonsten ist die Datenabtretung durch den Einzelnutzer normaler Teil aller digitalen Kommunikation – die jetzige Situation, dass die Daten bei den Unternehmen verbleiben, würde sich auch dann ergeben. Es kann mithin sein, dass auch ein radikales Dateneigentum auf Seiten der Verbraucher\*innen und Bürger\*innen an den Machtasymmetrien nichts ändern kann.

Andererseits ist das Fehlen eines konsistenten rechtlichen Rahmens für die Digitalisierung als Defizit staatlichen Handelns anzusehen, ist es doch eine traditionelle, selbst in strikt marktwirtschaftlichen Modellen befürwortete Aufgabe des Staates, eine rechtliche Infrastruktur für Markthandeln zu setzen. Zwar mag aktuell

die fehlende rechtliche Grundlagenklärung dazu beitragen, die Digitalisierung eher zu beschleunigen, also ökonomisch funktional zu sein, dies kann aber nur eine Momentaufnahme bei grundsätzlich rein positiver Beurteilung der Digitalisierung darstellen, denn ein dauerhafter Verzicht auf rechtliche Regelung schafft angesichts der offensichtlichen Interessendifferenzen Rechtsunsicherheit und eine Situation, in der durch Privatrechtsverträge und Allgemeine Geschäftsbedingungen die Regeln der Kommunikation und des wirtschaftlichen Austausches von den jeweils mächtigsten Akteuren weitestgehend einseitig gesetzt werden können. Sollten resultierende Rechtsunsicherheiten und der Verzicht auf eine alle Interessen einbeziehende Rechtsklärung in einem derart gesellschaftsbestimmenden Bereich wie der Digitalisierung dauerhaft fortexistieren, würde dies die *Rechtsstaatlichkeit* als Kernmerkmal öffentlichen Handelns in Frage stellen.

---

## Literatur

- Bundesministerium für Verkehr und digitale Infrastruktur (BMVI). 2018. „*Eigentumsordnung“ für Mobilitätsdaten? Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive*. Berlin: BMVI.
- Europäische Union. 2018. Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union. Straßburg: Amtsblatt der Europäischen Union. <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018R1807&from=EN>. Zugegriffen am 21.10.2019.
- European Commission. 2018. Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability. Final report (A study prepared for the European Commission DG Communications Networks, Content & Technology by Deloitte). Brüssel: European Commission. <https://ec.europa.eu/digital-single-market/en/news/study-emerging-issues-data-ownership-interoperability-re-usability-and-access-data-and>. Zugegriffen am 21.10.2019.
- Fezer, Karl-Heinz. 2018. Repräsentatives Dateneigentum. Ein zivilgesellschaftliches Bürgerrecht. Sankt-Augustin: Konrad-Adenauer-Stiftung [leicht verändert als: 2019: Digitales Dateneigentum – Ein grundrechtsdemokratisches Bürgerrecht in der Zivilgesellschaft. In *Dateneigentum und Datenhandel*, Hrsg. Stiftung Datenschutz, 101–160. Berlin: Erich Schmidt].
- Hoeren, Thomas. 2013. Dateneigentum. Versuch einer Anwendung von § 303a StGB im Zivilrecht. *Multimedia und Recht* 16(8): 486–491.
- Jöns, Johanna. 2016. *Daten als Handelsware*. Hamburg: Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI).
- Lanier, Jaron. 2014. *Wem gehört die Zukunft? Du bist nicht der Kunde der Internet-Konzerne. Du bist ihr Produkt*, 3. Aufl. Hamburg: Hoffmann und Campe.
- Pierson, Christopher. 2013. *Just property. A history in the Latin West*, Bd. I. Oxford: Oxford University Press.
- Pierson, Christopher. 2016. *Just property. A history in the Latin West*, Bd. II. Oxford: Oxford University Press.
- Scassa, Teresa. 2018. Data ownership. CIGI paper no. 187. Waterloo: Centre for International Governance Innovation. <https://www.cigionline.org/publications/data-ownership>. Zugegriffen am 21.10.2019.
- Schütze, Benjamin, Stefanie Hänel, und Nikolaus Forgó. 2018. Big Data – Eine informationsrechtliche Annäherung. In *Big Data und Gesellschaft. Eine multidisziplinäre Annäherung*, Hrsg. Barbara Kolany-Raiser et al., 233–308. Wiesbaden: Springer.
- Smart-Data-Begleitforschung, Hrsg. 2017. *Daten als Wirtschaftsgut. Europäische Datenökonomie oder Rechte an Daten?* Berlin: Smart Data.
- Stiftung Datenschutz, Hrsg. 2019. *Dateneigentum und Datenhandel*. Berlin: Erich Schmidt.

---

## **Teil IV**

### **Demokratisches Regieren**



---

# E-Democracy

Marianne Kneuer

## Inhalt

1 Klärung des Begriffs .....	268
2 Theoretische Grundlagen .....	271
3 Praktische Anwendung .....	273
4 Künftige Entwicklung .....	276
Literatur .....	276

---

## Zusammenfassung

Das Konzept von *E-Democracy* basiert auf der Grundidee, dass mit Hilfe der digitalen Technologie demokratische Strukturen, Prozesse und Inhalte verbessert werden und somit vorhandene Legitimationsprobleme der repräsentativen Demokratie gelöst werden können. Der von Euphorie getragenen Debatte der ersten Jahrzehnte stehen in den letzten Jahren allerdings zunehmend skeptische Stimmen gegenüber. Diese normativen Ausschläge in beide Richtungen verstellen nicht selten einen netzrealistischen Blick auf den Untersuchungsgegenstand. Umgesetzt finden sich mittlerweile vor allem zwei Varianten von *E-Democracy*: fortgeschrittene hybride Modelle, bei denen *online*- und *offline*-Prozesse (fast) gleichberechtigt existieren (Estland, Finnland, Vereiniges Königreich) oder – und dies sind die meisten Fälle – die Übernahme elektronischer *Tools* als Ergänzung repräsentativ-demokratischer Prozesse.

---

## Schlüsselwörter

E-government · E-participation · Netzoptimismus · Netzessimismus ·  
Netzrealismus · Demokratiebelebung

---

M. Kneuer (✉)

Institut für Sozialwissenschaften, Universität Hildesheim, Hildesheim, Deutschland  
E-Mail: [kneuer@uni-hildesheim.de](mailto:kneuer@uni-hildesheim.de)

## 1 Klärung des Begriffs

So wie Digitalisierung auf alle Lebensbereiche einwirkt, gilt dies auch für die demokratischen Strukturen, Prozesse und Akteure. Die Effekte bestehen zum einen in der quantitativen Vervielfachung der Kanäle politischer Kommunikation, zum anderen qualitativ in neuen Arrangements der Interaktion zwischen politischen Akteuren, gesellschaftlichen Gruppen und Bürgern (und zwar sowohl horizontal – Bürger zu Bürger – als auch vertikal – Bürger zu Politiker und Politiker zu Bürger). Insofern Politik und insbesondere Demokratie als kommunikativer Prozess verstanden wird, bei dem öffentliche Meinungsbildung, Verständigungs- und Aushandlungsprozesse zwischen den politischen Eliten, gesellschaftlichen Akteuren und der Bevölkerung kommunikativ basiert und legitimiert sind, rücken neue Möglichkeiten in den Blick: für Bürger bei der Informationsgewinnung, Zustimmung zu und Teilhabe an Politik; für die politischen Akteure bei der Adressierung der Bürger und dem Austausch mit ihnen.

In der Politik- und Verwaltungswissenschaft beschäftigen sich Vertreterinnen und Vertreter u. a. mit der Infrastruktur digitaler Medien, ihren Funktionslogiken, den diskursiven Dimensionen der unterschiedlichen Plattformen, vor allem aber mit ihrem demokratietheoretischen Potenzial oder den politischen Implikationen und Effekten digitaler Kommunikation. Terminologisch herrscht Vielfalt: „Cyberdemocracy“, „digitale Demokratie“ oder „elektronische Demokratie“ werden synonym verwendet. Ausgangspunkt des Konzepts von „E-Democracy“ sind in jeder Hinsicht verbesserte demokratische Prozesse: besseres Regieren, bessere Teilhabe der Bürger, bessere Kommunikation zwischen Regierten und Regierenden. Zugleich lässt sich *E-Democracy* in verschiedene Bereiche ausdifferenzieren.

Drei Konzepte sind in Forschung und Praxis vor allem präsent und relevant: *E-Democracy*, *E-Government* und *E-Participation*. Konsens besteht in der Literatur darüber, dass *E-Government* ein dienstleistungsorientiertes *Top-down*-Konzept verkörpert, das zuvorderst auf erhöhte Effizienz und Kostensenkung ausgerichtet ist. Die ‚klassische‘ Speyerer Definition (Reinermann und von Lucke 2002) versteht *E-Government* als Abwicklung geschäftlicher Prozesse im Zusammenhang mit Regieren und Verwalten mit Hilfe von Informations- und Kommunikationstechniken über elektronische Medien, inkludiert dann aber neben Exekutive auch Legislative und Judikative. Anders und konsistenter bezieht die OECD *E-Government* allein auf die Exekutive. Ähnlich spiegelte sich in der Enquete-Kommission „Internet und digitale Gesellschaft“ des Bundestages die Trennung in E-Parlament (Legislative), *E-Government* (Exekutive) und E-Justiz (Judikative) unter dem Dach von *E-Democracy* wider.

Im *E-Government*-Konzept wird dem Bürger eine Rolle als Verbraucher zugeschrieben, dem eine bürgerfreundliche Verwaltungsleistung in Form von *Online*-Abwicklung behördlicher Vorgänge (bei der Steuererklärung, der Kfz-Anmeldung etc.) ermöglicht werden soll. Die Leistung des Netzes wird insofern weniger im Sinne demokratiebelebender Aspekte gesehen, vielmehr ist das Ziel die effektivere und dezentrale Bearbeitung von Dienstleistungen und Problemen. Dennoch kann durch *E-Government* erhöhte Transparenz und somit eine Stärkung der Zufrieden-

heit von Bürgern mit staatlichen Dienstleistungen erreicht werden. Damit sind zwei wichtige Aspekte zur Festigung von Legitimität anvisiert. Die OECD etwa unterstreicht explizit die Komponente der Vertrauensbildung zwischen Bürgern und Staat, insofern der Staat zu mehr Offenheit und Rechenschaftspflicht angehalten wird sowie die Vermeidung bzw. Verringerung von Korruption. Insgesamt birgt *E-Government* daher, auch wenn es eher ein effizienz- und serviceorientiertes Konzept darstellt, das Potenzial, die Performanzdimension von *E-Democracy* zu stützen (im Sinne einer Verbesserung der politischen Ergebnisse) und somit die Legitimität des Staates (im Sinne der *Output*-Legitimität) zu fördern. Auf Grund dieses Wirkungszusammenhangs ist bei *E-Government* durchaus ein demokratierelevantes Moment enthalten.

*E-Participation* ist davon analytisch insofern zu trennen, als dieses Konzept im Gegensatz zu dem reinen *top-down*-Ansatz von *E-Government* beide Interaktionsrichtungen enthält: Sowohl *top-down* in Form von Beteiligungsangeboten der Regierung an die Bürger als auch im Sinne von Teilhabeaktivitäten, die von den Bürgern selbst ausgehen (*bottom up*) (siehe dazu Coleman/Blumler 2009). Diese Doppelgesichtigkeit von *E-Participation* birgt demokratietheoretisch gesehen einen Widerspruch, denn demnach stellt Partizipation grundsätzlich einen *bottom-up*-Prozess dar, bei dem Bürger am politischen Willensbildungs- und Entscheidungsprozess teilnehmen und dort einen *Input* einspeisen. Der Ansatz, dass *E-Participation* auch von Regierungen genutzt werden kann, um Bürgern entsprechende Angebote zu machen – wie etwa Plattformen zur Deliberation oder Konsultation politischer Projekte oder Lösungsvorschläge – erscheint daher als eine *contradiccio in adiecto*.

Diese Doppelgesichtigkeit von *E-Participation* ist darauf zurückzuführen, dass Regierungen auf den Reformbedarf der kommunikativen Arrangements zwischen staatlichen Akteuren und Bürgern – oft auch von letzteren eingefordert – reagieren und daher Initiativen entstehen, die von staatlichen Stellen und Akteuren initiiert, finanziert und gepflegt werden. Auch wenn dies weiterhin als Regierungskommunikation zu werten ist, birgt die elektronische Variante – anders in der analogen Welt – die Möglichkeiten des interaktiven Austauschs. So ergibt sich das Nebeneinander von institutionell gestalteter und verwalteter öffentlicher Diskussion, während die *bottom-up*-Variante als autonome Interaktion jenseits des Staats, zwischen und innerhalb von Öffentlichkeiten und Gegenöffentlichkeiten bestimmt wird. Beide Varianten basieren gleichermaßen darauf, dass Bürger mit neuen demokratischen Gelegenheiten der Teilhabe und Mitsprache ausgestattet sind. Ebenso lassen sich die demokratietheoretischen Erwartungen, die sich mit *E-Participation* verbinden, auf beide Varianten beziehen: Mehr Bürger und vor allem mehr bislang marginalisierte Bürger sollen in den öffentlichen Diskurs und in die Entscheidungsprozesse einbezogen werden können, Willensbildung und Entscheidungen sollen inklusiver gestaltet und damit demokratische Prozesse auf eine breitere Legitimationsbasis gestellt werden.

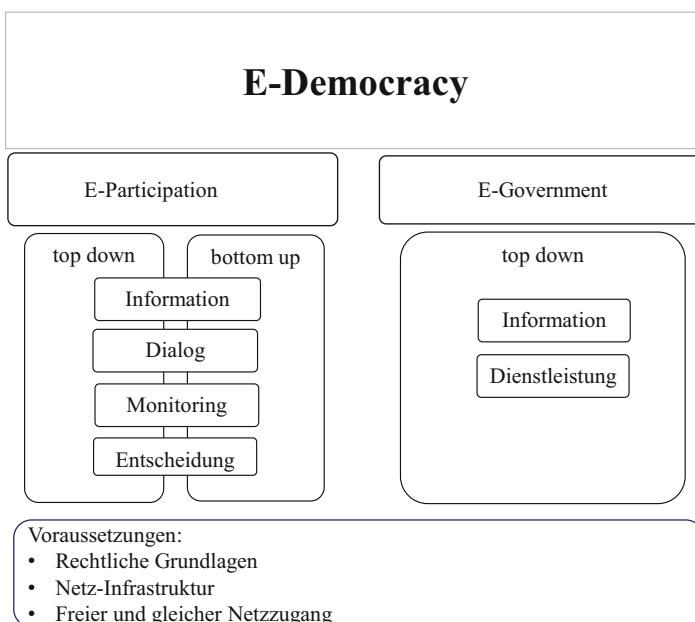
Man kann die drei Konzepte miteinander in eine Beziehung setzen, indem *E-Democracy* als übergeordneter Begriff gilt, unter den sich *E-Participation* und *E-Government* subsumieren lassen, wenngleich analytisch getrennt (Kneuer 2016). *E-Democracy* umfasst demnach Aktivitäten aller im politischen Prozess potenziell

eingebundenen Akteure (*top-down* wie *bottom-up*), die das Verhältnis zwischen Staat und Bürger im Sinne einer Verbesserung demokratischer Prozesse verändern, wobei sowohl die Interpretation der Verbesserung als auch der Grad der möglichen Veränderung wiederum von den normativen Grundannahmen abhängen (Abb. 1).

Eingeschlossen in dieses Modell von *E-Democracy* sind zwei grundlegende Voraussetzungen, nämlich der freie und gleiche Netzzugang, einmal im technischen Sinne als Zugang zur Netzinfrastruktur und zum anderen die rechtlichen Grundlagen, die sich auf die Internetfreiheit und die inhaltliche Regulierung (*content regulation*) beziehen.

In Bezug auf die Funktionen von *E-Participation* werden gemeinhin Information, Dialog und Teilhabe an Entscheidungen als grundlegende Charakteristika *online*-basierter Tools ausgemacht. Hinzugefügt werden kann des Weiteren die Monitoring-Funktion, insofern Bürger über soziale Medien nicht nur bessere Kenntnis über mögliche Missstände oder Fehlentwicklungen erlangen können, sondern auch eine stärkere Stimme haben, um „Alarm zu schlagen“.

Zusammengefasst: Das Konzept von *E-Democracy* basiert auf der Grundidee, dass mit Hilfe der digitalen Technologie die demokratischen Strukturen, Prozesse und Inhalte verbessert werden können. Der von Euphorie getragenen Debatte der 1990er-Jahre stehen in den letzten Jahren zunehmend skeptische Stimmen gegenüber. Es lassen sich Konjunkturen bestimmter Positionen in diesen Debatten ausmachen, die im nächsten Kapitel kurz umrissen und diskutiert werden.



**Abb. 1** Konzept von *E-Democracy* (vgl. Kneuer 2016, S. 672)

## 2 Theoretische Grundlagen

Im Bereich *E-Democracy* folgen Forschungswellen sehr viel rascher aufeinander und überlappen sich demzufolge. So verkörperte die akademische Debatte bei der Emergenz des Internets Anfang der 1990er einen überwiegend netzoptimistischen Ansatz, der auf das enorme Potenzial des neuen Mediums abstellte für die Verbesserung demokratischer Prinzipien wie etwa Partizipation, Deliberation und Inklusion (zu den Debattensträngen und ihrer Einordnung ausführlich: Kneuer und Salzborn (2016); Wilhelm (2000)). Das Modell digitaler Demokratie implizierte vor allem eine Neukonfiguration politischen Einflusses bzw. Macht – auch im Sinne von Kommunikationsmacht –, wobei insbesondere dem Bürger eine veränderte Rolle zugesucht wurde in neuen Bürgerschaftsmodellen wie „participatory citizenship“, „deliberative citizenship“ oder „monitorial citizenship“. Die stark normativ geprägten Überlegungen gingen von der Verwirklichung bislang nur theoretisch gedachter Möglichkeiten aus: Die elektronische *agora* stellte eine dieser durchaus euphorischen Ideenkonstrukte dar. Demokratietheoretische Hoffnungen basierten zum einen auf besseren Zugangschancen zur Meinungsbildung; mehr Bürger und vor allem mehr marginalisierte Bürger sollten in den öffentlichen Diskurs und in die Entscheidungsprozesse einbezogen werden können, letztere sollten demokratischer gestaltet und zudem auf eine breitere Legitimationsbasis gestellt werden. Erwartungen richteten sich, zweitens, auf die Ergänzung repräsentativer Verfahren durch deliberative oder direktdemokratische Verfahren. Oder es würde gar das Ersetzen repräsentativer Verfahren durch eine bürgerliche Selbstregierung erhofft, die mithilfe des Netzes möglich werden könnte. Dabei kam der aktiven und aktivierenden Zivilgesellschaft eine gewichtige Rolle zu. Das Internet solle, so die Mobilisierungsthese etwa von Rheingold (1993), zu basisdemokratischem politischen Aktivismus führen. Der entscheidende Beitrag des Internets aber wurde, drittens, in der Verwirklichung alternativer Partizipationsmöglichkeiten auf elektronischem Wege gesehen wie E-Wahlen, E-Petitionen und E-Referenda.

Mit dem Aufkommen der Web 2.0-Technologie bekam die Debatte um die Vitalisierung, Modernisierung oder Reform der repräsentativen Demokratie neue Nahrung: Die Dynamik der technischen Entwicklung (*social software*, drahtlose Netzwerke, internetfähige Mobiltelefone) und die rasche Penetration durch neue Formen der Vernetzung bringen neue und umfassende Möglichkeiten der Bürgerteilhabe ins Spiel. Web 2.0 beinhaltet in Form von sozialen Netzwerken wie *Facebook* oder *Microblogging*-Diensten wie *Twitter* neue technische Möglichkeiten interaktiver *many-to-many*-Echtzeitkommunikation, (transnationale) Vernetzung, multimodale (Wort/Ton/Bild) Formate und Verlinkung. Zudem ist eine neue Rolle entstanden, nämlich der „Bürgerjournalist“ oder „produser“, ein Nutzer, der selbst Inhalte generiert und verbreitet.

Die netzoptimistische Welle fand ihren vorläufigen Höhepunkt und ihre Bestätigung, als die mobilisierende Kraft sozialer Plattformen bei den Umstürzen in Tunesien, Ägypten und anderen arabischen Diktaturen sichtbar wurde. Die Aufstände in der arabischen Region, auch Beispiele wie die *Acampada*- und *Occupy*-Bewegung

oder andere Bewegungen sozialen Protestes haben verdeutlicht, dass die Wirkmächtigkeit weit über die schlichte Kommunikation hinausgeht, sondern soziale Medien eine wichtige Rolle bei der Organisation und Mobilisierung von Kampagnen und Protesten spielen. Mancher sah – freilich voreilig – im Internet eine Befreiungstechnologie. Die so genannten „Facebook-Revolutionen“ selbst, aber auch die von ihnen inspirierten Protestbewegungen wie *Democracia Ya* in Spanien, *Occupy*, Gezi-Park, die Regenbogen-Proteste in Hongkong etc. wurden auf Grund ihrer neuartigen und intensiven Nutzung sozialer Plattformen zu einem intensiv bearbeiteten Forschungsgegenstand. Überwiegender Konsens bestand – auch in dieser Literatur – in einer dezidiert positiven Sicht auf die veränderten Möglichkeiten vernetzten und *online*-basierten Protests, insofern autonome Räume der Kommunikation jenseits der Kontrolle von Regierungen und Konzernen gewonnen werden konnten (Castells 2012).

Bereits vor dieser letzten Konjunktur der netzoptimistischen Interpretation hatten sich aber ernüchternde Stimmen erhoben, die eher einer netz pessimistischen Richtung zuzuordnen waren (in den 2000ern gleichwohl noch in der Minderheit). So wurde der Mobilisierungsthese die Verstärkerthese entgegengesetzt, die davon ausging, dass sich im Netz lediglich die bereits in der *Offline*-Welt vorhandenen Muster von Partizipation und Deliberation spiegeln würden (Margolis und Resnick 2000). Des Weiteren wurde darauf verwiesen, dass die ungeheure Zunahme an Informationskanälen und ungefilterten Daten zu einer Überflutung und zugleich Überforderung der Bürger führen könne. Die als Vorteil verbuchte Tatsache, dass die Journalisten als *Gatekeeper* in den Massenmedien umgangen und stattdessen die Informationen direkt abgerufen werden können, würde so zum Nachteil, denn ohne die Fähigkeiten zur Einordnung (z. B. Relevanz, Priorisierung von Informationen) und Orientierung (z. B. Vertrauenswürdigkeit der Quelle) ist es schwierig, mit der Informationsmenge sinnvoll umzugehen. Als zentraler Aspekt der Debatte kristallisierte sich die Kritik an der Idee deliberativer Demokratieverstellungen heraus. Den Argumenten der Netzoptimisten, die eine Herstellung von Öffentlichkeit durch elektronische Deliberation erwarteten, wurde entgegen gehalten, dass das Internet eher zu einer Fragmentierung oder gar zur Erosion der öffentlichen Sphäre führe (Buchstein 1996; Dahlgren 2009). Diese Warnungen gingen zudem einher mit der kritischen Betrachtung des Potenzials zur gesteigerten Inklusion und Beteiligung von Bürgern. Ganz anders könnten bestimmte Nutzerprofile zementiert werden, die tatsächlich für die Herausbildung einer überlegenen politischen Informationselite gegenüber einer gleichbleibend breiten Mehrheit an schlechter informierten Bürgern und zudem einer Exklusion von bestimmten Bevölkerungsteilen sprechen (Hindman 2009).

Gleichzeitig bildete sich ein weiterer Forschungsstrang heraus, der sich als netzrealistisch versteht und einen Ansatz verfolgt, der einen neuen Weg zur kritischen Betrachtung der Technologie gehen und dabei den „fruchtbaren Mittelweg zwischen den extremen Visionen des technologischen Potenzials“ aufzeigen will (Wilhelm 2000, S. 22). Ausgangspunkt war dabei anfänglich vor allem die Frage nach der Wirkung digitaler Technologie auf Verwirklichung von Werten. Als problematisch stellte sich dabei heraus, dass weitgehend unklar blieb, an welchen Prinzipien oder Kriterien und an welchem Werten man sich orientierte. Konkretere Vorschläge zielen darauf ab, dass die ambivalente Wirkung digitaler Medien von mehreren

Faktoren abhängt: den Nutzern, ihren übermittelten Botschaften und der Art der Nutzung (Was wird wie kommuniziert?), den Nutzungsmotiven und -zielen (Warum wird mit welchem Ziel kommuniziert?) sowie dem politisch-institutionellen und dem sozialen Kontext, in dem sie agieren. Barber etwa machte die Richtung der Wirkung des Netzes auf demokratische Prozesse – also: bereichernd oder unterminierend – abhängig von der Qualität der vorhandenen Institutionen und „dem Charakter der Bürger“ (Barber 1998, S. 131 f.). Weitere Konkretisierungen des netzrealistischen Ansatzes postulieren klare Kriterien für demokratiehinderliche oder -fördernde Wirkungen. So stellt Kneuer darauf ab, dass eine die Demokratiequalität stärkende oder mindernde Wirkung an zentralen demokratischen Prinzipien wie Repräsentation, Partizipation, Responsivität und Inklusion gemessen werden müssen (2013). Ein anderer Ansatz orientiert sich an den Dahlschen Vorstellungen der „dritten Transformation von Demokratie“: a) Verfügbarkeit von und der Zugang zu bestmöglicher Information, b) leichte und universell zugängliche Gelegenheiten für alle Bürger, c) Einfluss auf die politische Agenda, und d) maßgebliche Teilhabe an politischen Diskussionen (Kneuer 2016; Kneuer und Salzborn 2016, S. 4 f.). Kern des netzrealistischen Ansatzes ist es, für eine Analyse und Abwägung demokratieförderlicher und -hinderlicher Effekte einzutreten und die Ambivalenzen aufzuzeigen, ohne dabei, wie es in Bezug auf soziale Medien in den letzten Jahren zu beobachten war, in Euphorie oder Verteufelung des Mediums zu verfallen.

Gerade in jüngster Zeit verdichtete sich die stark netzessimistische Haltung angesichts von regierungsgesteuerten *social bots*, Manipulation von Information, Propaganda, Intervention in Wahlen, Inzivilität in der Debattenkultur (*hate speech*) bis hin zu kriminellen Aktivitäten. Auch wenn der politikwissenschaftlichen Forschung noch sehr viel weitgehendere Befunde zu einzelnen Aspekten der Interaktionsmechanismen zwischen politischen Akteuren und Bürgern (und damit letztlich auch zur demokratiefördernden oder -schädigenden Wirkung sozialer Medien) fehlen, kann zweifelsohne konstatiert werden, dass die starke normative Aufladung der Debatten – in die eine oder andere Richtung – den Blick für etliche Entwicklungs-perspektiven (negative wie positive) bislang verstellt hat. So sind weder Propaganda noch Informationsmanipulation etwas Neues; es sind die technischen Attribute der Beschleunigung, die Skalierbarkeit, der Entmenschlichung (durch *Bots*) und der Ubiquität, die dem Phänomen seine neue Brisanz verleihen. Ernst zunehmende Sorgen von Praktikern wie Wissenschaftler beziehen sich auf die Datensicherheit und den Umgang mit Daten. Hier ist die Anwendungsebene von *E-Democracy* betroffen, insofern Datensicherheit eine Voraussetzung sowohl für Anbieter als auch für Nutzer digitaler *Tools* ist.

---

### 3 Praktische Anwendung

Praktische Anwendung im Bereich *E-Democracy* umfasst die Angebots- und Nutzungsseite; im Rückgriff auf das zuvor vorgestellte Modell geht es somit einerseits um regierungsgestützte Angebote oder *bottom-up*-Aktivitäten und andererseits um die Nutzung der Angebote durch die Bürger. Dabei können *E-Democracy-tools* auf

allen Ebenen installiert und präsent sein – nicht nur national, sondern auch auf subnationaler Ebene und im lokalen Bereich (Kommunen, Städte). Bei der *E-Participation* kann – neben der Richtung: *top-down* oder *bottom-up* – zwischen den jeweils genutzten Interaktionsformen unterschieden werden: Information, Dialog (*consultation*) und Entscheidung (*decision-making*). Während es bei den *bottom-up*-Aktivitäten eine große Vielzahl an unterschiedlichsten Aktivitäten gibt – von der *Online*-Handlungen individueller Bürger bis hin zu organisierten Kampagne und *online*-gestützten Protestbewegungen –, die in ihrer Gesamtheit nur schwer zu quantifizieren sind, sind die regierungsgestützten Angebote gut zu überblicken. Diese lassen sich an Hand des *UN E-Government Survey* seit 2003 messen. Dabei sind mehrere Trends erkennbar:

Erstens ist eine – kaum überraschende – Sequenzierung bei der Implementierung der Interaktionsform erkennbar. So implementieren Regierungen meist zuerst E-Information, während sie sich der Umsetzung von *E-Consultation* deutlich später zuwenden, und noch später erst *E-Decision-Making Tools*. So ermutigten zwar viele Länder zu Partizipation, aber stellten nur wenige relevante und qualitätsvolle Mechanismen mit *Feedback*-Möglichkeit für Nutzer zur Verfügung. Während der Anteil der Länder, die bereits 2005 E-Information einsetzten, je nach *Tool* bei 40 bis 50 Prozent lagen, waren es nur 13 Prozent, die Konsultation ermöglichten; und noch stärker reduziert präsentierte sich die Angebote zur Entscheidungsfindung: Acht Prozent der Länder boten *Online*-Petitionen an, 16 Prozent der Regierungen deuteten an, dass sie den *Input* der Bürger in ihre Entscheidungen mit einbeziehen.

Die asymmetrische Verteilung der drei Interaktionsformen setzt sich, zweitens, bis heute fort, wenngleich – und dies bestätigt die Sequenzierungslogik – die Installierung von Konsultationsinstrumenten stark ‚aufgeholt‘ hat. Weiterhin bleibt aber *E-Decision-Making* die am wenigsten angebotene Form.

Wenig überraschend ist drittens eine erhebliche Dynamik in Bezug auf alle drei Bereiche – Information, Konsultation und Entscheidung – festzustellen. Fast alle Länder (95 Prozent) stellen in den untersuchten Kernbereichen Informationen zur Verfügung. Die stark angestiegene Präsenz an sozialen Medien im letzten Jahrzehnt bewirkte insbesondere eine Beschleunigung im Bereich der Konsultationsinstrumente. Allein von 2014 zu 2016 vollzog sich ein enormer Sprung. In diesem kurzen Zeitraum haben Regierungen ihr Angebot an Konsultationsinstrumenten fast verdoppelt. Bei *E-Decision-Making* ist nur ein leichter Anstieg erkennbar.

Ein vierter Trend besteht darin, dass regionale Differenzen zwar weiterhin bestehen, sich aber deutlich verringert haben – zumindest im Bereich Information und Konsultation. Das Einkommensniveau eines Landes beeinflusst zwar weiterhin die Intensität des Angebots, aber nicht mehr die Bereitschaft und das Angebot der Regierungen; so existieren in mehr als der Hälfte der *low income*-Länder Konsultationsinstrumente. Zudem zeigt sich eine besondere Dynamik bei den Ländern mit mittleren Einkommensniveaus, die in den letzten Jahren in die *E-Participation*-Spitzengruppe vorgedrungen sind wie etwa China, Mexico, Ukraine, Marokko (United Nations 2016) (Tab. 1).

**Tab 1** E-Participation-Index (EPI) nach Ländergruppen und digitalen Instrumenten

	Sehr hoher EPI (31 Länder)	Hoher EPI (59 Länder)	Mittlerer EPI (52 Länder)	Niedriger EPI (51 Länder)
<b>E-Information</b>	92,1 %	75,8 %	49,8 %	19,2 %
<b>E-Consultation</b>	89,1 %	60,9 %	29,0 %	8,9 %
<b>E-Decision-Making</b>	54,4 %	10,7 %	3,0 %	0,3 %

Eigene Darstellung auf der Grundlage der UN E-Government Survey 2016, S. 72

Diese Zahlen geben freilich keine Auskunft über zwei wichtige Aspekte: zum einen die Qualität der Angebote sowie zum anderen die tatsächliche Nutzung durch die Bürger. Breite systematische Studien gibt es dazu nicht; es liegen gleichwohl einige vertiefte Analysen von *best-practice*-Beispielen vor. So ermöglicht im quasi vollständig digitalisierten Finnland der 2012 eingeführte „New Citizen Initiative Act“ den Bürgern über *Crowdsourcing* direktdemokratische Beteiligung an Gesetzesvorhaben: entweder als Petition, um ein bestehendes Gesetz zu ändern oder ein gänzlich neues Gesetz vorzuschlagen. Von 2012 bis 2015 gab es neun erfolgreiche Initiativen, die an das Parlament geleitet wurden – eine Initiative wurde sogar zum Gesetz. Inhalt war die Einführung der Ehe gleichgeschlechtlicher Paare. Tatsächlich zeigte sich eine hohe Mobilisierung (120.000 Unterschriften in 24 Stunden). Neben dem positiven Ergebnis, dass das Instrument erfolgreich genutzt wurde, lautete die eher kritische Einschätzung, dass die Mobilisierung und Involvierung kein repräsentatives Bild der Bevölkerung spiegelte. Es hatten sich vor allem gut gebildete Männer in urbanem Umfeld beteiligt. Zudem gab es eine Überrepräsentation der 21–40-Jährigen. Eine nachteilige Wirkung bezieht sich somit darauf, dass nur bestimmte Segmente der Gesellschaft mit den *Tools* erreicht werden und diese nutzen.

Dieses Beispiel weist auf einige dysfunktionale Effekte selbst bei sehr umfassend konstruierten und ausgefeilten Konsultations- und Entscheidungsinstrumenten hin: Erstens, erreichen *online*-basierte Demokratieinnovationen eher eine ohnehin schon aktive und interessierte Gruppe und nicht die breite Masse. Somit wird, zweitens, Beteiligung eher nicht erhöht. Die Ambivalenz dieser Instrumente liegt daher darin, dass sie einerseits eine stärkere Inklusion von Bürgern anstreben, was zugleich eine höherwertige Involvierung der Bürger erfordert; andererseits aber die tatsächliche Beteiligung niedrig und/oder selektiv bleibt. So nahmen an einem anderen finnischen *Crowdsourcing*-Verfahren des Parlaments, bei dem die Bevölkerung explizit aufgerufen wurde, sich an der Diskussion über und der Formulierung des Gesetzes (*off-road traffic*) zu beteiligen, nur etwa 700 Bürger teil.

Diese Beispiele decken sich mit den Befunden zur Nutzerseite in Bezug auf Information, Dialog und Entscheidungsbeteiligung. So ist die Informationsgewinnung im Internet überwiegend interessens- und ereignisgetrieben. Hinsichtlich Konsultation und Entscheidung werden Nutzungsformen mit hohen Nutzerzahlen bei geringem Zeitaufwand (*Online*-Petitionen zeichnen, politische Sachverhalte abstimmen) solchen Nutzungsformen vorgezogen, für die Nutzer viel Zeit aufwenden müssen (über Bürgerhaushalte beraten, an *Online*-Konsultationen teilnehmen, *Online*-Petitionen erstellen).

## 4 Künftige Entwicklung

Das Forschungsfeld *E-Democracy* hat, so jung es einerseits ist, in den letzten Jahrzehnten eine ungeheure Dynamik entfaltet. Das trifft auf die theoretischen Debattenstrände ebenso zu wie auf die inzwischen schwer übersehbare Menge an empirischen Studien. Dennoch bedürfen etliche Aspekte ohne jeden Zweifel weiterer Erforschung, denn die Forschungsgegenstände unterliegen einer ungleich höheren Dynamik, insofern sie zwangsläufig der gleichermaßen hochdynamischen technischen Entwicklung folgen.

*E-Democracy* ist ein Modell, mit dem die Erwartung verbunden wurde und teils noch wird, vorhandene Legitimationsprobleme der repräsentativen Demokratie zu lösen. Die Vorstellung jedoch, allein die Existenz neuer technischer Wege sei dazu in der Lage, Defizite oder Fehlentwicklungen repräsentativer Demokratie zu beheben, war von Anfang an naiv. Gleichwohl können *E-Democracy-Tools* unter bestimmten Bedingungen eine gelungene Ergänzung zu *offline*-Prozessen bieten. Künftige Forschung müsste sich daher insbesondere mit den Bedingungen beschäftigen, unter denen sich *offline*- und *online*-Prozesse sinnvoll und komplementär umsetzen lassen. Hier liegt ein praktisch-politisches Potenzial und zugleich erheblicher wissenschaftlicher Analysebedarf.

---

## Literatur

- Barber, Benjamin R. 1998. Wie demokratisch ist das Internet? In *Internet & Politik. Von der Zuschauer- zur Beteiligungsdemokratie*, Hrsg. Claus Leggewie und Christa Maar, 120–133. Köln: Böllmann.
- Buchstein, Hubertus. 1996. Bittere Bytes. Cyberbürger und Demokratietheorie. *Deutsche Zeitschrift für Philosophie* 44(4): 583–608.
- Castells, Manuel. 2012. *Networks of outrage and hope. Social movements in the internet age*. Cambridge: Polity Press.
- Coleman, Stephen, Blumler, Jay G. 2009. *The internet and democratic citizenship. Theory, practice and policy*. Cambridge: Cambridge University Press.
- Dahlgren, Peter. 2009. *Media and political engagement. Citizens, communication, and democracy*. Cambridge: Cambridge University Press.
- Hindman, Matthew. 2009. *The myth of digital democracy*. Princeton: Princeton University Press.
- Kneuer, Marianne, Hrsg. 2013. Bereicherung oder Stressfaktor? Überlegungen zur Wirkung des Internets auf die Demokratie. In *Das Internet. Bereicherung oder Stressfaktor für die Demokratie?* 7–35. Baden-Baden: Nomos.
- Kneuer, Marianne. 2016. E-democracy. A new challenge for measuring democracy. *International Political Science Review* 37(5): 666–678.
- Kneuer, Marianne, und Samuel Salzborn, Hrsg. 2016. *Web 2.0 – Demokratie 3.0. Digitale Medien und ihre Wirkung auf demokratische Prozesse*. Sonderheft der Zeitschrift für Vergleichende Politikwissenschaft. Wiesbaden: Springer.
- Margolis, Michael, und David Resnick. 2000. *Politics as usual. The cyberspace „revolution“*. Thousand Oaks: Sage.

- Reinermann, Heinrich, und Jörn von Lucke, Hrsg. 2002. *E-Government – Gründe und Ziele*. In *Electronic Government in Deutschland. Ziele – Stand – Barrieren – Beispiele – Umsetzung*. Speyerer Forschungsberichte 226, 1–8. Speyer: Forschungsinstitut für öffentliche Verwaltung.
- Rheingold, Howard. 1993. *The Virtual community: Homesteading at the electronic frontier*. Reading: Addison-Wesley.
- United Nations. 2016. *E-government survey* (2001, fortlaufend). <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016>. Zugegriffen am 29.06.2019.
- Wilhelm, Anthony G. 2000. *Democracy in the digital age. Challenges to political life in cyberspace*. New York: Routledge.



---

# Online-Partizipation von Bürgerinnen und Bürgern

Stefan Marschall und Katrin Möltgen-Sicking

## Inhalt

1 Klärung des Begriffs „Online-Partizipation“ .....	280
2 Theoretischer Bezugsrahmen .....	281
3 Praxis der Online-Partizipation .....	283
4 Perspektiven für Staat und Verwaltung .....	287
Literatur .....	288

---

## Zusammenfassung

Die Digitalisierung in Staat und Verwaltung schafft neue Möglichkeiten, Bürgerinnen und Bürger in Entscheidungsprozesse einzubinden. Über Formen von *Online-Partizipation* können politische Entscheidungen stärker legitimiert und auch qualitativ verbessert werden. Wie bisherige Erfahrungen zeigen, sind diesen Möglichkeiten zugleich Grenzen gesetzt – rechtliche, (verwaltungs-)technische, aber auch solche, die die Bereitschaft betreffen, *Online-Partizipation* anzubieten und an ihr teilzunehmen.

---

## Schlüsselwörter

Online-Beteiligung · E-Partizipation · New Public Management · Kooperative Demokratie · Evaluation · Direkte Demokratie · Repräsentative Demokratie

---

S. Marschall (✉)

Institut für Sozialwissenschaften, Heinrich-Heine-Universität Düsseldorf, Düsseldorf, Deutschland  
E-Mail: [stefan.marschall@uni-duesseldorf.de](mailto:stefan.marschall@uni-duesseldorf.de)

K. Möltgen-Sicking

Fachhochschule für öffentliche Verwaltung NRW, Köln, Deutschland  
E-Mail: [katrin.moeltgen@fhoev.nrw.de](mailto:katrin.moeltgen@fhoev.nrw.de)

## 1 Klärung des Begriffs „Online-Partizipation“

Der Begriff *Online*-Partizipation wird sowohl im wissenschaftlichen Diskurs als auch in der Praxis von Staat und Verwaltung nicht einheitlich verwendet. Unterschiedliche Fragestellungen und Zugänge ergeben sich insbesondere aus dem Blickwinkel verschiedener wissenschaftlicher Disziplinen. Zudem können einzelne *Online*-Verfahren nicht immer eindeutig von *Offline*-Verfahren abgegrenzt werden. Schließlich ist die Abgrenzung zu anderen Begriffen nicht immer präzise vorzunehmen.

Im Weiteren liegt der Schwerpunkt auf der politischen entscheidungsbezogenen *Online*-Partizipation (Voss 2014). *Online*-Partizipation als eine Form der politischen Beteiligung, d. h. solcher „Tätigkeiten, die Bürger freiwillig mit dem Ziel unternehmen, Entscheidungen auf den verschiedenen Ebenen des politischen Systems zu beeinflussen“ (Kaase 1992, S. 682), muss somit eine „politische“ Intention haben, d. h. auf allgemein verbindliche Entscheidungen, ihr Zustandekommen oder ihr Ergebnis ausgerichtet sein. Zudem muss sie im Wesentlichen unter Nutzung des Internets erfolgen. Dadurch unterscheidet sie sich von anderen Partizipationsformen, die hauptsächlich analog durchgeführt werden und lediglich durch *Online*-Elemente angereichert werden – hier sollte eher von „augmented participation“ oder „blended participation“ gesprochen werden.

Die Politikwissenschaft vertritt damit ein engeres Verständnis von *Online*-Partizipation. In den Kommunikationswissenschaften werden dagegen nahezu alle Dialogmöglichkeiten über das Internet der „Partizipationskommunikation“ zugeordnet. Die Betriebswirtschaft betrachtet diese dagegen vorrangig aus der internen Managementperspektive und fokussiert auf die Beteiligung der Mitarbeiterinnen und Mitarbeiter („empowerment“).

*Online*-Partizipation wird in der Regel synonym verwendet mit den Begriffen der „elektronischen Partizipation“ bzw. der „E-Partizipation“ sowie der „Online-Beteiligung“. Abzugrenzen ist der Begriff von denen des „E-Government“ und des „Open Government“, die oft in einem Atemzug genannt werden. *E-Government* meint die elektronische Abwicklung von Verwaltungsprozessen, worunter sowohl Prozesse zwischen Verwaltung und Bürgerinnen und Bürgern bzw. Unternehmen zu fassen sind als auch Prozesse zwischen verschiedenen Verwaltungen. Mit dem Begriff des „Open Government“ wird die „Öffnung“ von Regierung und Verwaltung gegenüber der Gesellschaft und innerhalb von Verwaltungsorganisationen beschrieben, wobei das Verhältnis von *Online*-Partizipation und „Open Government“ nicht eindeutig definiert ist. In der Regel wird die *Online*-Partizipation als eine Dimension unter den Begriff des „Open Government“ gefasst. Hinzu kommen die Dimensionen der Transparenz, die wesentlich durch die Bereitstellung „offener Daten“ („Open Data“) erreicht werden soll, und der elektronischen Kooperation mit Bürgerinnen und Bürgern, Wirtschaft und Wissenschaft (Bundesministerium des Innern 2012, S. 27).

*Online*-Partizipation ist somit nicht gleich *Online*-Partizipation. Die unterschiedlichen Varianten lassen sich entlang relevanter Merkmale typologisieren. Eine eher deskriptive Unterscheidung betrifft die Frage, auf welcher Ebene und unter Einbindung welcher potenzieller Teilnehmendengruppe(n) *Online*-Partizipation organisiert wird. Wesentlich für die Wirksamkeit und die Folgen von *Online*-Beteiligung ist

jedoch, mit welcher Verbindlichkeit *Online*-Partizipation in Entscheidungsprozesse integriert ist. Hier gibt es unterschiedliche Grade der Bindeglieder. Eine in der Literatur oft verwendete generelle Systematik partizipativer Verfahren ist die „ladder of citizen participation“ von Arnstein (1969). Diese unterscheidet vier Verfahren nach den folgenden Stufen der Beteiligung, wobei der Einfluss der Betroffenen bzw. der Bürgerinnen und Bürger von Stufe zu Stufe zunimmt: (1) Information, (2) Konsultation, (3) Kooperation, (4) Entscheidung. Diese vier Stufen lassen sich „analog“ auch auf Formen der *Online*-Partizipation übertragen.

Elektronische Partizipation kann zudem auf verschiedenen staatlichen Ebenen stattfinden und sich an unterschiedliche Adressaten richten. Kommunen sind ebenso Adressaten von internetgestützten Partizipationsverfahren wie Bund, Länder und die Europäische Union. Dabei ist nicht nur der politische Bereich im engeren Sinne betroffen, also die Regierungen, Parlamente, Räte, Ausschüsse etc. Die Verwaltung kann in ihrer Funktion als Vorbereiterin und „Administratorin“ politischer Entscheidungen ebenso Adressat politischer *Online*-Partizipation sein. Politische *Online*-Partizipation kann sich somit auf das gesamte *politisch-administrative System* beziehen.

Zudem kann sie alle Phasen des *Policy-Cycle* betreffen, von der Problemdefinition („agenda setting“) über die (Vorbereitung der) Politikdurchführung und die Implementation politischer Programme. Für die Evaluation von Politik können *Online*-Partizipationsformen ebenfalls genutzt werden.

Die Möglichkeit der politischen Beteiligung online auf den verschiedenen staatlichen Ebenen einerseits, in verschiedenen Phasen des Politikzyklus andererseits, ist oft damit verbunden, dass nicht nur Bürgerinnen und Bürger auf diese Weise teilhaben können. Vielmehr können auch Menschen, die nicht Staatsbürgerinnen bzw. Staatsbürger sind, diese Form der politischen Einflussnahme über *Online*-Partizipationsverfahren nutzen, beispielsweise alle Einwohnerinnen und Einwohner einer Stadt oder Gemeinde, die Anwohnerinnen und Anwohner eines städtischen Neubauprojektes o. ä. Dies ist insofern ein wichtiger Aspekt, als dass unverbindliche, freiwillige Partizipationsformen für bestimmte Bevölkerungsgruppen häufig die einzige Möglichkeit bieten, sich politisch einzubringen.

---

## 2 Theoretischer Bezugsrahmen

Die unter dem Begriff „*Online*-Partizipation“ verhandelten neuen technischen Möglichkeiten treffen seit geraumer Zeit auf laufende Veränderungen und Debatten, die unabhängig von den technologischen Entwicklungen stattgefunden haben und immer noch stattfinden, die sich aber mit dem Wandel im Bereich der Informations- und Kommunikationsmedien in Bezug setzen lassen.

Einer dieser Debatten ist diejenige, die unter dem Label „Krise der repräsentativen Demokratie“ läuft. Hierunter versteht man die beobachtbare Abwendung eines Teils der Bürgerschaft von den klassischen politischen Institutionen. Diese Beobachtung ist insbesondere an Entwicklungen bei der konventionellen, also „üblichen“, politischen Partizipation, insbesondere bei der Wahlbeteiligung, festgemacht

worden. Aber auch die Schwierigkeit, in repräsentativen Strukturen gefundene politische Entscheidungen umzusetzen (Beispiel: Stuttgart 21), hat die Defizite in der Qualität und Wahrnehmung repräsentativer Demokratie deutlich gemacht.

Die Digitalisierung trifft aber auch auf eine Debatte über den Wandel in der Verwaltungskultur und -struktur. Verschiedene Reformansätze in den vergangenen Jahrzehnten haben zu einer radikalen Neuaufstellung und einer neuen Philosophie in Verwaltungen geführt. Wichtige Stichworte in dieser Debatte sind Modelle des „new public management“, die eine stärker *output*- und dienstleistungsorientierte Verwaltung zum Ziel haben, sowie das Leitbild „new public governance“, das eine neue Form der Steuerung öffentlichen Handelns verspricht, in der verschiedene staatliche und nicht-staatliche Akteure in den Prozess der Politikformulierung und -umsetzung eingebunden werden. Hier lässt sich *Online*-Partizipation als ein denkbarer Beitrag zur Steigerung der Dienstleistungsqualität der Verwaltung einerseits, zur stärkeren Einbindung von Bürgerinnen und Bürgern in Verwaltungsvorgänge andererseits verstehen. Prozesse einer stärkeren Bürgerorientierung der Tätigkeit der Verwaltungen könnten – so die immer wieder geäußerte Erwartung – durch die technischen Entwicklungen noch beschleunigt werden, zumindest aber effizienter gestaltet werden.

Die Diskussionen über die Chancen und Risiken von *Online*-Partizipation lassen sich also mit generellen Debatten über den Wandel von Staat und Demokratie in komplexen Gesellschaften und den entsprechenden Herausforderungen an die Legitimierung von Entscheidungsfindungsprozessen verbinden. In der Behandlung des Themas kommen unterschiedliche demokratische Modelle und Ansätze zum Tragen: in erster Linie traditionelle partizipative Demokratieverstellungen, die eine hohe quantitative Beteiligung der Bürgerinnen und Bürger als systemrelevant und normativ wünschenswert einstufen – auch innerhalb der Strukturen einer repräsentativen Demokratie. Durch *Online*-Partizipation könne, so die Hoffnung, die *Input*-Legitimation politischer Entscheidungen gesteigert werden, wenn Bürgerinnen und Bürger in ihre Einflussnahme auf politische Entscheidungsprozesse vertrauen (vgl. Kersting 2008, S. 14). Die Verbindungen zu republikanischen Vorstellungen vom aktiven Bürger, der eine wichtige mitgestaltende politische Rolle spielt, liegen auf der Hand. Der Diskurs über *online*-basierte Partizipation steht in Verbindung mit generellen Debatten über die Stärkung partizipativer Elemente in den überwiegend repräsentativen Systemen angesichts einer empirisch festzustellenden gewachsenen Bereitschaft der Bürgerinnen und Bürger, an politischen Entscheidungen mitwirken zu wollen.

Die Debatte um *Online*-Partizipation ist zugleich eingebettet in die breiten Diskussionen über den Wandel von Politik und Öffentlichkeit im digitalen Zeitalter. Schon in den frühen Jahren des Internets ist mit dem „Netz der Netze“ die Hoffnung verknüpft worden, positive Effekte für die Demokratie zu erzeugen. Hier wurde frühzeitig die so genannte Mobilisierungsthese entwickelt; diese vermutet, dass via Internet neue Gruppen an den politischen Prozess herangeführt werden. Demgegenüber stand und steht die Normalisierungs- oder Verstärkungsthese, in der skeptisch vermutet wird, dass neue Beteiligungstechnologien vorwiegend von denjenigen genutzt werden, die sich ohnehin schon stark beteiligen und damit bestehende

Partizipationsklüfte noch vertieft werden. Beide Ansätze gehen freilich gleichermaßen davon aus, dass in einer digitalen Gesellschaft mit mehr Partizipation zu rechnen ist – entweder weil sich mehr Personen engagieren oder weil sich bereits Engagierte noch mehr engagieren.

Ein weiterer Debattenstrang über die Vorzüge von *Online*-Prozessen betrifft die Qualität der jeweiligen Ergebnisse. Eine *online*-basierte erhöhte Beteiligung könnte einen positiven Einfluss auf die Ergebnisse von Entscheidungsprozessen, also den politischen *Output*, haben. Die Logik solcher Ansätze liegt in dem Mechanismus, der als „*wisdom of the crowd*“ bezeichnet wird: d. h., dass die Einbindung von Vielen in laufende Rechtsetzungsverfahren zu einer stärkeren Berücksichtigung der Betroffenenexpertise führt. Hier verbinden sich die *input*-orientierte Partizipationstheorie mit einem *output*-orientierten Legitimationsansatz.

Die frühzeitige Einbindung der Politikbetroffenen im Sinne einer „kooperativen Demokratie“ erleichtert letzten Endes auch die Implementation von Entscheidungen. In der Frage der Umsetzung kommt dann wieder die Verwaltung ins Spiel mit der Vorstellung einer stärkeren Dienstleistungsorientierung, bürgernahen Servicephilosophie und verschiedenen Formen der Beteiligung der Zivilgesellschaft an politisch-administrativen Prozessen. Ebenso wie politische Entscheidungsprozesse geöffnet werden sollen, soll es zu einer Öffnung derjenigen staatlichen Einrichtungen kommen, die für die Umsetzung der Entscheidungen und den Erstkontakt mit den Bürgerinnen und Bürgern Verantwortung tragen. Die Einbindung der Bürgerinnen und Bürger wird hier nicht nur als demokratietheoretisch wünschenswert, sondern auch als funktional im Sinne einer effektiven und effizienten Umsetzung politischer Entscheidungen gesehen.

Sowohl auf der Grundlage der *input*- als auch *output*- sowie implementationsorientierten Ansätze scheint die Erwartung einer zweiten – diesmal digitalen – „partizipatorischen Revolution“ durch. Analog zu der Debatte in den 1970er-Jahren werden ein neuer Beteiligungsschub und ein grundlegender partizipatorischer Wandel erwartet; dieser wäre – und das unterscheidet die Diskussion über *Online*-Beteiligung von der „alten“ Diskussion – nicht zuletzt auch technisch induziert.

Ob und wie dieser Schub stattfinden wird, sind Fragen, die empirisch beantwortet werden müssen und können. Tatsächlich hat die entsprechende Forschung ein eher skeptisches Bild der Partizipationspotenziale gezeichnet. So scheint sich die Verstärkungsthese zu bewahrheiten, nach der bereits Mobilisierte durch das Internet noch weiter mobilisiert werden, wobei ein Aktivierungseffekt durchaus für bestimmte Personengruppen (insbesondere junge Menschen) ausgemacht werden kann (Escher 2013).

---

### 3 Praxis der Online-Partizipation

Ein Blick in die Praxis der *Online*-Partizipation bestätigt die bereits angesprochene Vielfalt und Bandbreite von Verfahren im Hinblick auf die (staatlichen) Ebenen, Adressaten und Teilnehmenden sowie die Partizipationstiefe, so dass hier lediglich einige Beispiele vorgestellt werden können. Dabei wird der Fokus auf die unver-

bindlichen, also die rechtlich nicht näher definierten, Partizipationsverfahren gelegt, weil hier weniger gesetzliche Vorgaben existieren und entsprechend ein wesentlich höherer Spielraum für die Durchführung von *Online*-Partizipationsverfahren besteht. Auch in der Praxis finden sich im Bereich der informellen *Online*-Partizipation daher die meisten Beteiligungsverfahren. Diese dienen in der Regel der Vorbereitung politischer Entscheidungen durch die dafür demokratisch legitimierten Gremien, sind also rein konsultativ. Die Entscheidungskompetenz wird nicht an die Bürgerinnen und Bürger delegiert. Sie sind auf der Partizipationsleiter daher maximal der dritten Sprosse „Kooperation“ zuzuordnen, dürften sich aber mehrheitlich auf den Stufen darunter bewegen.

Eine weitere Fokussierung ergibt sich aus dem dargelegten Begriffsverständnis, wonach von *Online*-Partizipation nur dann die Rede sein kann, wenn die Verfahren *wesentlich* über das Internet realisiert werden. Dazu ist es wichtig zu wissen, dass *Online*- und *Offline*-Verfahren in praxi regelmäßig kombiniert werden. Schließlich ist noch darauf hinzuweisen, dass sich die Evaluationen von *Online*-Partizipationsverfahren in der Regel auf einzelne Verfahren konzentrieren, so dass keine umfassende Übersicht zu allen *Online*-Beteiligungsprozessen existiert.

Mit Blick auf die staatlichen Ebenen kann davon ausgegangen werden, dass *Online*-Partizipationsangebote am häufigsten auf der kommunalen Ebene zu finden sind. Ursächlich dafür dürfte nicht nur die hohe Anzahl von mehr als 11.000 kommunalen Gebietskörperschaften in Deutschland sein, sondern auch langjährige Erfahrungen mit verschiedenen Partizipationsformaten, die in den „Schulen der Demokratie“ gesammelt wurden: So sieht das Baugesetzbuch bereits seit den 1970er-Jahren die Verpflichtung der Kommunen zur frühzeitigen Beteiligung der Öffentlichkeit an der Bauleitplanung vor, in deren Rahmen zunehmend *Online*-Anwendungen genutzt werden (s. die Übersicht/Beispiele auf <https://www.bauleitplanung.nrw/>, <https://www.bob-sh.de/>, <https://bauleitplanung.hamburg.de/>, <https://buergerbeteiligung.sachsen.de/portal/bplan/beteiligung/aktuelle-themen>). Auch die Möglichkeit, durch lokale Referenden, Bürgerbegehren und Bürgerentscheide Einfluss auf politische Entscheidungen zu nehmen, besteht seit Beginn der 1990er-Jahren in den Kommunen aller Bundesländer (direkte Demokratie). Darüber hinaus werden Bürgerinnen und Bürger auf freiwilliger Basis an der Entwicklung des kommunalen Gemeinwesens beteiligt, wozu kooperative Formate wie Runde Tische, Planungszellen, Bürgerhaushalte, Bürgerbefragungen u. v. m. genutzt (kooperative Demokratie) und ebenfalls durch *Online*-Beteiligungsformate ergänzt oder ersetzt werden.

Für Nordrhein-Westfalen zeigt der „DIID-Monitor Online-Partizipation“, wie zahlreich die Erfahrungen mit *Online*-Partizipationsverfahren auf kommunaler Ebene sind. Demnach wurde bis 2016 in 130 von insgesamt 396 Städten und Gemeinden sowie in sieben von 31 Kreisen mindestens ein internetgestütztes Verfahren zur Bürgerbeteiligung im Bereich der Haushaltplanung, der Bauleitplanung, der Stadtentwicklung, der Lärmaktionsplanung oder des Mängelmanagements durchgeführt (<https://diid.hhu.de/projekte/diid-monitor-online-partizipation/>).

Daneben werden Themen von aktueller politischer Bedeutung auf lokaler Ebene häufig *online* diskutiert. Auch hier zeigt sich sowohl thematisch und auch vom

Beteiligungsformat her eine sehr breite Vielfalt. Die Beispiele reichen von *Online*-Dialogen im Rahmen der Entwicklung von Leitlinien zur Bürgerbeteiligung (Köln) über regelmäßige *Online*-Bürgerbefragungen zur Lebensqualität (Konstanz) bis zu einem multimedialen *Online*-Beteiligungsverfahren zum Abriss einer Hochstraße, für das die Stadt Ludwigshafen 2014 einen Preis für *Online*-Partizipation erhielt (<http://www.ludwigshafen.de/nachhaltig/city-west/buergerbeteiligung-bis-2014/partizipationspreis-2014/>). Auch das Thema Radverkehr ist häufig Inhalt von Bürgerbeteiligung online. Beispielsweise wurden 2017 gleichstrukturierte *Online*-Dialoge zum Radverkehr in den Städten Bonn und Moers sowie im Kölner Bezirk Ehrenfeld durchgeführt mit dem Ziel, den Radverkehr in den einzelnen Städten sicherer zu machen. Die Vorschläge der Bürgerinnen und Bürger dienten den einzelnen Kommunen vor allem als Grundlage für die Beschlussfassung der politischen Gremien und für die vorbereitenden Stellungnahmen der Verwaltung (<https://www.raddialog.bonn.de/>). Zudem konnten durch eine vergleichende Analyse, begleitende Befragungen der Teilnehmenden sowie repräsentative Umfragen der Bevölkerung Hinweise zu den Wirkungen und Einflussfaktoren der *Online*-Diskurse gewonnen werden. Unterstützt wird die internetgestützte Partizipation durch entsprechende Plattformen, wie etwa die Plattform <https://offenedaten-koeln.de/> der Stadt Köln.

Im Bund beschränkt sich die politische Partizipation dagegen grundsätzlich auf Wahlen und Abstimmungen und auch auf der Ebene der Länder werden politische Entscheidungen regelmäßig von den dafür gewählten Abgeordneten getroffen. Zudem sehen die meisten Landesverfassungen direktdemokratische Elemente wie Volksinitiativen, Volksbegehren und -entscheide vor. Allerdings werden auch in den Ländern und im Bund zunehmend *Online*-Beteiligungsformate zur Vorbereitung politischer Entscheidungen oder zur Umsetzung politischer Programme genutzt und/oder Programme zur Unterstützung partizipativer Prozesse in den Ländern und Kommunen angeboten. Ferner werden wesentliche rechtliche Rahmenbedingungen für die politische *Online*-Partizipation durch Bund und Länder bestimmt.

Als Beispiel soll auch hier Nordrhein-Westfalen mit seiner „open.nrw“-Plattform dienen: Neben der Möglichkeit, sich über Verwaltungsdaten aus Land und Kommunen zu informieren, gibt das Portal einen gebündelten Überblick über Partizipationsangebote in Nordrhein-Westfalen auf der Ebene des Landes und in nordrhein-westfälischen Kommunen. Zudem kann die Partizipation und die Zusammenarbeit staatlicher und zivilgesellschaftlicher Akteure über „open.nrw“ organisiert werden (<https://open.nrw/>). In dem Bereich der „Partizipation“ finden sich u. a. Hinweise zu abgeschlossenen *Online*-Partizipationsprojekten in NRW, wie etwa zum Projekt „Digitale Lebenswelten“, das 2015 durch das damalige Ministerium für Familie, Kinder, Jugend, Kultur und Sport NRW durchgeführt wurde, oder der *Online*-Beteiligung zum Normenscreening, die 2017 vom Wirtschafts- und Digitalministerium NRW initiiert wurde mit dem Ziel, die Verwaltung einfacher zu machen. Auch die Nachhaltigkeitsstrategie des Landes NRW und der Dialog zum Hochschulgesetz NRW wurden mit Hilfe von *Online*-Beteiligungsinstrumenten erarbeitet. Schließlich bestand im Rahmen der Erarbeitung der Grundlagen für den so genannten *Open Government Pakt* in Nordrhein-Westfalen die Möglichkeit der *Online*-Partizipation (<https://open.nrw/beteiligung-zum-open-government-pakt>). Gemeinsam ist allen

Projekten, dass die *Online*-Partizipation konsultativ erfolgte, also der Vorbereitung politischer und administrativer Entscheidungen diente.

In anderen Bundesländern und Stadtstaaten existieren ähnliche Beispiele:

- In Brandenburg konnte die „Mobilitätsstrategie 2030“ durch Stellungnahmen der Bürgerinnen und Bürger mitgestaltet werden (<https://service.brandenburg.de/de/mobilitaetsstrategie-2030-onlinebeteiligung/387789>).
- In Berlin wird der Leitlinienprozess für die Bürgerbeteiligung an der Stadtentwicklung durch ein *Online*-Portal flankiert, über das sich Bürgerinnen und Bürger *online* in den Prozess einbringen können (<https://mein.berlin.de/projects/fragen-an-das-arbeitsgremium-berliner-leitlinien/>).
- Das Gesetzgebungsverfahren zum Transparenzgesetz in Rheinland-Pfalz wurde durch einen *Online*-Bürgerbeteiligungsprozess unterstützt (<https://transparenzgesetz.rlp.de/transparenzrlp/de/home.html>).
- Hamburg bietet die Möglichkeit, sich *online* an der Bauleitplanung zu beteiligen (<https://bauleitplanung.hamburg.de>); ähnlich verhält es sich in Schleswig-Holstein.
- Baden-Württemberg kann auf die längste Tradition von Bürgerbeteiligungsprozessen zurückblicken. Hier wurden seit 2013 über 80 Beteiligungsprozesse *online* unterstützt. Diese reichen von *Online*-Dialogen zu einem Wegekonzept im Nationalpark Schwarzwald über einen internetgestützten Dialog zum Bau einer Justizvollzugsanstalt bis zur Fahrgastbeteiligung zur Gestaltung des Fahrplanes (<https://beteiligungsportal.baden-wuerttemberg.de/de/informieren/beteiligungsprojekte-der-landesregierung/>).

Auf Bundesebene werden Planungsprozesse ebenfalls durch *Online*-Beteiligungsformate begleitet, wie etwa die Projekte „Gut Leben in Deutschland – was uns wichtig ist“ oder die Bürgerbeteiligung beim Netzausbau zeigen. Während im ersten Fall die Regierungsstrategie im Rahmen von *Offline*-Dialogen vor Ort und *Online*-Dialogen im Internet diskutiert werden konnte, wurden beim Bürgerdialog zum Netzausbau verschiedene Beteiligungsformate auf allen Stufen der Öffentlichkeitsbeteiligung genutzt: Neben den formalen Beteiligungsmöglichkeiten war ein Dialog über eine Informations- und Dialogplattform möglich. Auch im Rahmen von Gesetzgebungsverfahren wurden Bürgerinnen und Bürger und Verbände bereits auf freiwilliger Ebene partizipativ einbezogen (Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit 2017). Flankiert werden die Aktivitäten auf Bundesebene durch die so genannte *Digitale Agenda* der Bundesregierung 2014–2017 (<https://digitale-agenda.de>), die u. a. einen Aktionsplan zur Digitalen Verwaltung 2020 beinhaltet, und das Bundesportal „govdata“ (<https://www.govdata.de>), in dem sich Daten aus Bund und Ländern finden.

Schließlich können Bürgerinnen und Bürger durch *Online*-Petitionen versuchen, Einfluss auf politische Entscheidungen zu nehmen. Sowohl der Bund als auch die meisten Länder sehen diese Möglichkeit vor. Genutzt werden sie für Forderungen wie die Abschaffung der KiTa-Gebühren, Schulreformen oder die Wiederholung von Abiturprüfungen. Die Petitionen werden in den entsprechenden Petitionsaus-

schüssen beraten, so dass auch hier die letzte Entscheidung bei den politischen Repräsentanten verbleibt. Im Gegensatz zu den vorher beschriebenen Verfahren, muss die Initiative hier von den Bürgerinnen und Bürgern ausgehen.

Die Beispiele zeigen erstens, dass die Bürgerbeteiligung *online* immer bedeutsamer wird und *Offline*-Verfahren ergänzt oder ersetzt. Zweitens ist deutlich geworden, dass die Verfahren in der Regel von der Politik oder der Verwaltung initiiert werden. Drittens bewegen sich die meisten Verfahren auf der konsultativen Ebene. Es stellt sich daher die Frage nach den Wirkungen und Erfolgsfaktoren von *Online*-Partizipation, die bisher nur beispielhaft evaluiert wurden.

Gerl et al. (2016) schlagen zur Evaluation politischer *Online*-Partizipation ein Set von Evaluationskriterien vor, das sie normativ begründen. Die Indikatoren Inklusivität und Repräsentativität sollen das Problem der ungleichen Teilhabe an politischer *Online*-Partizipation adressieren, beziehen sich also auf die Teilhabemöglichkeiten und die Partizipation aller betroffenen oder relevanten Gruppen eines Vorhabens. Mittels der Indikatoren Transparenz, Einfluss und Wirkung können dagegen das eigentliche Beteiligungsverfahren und dessen Wirkungen gemessen werden.

Kubicek et al. (2011) orientieren sich wiederum an den „klassischen“ Evaluationskategorien *Input*, *Output*, *Outcome* und *Impact*, anhand derer sie zwölf Fallbeispiele von *Online*-Partizipation untersuchen (s. auch Aichholzer et al. 2016). Die Ergebnisse zeigen, dass Bürgerbeteiligung dazu beitragen kann, „Lösungen für gesellschaftliche Probleme zu finden, Bedarfe und Interessen der Bevölkerung besser aufzunehmen und auszugleichen und Verständlichkeit und Akzeptanz von Maßnahmen zu fördern“ (Kubicek et al. 2011, S. 10). Als wesentliche Erfolgsfaktoren stellen sie neben einem Thema von hoher Dringlichkeit eine klare Zielsetzung für die Konsultation sowie die Bereitstellung ausreichender Ressourcen heraus (ebd.). Damit bestätigt die Studie Ergebnisse anderer Forschung, verweist aber gleichzeitig darauf, dass nicht alle Beteiligungsverfahren anhand desselben Rasters bewertet werden können.

---

## 4 Perspektiven für Staat und Verwaltung

*Online*-Partizipation ist in den vergangenen Jahren immer stärker zum Einsatz gekommen – auf allen Ebenen und für unterschiedliche Prozesse der Entscheidungsfindung. Dabei relativiert die Empirie der *Online*-Partizipation die demokratischen Hoffnungen, die mit den neuen Möglichkeiten verbunden waren. So wird zurecht gefragt, ob eine nur *online*-basierte Partizipation überhaupt wünschenswert und realisierbar ist. Womöglich sind hybride Formen einer „blended participation“ das Mittel der Wahl für mehr Beteiligung der Bürgerinnen und Bürger in der Politik.

Jedenfalls ist *Online*-Partizipation selbst kein Allheilmittel für die Probleme der repräsentativen Demokratie. Die Forschung zur *Online*-Partizipation kommt in der Gesamtschau zu dem Ergebnis, dass weniger eine Mobilisierung neuer zuvor partizipationsscheuer Gruppen zu beobachten ist, sondern dass sich die Kluft zwischen den zuvor Aktiven und den zuvor Inaktiven durch die Etablierung von *Online*-Kommunikation noch verstärkt. Die Mobilisierungsthese kann höchstens für ein-

zelne Zielgruppen, insbesondere für Jugendliche, bestätigt werden. Dies mag damit zusammenhängen, dass die Voraussetzungen für eine effektive Teilnahme an solchen Prozessen zwar insgesamt niedrigschwelliger erscheinen, weil sie eine größere Flexibilität hinsichtlich der Nutzung und damit eine leichtere Erreichbarkeit einer größeren Anzahl an Personen versprechen, umgekehrt aber neue Kompetenzen bei den Beteiligten erfordern.

Der effektive Einsatz von *Online*-Partizipation verlangt aber nicht nur den Bürgerinnen und Bürgern mehr ab, sondern auch den Akteuren in Politik und Verwaltung. Soll *Online*-Partizipation gelingen, setzt dies die Bereitschaft von politischen und administrativen Eliten voraus, sich der Logik und den Konsequenzen dieser Verfahren gegenüber zu öffnen – dies kann insgesamt eine Neudefinition der entsprechenden Amts- und Mandatsrollen inklusive einer Öffnung gegenüber Laienperspektiven sowie einer Abgabe an Entscheidungskompetenzen erfordern. Hier stellt sich auch die Frage, inwieweit *Online*-Partizipation mit mehr verbindlicher Entscheidungsmacht für die Bürgerinnen und Bürger verbunden werden sollte. Die Ergebnisse aus diesen Verfahren müssen von Politik und Verwaltung ernst genommen werden, damit sich die Bürgerinnen und Bürger auch ernst genommen fühlen.

*Online*-Partizipation stellt ebenso wenig ein Allheilmittel zur Modernisierung der Verwaltung dar. Vielmehr sind mit der Durchführung von *Online*-Partizipationsverfahren neue Anforderungen an die Verwaltung verbunden. Beispielsweise erfordert die Organisation und Moderation von *Online*-Partizipationsverfahren digitale Kompetenzen und Kollaborationskompetenzen bei Führungskräften und Beschäftigten der Verwaltung.

Für diese Prozesse müssen die Voraussetzungen geschaffen werden. Partizipative Verfahren sind ressourcenaufwendig, sie benötigen mehr Zeit und erfordern einen klaren rechtlichen Rahmen. Notwendig ist zudem eine leistungsfähige digitale Infrastruktur. Aber vor allem Akteure, die bereit sind, *Online*-Partizipation anzubieten und wahrzunehmen.

---

## Literatur

- Aichholzer, Georg, Herbert Kubicek, und Lourdes Torres, Hrsg. 2016. *Evaluating e-participation. frameworks, practice, evidence*. Cham: Springer.
- Arnstein, Sherry R. 1969. A ladder of citizen participation. *Journal of the American Institute of Planners* 35(4): 216–224.
- Bundesministerium des Innern. 2012. *Open Government Data Deutschland*. Berlin: BMI.
- Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit. 2017. Bürgerbeteiligung auf Bundesebene – Erfolge und Perspektiven (Dokumentation der Fachtagung vom 11.07.2017). Berlin: BMU.
- Escher, Tobias. 2013. Mobilisierung zu politischer Partizipation durch das Internet. Erwartungen, Erkenntnisse und Herausforderungen der Forschung. *Analyse und Kritik* 35(2): 449–476.
- Gerl, Katharina, Stefan Marschall, und Nadja Wilker. 2016. Evaluation von politischer Online-Partizipation – Demokratische Innovation vs. Symbolische Politik. *Zeitschrift für Politikberatung* 8(2–3): 59–68.
- Kaase, Max. 1992. Partizipation. In *Pipers Wörterbuch zur Politik*, Hrsg. Dieter Nohlen und Rainer-Olaf Schultze, 4. Aufl., 682–684. München: Piper.

- Kersting, Norbert., Hrsg. 2008. Innovative Partizipation: Legitimation, Machtkontrolle und Transformation. Eine Einführung. In *Politische Beteiligung. Einführung in dialogorientierte Instrumente politischer und gesellschaftlicher Partizipation*, 11–39. Wiesbaden: Springer VS.
- Kubicek, Herbert, Barbara Lippa, und Alexander Koop, Hrsg. 2011. *Erfolgreich beteiligt? Nutzen und Erfolgsfaktoren internetgestützter Bürgerbeteiligung. Eine empirische Analyse von 12 Fallbeispielen*. Gütersloh: Bertelsmann Stiftung.
- Voss, Kathrin, Hrsg. 2014. *Internet und Partizipation. Bottom-up oder Top-down? Politische Beteiligungsmöglichkeiten im Internet*. Wiesbaden: Springer VS.



---

# Elektronische Wahlen und Abstimmungen (Electronic Voting)

Frank Bätge und Thomas Weiler

## Inhalt

1 Klärung des Begriffs .....	292
2 Theoretische Grundlagen .....	293
3 Praktische Anwendung .....	296
4 Künftige Entwicklung .....	299
Literatur .....	300

---

## Zusammenfassung

*Electronic Voting (E-Voting)* bezeichnet die Teilnahme an Wahlen und Abstimmungen mithilfe elektronischer Geräte. Derzeit ist es (noch) nicht möglich, die hierfür im Grundgesetz genannten rechtlichen Vorgaben gleichzeitig in einem rein elektronischen Verfahren vollständig einzuhalten. Deutlich freier als bei gesetzlich vorgeschriebenen Wahlen und Abstimmungen auf staatlicher Ebene gestaltet sich der Einsatz von *E-Voting* im Rahmen von Wahlen und Abstimmungen bei Trägern der Selbstverwaltung wie z. B. den Kommunen und Universitäten. *E-Voting* bietet das Potenzial Wahlen und Abstimmungen schneller und kostengünstiger durchzuführen, die Beteiligung zu erhöhen und Fehler bei der Stimmauszählung zu verhindern.

---

F. Bätge (✉)

Fachhochschule für öffentliche Verwaltung Nordrhein-Westfalen, Köln, Deutschland

E-Mail: [frank.baetge@fhoev.nrw.de](mailto:frank.baetge@fhoev.nrw.de)

T. Weiler

NRW Fortschrittskolleg Online-Partizipation, Fachhochschule für öffentliche Verwaltung NRW, Köln, Deutschland

E-Mail: [thomas.weiler@fhoev.nrw.de](mailto:thomas.weiler@fhoev.nrw.de)

**Schlüsselwörter**

Bürgerhaushalt · Risikofaktoren · Manipulation · Online-Voting · Wahlrechtsgrundsätze

---

## 1 Klärung des Begriffs

Unter *E-Voting* versteht man die Teilnahme an rechtlich verbindlichen politischen Entscheidungsprozessen (Wahlen und Abstimmungen) durch die Stimmabgabe mittels elektronischer Geräte. Die für das *E-Voting* charakteristische elektronische Stimmabgabe ist rechtlich zu differenzieren von der bloßen Stimmenauszählung oder Stimmenzusammenzählung mit Hilfe elektronischer Geräte (etwa Scanner oder Rechengeräte zur Auszählungshilfe). Für die elektronische Stimmabgabe einerseits und die elektronische Auszählungshilfe anderseits bestehen unterschiedliche juristische Maßstäbe. Die hier interessierende elektronische Stimmabgabe unterliegt höheren juristischen Hürden.

Ein Unterfall des *E-Voting* ist das *Online-* bzw. *Internet-Voting*. Hierbei wird die Stimme auf einer dafür eingerichteten *Website* über das Internet abgegeben. *Online-* bzw. *Internet-Voting* ist auch außerhalb des Wahlraums möglich. *E-Voting* kann damit entweder als Präsenzwahl in einem öffentlichen Wahlraum auf amtlichen Wahlgeräten (*Hard- und Software*) oder über privat genutzte (auch mobile) Endgeräte außerhalb von Wahlräumen mittels amtlich zur Verfügung gestellter bzw. amtlich zertifizierter *Software* als Distanzwahl erfolgen. Während bei der elektronischen Präsenzwahl eine öffentliche Kontrolle der Stimmabgabemodalitäten möglich bleibt, findet die Distanzwahl ohne diese statt.

Abzugrenzen ist der Begriff des *E-Voting* von unverbindlichen Partizipationsformen mit lediglich empfehlendem Charakter (Bürgerhaushalt, Stadtblog, Einwohnerdialog auf einer kommunalen *Website* oder ähnliches). Da die beim *E-Voting* getroffenen Entscheidungen umgesetzt werden müssen und erforderlichenfalls eingeklagt werden können, sind hier deutlich strengere rechtliche Anforderungen zu erfüllen. Rechtliche Risikofaktoren wie die Sicherung der authentischen Stimmabgabe, der Schutz der Erkennbarkeit und Nachvollziehbarkeit der Stimmabgabe sowie die Gefahr der Manipulation sind bei der Einführung von *E-Voting* zu berücksichtigen und mit den relevanten Vorteilen abzuwägen. *E-Voting* bietet gegenüber den derzeit genutzten Verfahren mehrere Vorteile: Fehler bei der Stimmenzusammenzählung oder die falsche Einordnung einer unklaren Stimme können vermieden werden. Das elektronische Verfahren ist zudem deutlich schneller als eine Auszählung von Hand. Des Weiteren kann *E-Voting* Personen mit Behinderungen die Stimmabgabe eher ermöglichen; zum Beispiel können sich die Wahlberechtigten die Kandidatenliste vorlesen lassen. Beim *Online-Voting* muss die Wählerin oder der Wähler noch nicht einmal die Wohnung verlassen. Dies würde auch Wählerinnen und Wählern im Ausland die Teilnahme leichter ermöglichen. Elektronisch unterstützt kann bei der Stimmabgabe der Wählerin bzw. dem Wähler zudem während des Wahlvorganges gespiegelt werden, ob eine ungültige Abgabe der Stimme vorliegt oder nicht.

Insbesondere bei komplizierten Verfahren (zum Beispiel bei kumulierter und panaschierter Stimmabgabe) können so unbewusst ungültig abgegebene Stimmen deutlich reduziert werden. Mittel- bis langfristig ist auch die Einsparung von Ressourcen (wie etwa Papier) möglich. *E-Voting* kann insgesamt kostengünstiger sein, wenn Ausgaben für Mitglieder der Wahlvorstände, das Anmieten von Räumen usw. wegfallen. Dazu müssen aber zunächst die Kosten für die Anschaffung der Geräte, *Software* usw. amortisiert sein. Fürsprecher des *E-Voting* versprechen sich hiervon auch eine Steigerung der Wahlbeteiligung (Weiler 2015, S. 7). Aus demokratietheoretischer Sicht ist hierin ein Vorteil zu sehen, da sehr niedrige Beteiligungsquoten zu einer Abnahme zumindest der politischen Legitimation führen können.

Auf der anderen Seite kann eine Wahl oder Abstimmung per Computer zu einem Verlust von Vertrauen in das Ergebnis führen. Wer nicht von der Sicherheit der elektronischen Systeme überzeugt ist, fürchtet gegebenenfalls, dass die Stimmabgabe nicht mehr geheim bleibt oder die abgegebene Stimme nicht ordnungsgemäß gezählt wird. Möglicherweise beteiligen sich Personen daher nicht mehr, wenn *E-Voting* eingeführt wird. Auch würde aus dem derzeit öffentlichen Verfahren der Teilnahme an einer Wahl oder Abstimmung mit anderen an einem Stichtag durch die Einführung von *Online-Voting* eine „Wahl im Verborgenen“. Diese Tendenz ist bereits infolge der Zunahme der Briefwahl als herkömmliche Form der Distanzwahl erkennbar.

---

## 2 Theoretische Grundlagen

Nach Art. 20 Abs. 2 Satz 2 Grundgesetz (GG) übt das Volk die Staatsgewalt unmittelbar in Wahlen und Abstimmungen aus. Während Wahlen Entscheidungen über Personen darstellen, betreffen Abstimmungen unmittelbare Sachentscheidungen des Volkes. Man bezeichnet die Abstimmungen auf staatlicher Ebene als Volksentscheide und auf kommunaler Ebene als Bürgerentscheide. Das Grundgesetz sieht bundesweite Volksentscheide nicht vor. Auf Ebene der Länder und Kommunen sind Abstimmungen hingegen durch die Landesverfassungen und Kommunalgesetze ausdrücklich normiert. Wahlen und Abstimmungen als zentrale demokratische Legitimationsverfahren sind in der Bundesrepublik Deutschland gemäß Art. 20 Abs. 2 Satz 2 GG grundsätzlich gleichgestellt. Die für Wahlen geltenden Grundsätze (*Wahlrechtsgrundsätze*) können daher mit wenigen Einschränkungen auf Abstimmungen übertragen werden. Die Wahlrechtsgrundsätze für Wahlen zum Bundestag finden sich in Art. 38 Abs. 1 Satz 1 GG. Über das Homogenitätsprinzip gelten diese nach Art. 28 Abs. 1 Satz 2 GG auch für Wahlen in den Ländern, Kreisen und Gemeinden. Wahlen müssen danach fünf Grundsätze erfüllen: Sie müssen allgemein, unmittelbar, frei, gleich und geheim sein.

Allgemein sind Wahlen, wenn niemand unberechtigterweise von der Wahl ausgeschlossen wird. Grundsätzlich soll jede Person mit der erforderlichen Einsichtsfähigkeit (Wahlalter) wählen dürfen, hinsichtlich des Wahlrechts soll formelle Gleichheit bestehen. Verboten ist ein Wahlausschluss aus sozialen, politischen oder

wirtschaftlichen Gründen. Daher kann – jedenfalls nach aktuellen Maßstäben – die elektronische Wahl nur eine zusätzliche Alternative sein. Es muss sichergestellt sein, dass auch Personen ohne eigenen Computer und Internetzugang sowie ohne entsprechende Fachkenntnisse die Wahlmöglichkeit haben. Eine Alternative hat zudem für den Fall zu bestehen, in dem eine elektronische Wahl – etwa wegen technischer Probleme – nicht möglich ist.

Das Wahlrecht hängt von bestimmten Voraussetzungen ab, die von Wahl zu Wahl differenzieren können, wie z. B. das Wahlalter, dem Wohnort, die Staatsangehörigkeit etc. Der Grundsatz der allgemeinen Wahl macht es, ebenso wie der Grundsatz der gleichen Wahl, notwendig, dass alle Wahlberechtigten an der Wahl teilnehmen dürfen, aber eben auch nur diese. Auch beim *E-Voting* muss daher sichergestellt werden, dass die Wählerin bzw. der Wähler tatsächlich wahlberechtigt ist. Hierzu hat vor dem eigentlichen Wahlakt eine Authentifizierung zu erfolgen. Dies kann bei der elektronischen Wahl im Wahlraum durch Kontrolle des Personalausweises erfolgen. Bei der Distanzvariante könnten der maschinenlesbare oder elektronische Ausweis verwendet werden, alternativ persönliche Zugangscodes wie PINs oder TANs, Passwörter oder die elektronische Signatur.

Unmittelbar sind Wahlen, wenn zwischen den Wählerinnen und Wählern sowie dem Wahlergebnis keine entscheidende Zwischeninstanz tritt. Insbesondere beim *E-Voting* muss daher garantiert sein, dass die zur Stimmabgabe genutzten Geräte ordnungsgemäß und manipulationsfrei funktionieren und die Stimmentscheidung unverfälscht aufnehmen. Zudem muss sichergestellt werden, dass keine nachträgliche Veränderung oder Löschung der Stimme vorgenommen werden kann.

Die Freiheit der Wahl gebietet es, dass die Wählerin bzw. der Wähler selbst entscheidet, ob überhaupt und gegebenenfalls welche Person gewählt wird; die Wahlentscheidung muss unverfälscht zum Ausdruck gebracht werden. Eine amtliche Beeinflussung dieser Entscheidung ist bei Wahlen nicht gestattet. Bei Abstimmungen ist sie unter bestimmten Voraussetzungen im Wege von amtlichen Hinweisen oder Empfehlungen erlaubt. In keinem Fall und von niemandem darf auf die wahlberechtigte Person Druck oder gar Zwang ausgeübt werden. Die technischen Systeme müssen es dieser auch ermöglichen, alternativ zur Abgabe einer bestimmten gültigen Stimme sich bewusst dafür zu entscheiden, keine oder eine ungültige Stimme abzugeben. Zudem muss es jeder wahlberechtigten Person möglich sein, unbeeinflusst ihre Entscheidung zu treffen. Insbesondere bei der *Online-Distanzwahl*, die außerhalb von öffentlich kontrollierten Räumen stattfinden kann, ist dieser Grundsatz gefährdet. Ähnlich wie bei der Briefwahl kann hier aber eine Verlagerung der Sicherung der freien Wahl auf die Wählerin bzw. den Wähler selbst stattfinden. Zum Schutz der Freiheit der Wahl kann der wahlberechtigten Person die Möglichkeit gegeben werden, mehrfach ihre Stimme abzugeben, wobei nur die letzte abgegebene Stimme zählt. So hätte sie die Möglichkeit, nach einer beeinflussten oder gar erzwungenen Wahl ihre Entscheidung gegebenenfalls zu ändern. Diese Möglichkeit wird z. B. im Wahlrecht in Estland genutzt.

Die Gleichheit der Wahl gebietet es, dass alle wahlberechtigten Personen in formal gleicher Weise wählen dürfen. Bei der elektronischen Wahl müssen also die verschiedenen Wahlsysteme die gleichen Optionen eröffnen. Es muss insbeson-

dere sichergestellt sein, dass eine Person auch nur einmal wirksam wählt. Die technischen Systeme müssen daher eine Authentifizierung der Wählerin bzw. des Wählers ermöglichen. Es ist des Weiteren sicherzustellen, dass im Falle einer etwaigen mehrfachen Stimmabgabe diese nur einmal zählt. Dieses Verbot der Doppelwahl erfordert deshalb bei jeder wahlberechtigten Person einen Abgleich der elektronisch und gegebenenfalls bei der Urnenwahl oder Briefwahl abgegebenen Stimmen. Aus dem Grundsatz der Gleichheit der Wahl folgt zudem die gleiche Werthaltigkeit der unterschiedlichen Stimmabgabemöglichkeiten (Urnenwahl, Briefwahl, elektronische Wahl).

Schließlich muss die Wahl geheim sein. Hieraus resultiert, dass jede Wählerin und jeder Wähler die Wahlentscheidung für sich behalten darf. Dies sichert die Freiheit der Wahl, indem verhindert wird, dass auf die wahlberechtigte Person Druck ausgeübt werden kann. Um dies und auch einen Stimmenkauf/Stimmenverkauf zu verhindern gilt ein grundsätzliches „Quittungsverbot“: die Wählerin bzw. der Wähler darf keinen Beleg als Beweis über den Inhalt seiner Stimmabgabe erhalten. Bei der Urnenwahl verbleibt der Stimmzettel im Wahlraum. Durch dieses Verbot können sich Friktionen mit dem noch darzustellenden Transparenzgebot der Wahl ergeben, die vom Gesetzgeber nur im Wege einer Abwägung aufzulösen sind. Der Grundsatz der geheimen Wahl ist bei der Distanzwahl stärker gefährdet. Auch hier ist erforderlich, dass die Wählerin bzw. der Wähler selbst die geheime Stimmabgabe sichert. Ähnlich wie bei der Briefwahl ist daher zu fordern, dass eine entsprechende eidesstattliche Versicherung abzugeben ist. Dies ist elektronisch durch hinreichend gesicherte und signierte Dokumente möglich; zudem könnte eine solche Versicherung durch die Angabe eines weiteren Codes bestätigt werden. Die abgegebene Stimme selbst ist zu verschlüsseln, so dass ihr Inhalt nicht unbefugt von Dritten eingesehen werden kann.

Neben diesen fünf geschriebenen Wahlrechtsgrundsätzen hat das Bundesverfassungsgericht (BVerfG) den Grundsatz der Öffentlichkeit der Wahl postuliert (Bundesverfassungsgericht 2009). Dieser besagt, dass die wesentlichen Schritte einer Wahl für den Wähler transparent und nachvollziehbar sein müssen. Das BVerfG leitet diesen Grundsatz aus den Staatsstrukturprinzipien der Demokratie, Republik und Rechtsstaatlichkeit ab (vgl. Art. 20 GG). Das BVerfG stützt seine Überlegungen darauf, dass bei Wahlen in der Regel staatliche Gewalt von den Wählerinnen und Wählern auf die gewählten Organe übertragen wird. Die Öffentlichkeit der Wahl unterstützt den Schutz vor Manipulationen und hat integrativen Charakter. Dieser Grundsatz gebietet es, eine öffentlich nachvollziehbare, transparente Möglichkeit der Stimmenauszählung zu schaffen. Bei elektronisch abgegebenen Stimmen ohne physisch vorhandenen Beleg stößt eine entsprechende Nachvollziehbarkeit auf Grenzen. Es müssten daher Alternativen gefunden werden, die eine öffentliche, nachvollziehbare Wahl auch auf rein elektronischem Wege ermöglichen.

Die genannten Grundsätze unterstützen sich teils gegenseitig, teils können sie im Rahmen einer Abwägung untereinander oder mit anderen hochwertigen Verfassungsgütern eingeschränkt werden – so garantiert die geheime Wahl die freie Wahl oder die Öffentlichkeit der Wahl findet ihre Grenze in der Geheimheit der Wahl. Eine Erhöhung der Wahlbeteiligung und damit Stärkung der Allgemeinheit der Wahl

kann gegebenenfalls Abstriche bei anderen Grundsätzen rechtfertigen. Hierbei ist jedoch zu berücksichtigen, dass *E-Voting* ein deutlich höheres Manipulationspotenzial und somit Risiko aufweist als eine Urnenwahl. Die verwendeten technischen Systeme müssen speziell gegen Ausspähungen, Hackerangriffe u. ä. gesichert werden und zudem amtlich zertifiziert sein.

Auf der Ebene der öffentlich-rechtlichen Selbstverwaltungsträger sind vor allem für Hochschulen und Kommunen (vgl. Bätge und Gerl 2018) sowie für die Sozialversicherungsträger die Möglichkeiten der elektronischen Stimmabgabe von besonderem Interesse (Bätge 2018a). So haben einige Hochschulen mittlerweile für die pflichtige Wahl ihrer Gremien durch Satzung (Wahlordnung) die Einführung einer elektronischen Stimmabgabe normiert.

Auch die Kommunen haben – anders als bei den gesetzlich vorgeschriebenen Wahlen und Abstimmungen – bei ihren freiwillig durchgeführten Partizipationsvorhaben (wie z. B. Wahl von freiwilligen Beiräten, konsultative Einwohnerbefragungen etc.) höhere Spielräume zur Einführung der elektronischen Stimmabgabe und Auszählung. Während eine rein konsultative Befragung kein *E-Voting* im rechtlichen Sinne darstellt, ist insbesondere im Bereich der auf satzungsrechtlicher Grundlage durchgeführten Wahl von beratenden Beiräten (Senioren-, Jugend-, Behindertenbeiräte etc.) ein Erprobungsfeld für den Einsatz von *E-Voting* zu sehen. Die Einrichtung solcher beratenden Gremien ist vom staatlichen Gesetzgeber nicht vorgeschrieben, sondern wird von den Kommunen auf ortsrechtlicher Basis freiwillig eingeführt. Während die Einrichtung derartiger Gremien damit für die Kommunen von freiwilliger Natur ist, ist die Wahl der Mitglieder rechtlich verbindlich durch die örtliche Wahlordnung festgelegt. Bei diesen freiwilligen Partizipationsformen können elektronische Elemente eingeführt sowie erprobt und evaluiert werden.

---

### 3 Praktische Anwendung

*E-Voting* in der Variante des *Internet-Voting* findet im europäischen Ausland insbesondere in Estland statt (Solvak und Vassil 2016). Dort gibt es die Möglichkeit, bei Wahlen zum Europäischen Parlament, dem nationalen Parlament und auf kommunaler Ebene seine Stimme über das Internet abzugeben. Etwa ein Drittel der Wählerinnen und Wähler nutzt diese Möglichkeit. Die Wählerin bzw. der Wähler identifiziert sich über einen elektronischen Ausweis und ein Kartenlesegerät zusammen mit einer Geheimzahl am Computer und kann dann auf die Wahlwebsite zugreifen. Hier trifft er die Auswahl unter den Kandidaten und bestätigt diese mit einer zweiten Geheimzahl. Danach wird ein QR-Code angezeigt; über ein anderes Gerät kann die Wählerin bzw. der Wähler auf einer anderen Website prüfen, ob und mit welchem Inhalt die Stimme verbucht wurde.

Bei der Übertragung der Stimme gilt das „Zwei-Umschlag-Prinzip“: die elektronisch abgegebene Stimme wird doppelt asymmetrisch verschlüsselt in einem „inneren elektronischen Umschlag“ gespeichert, während die Wählerdaten in einem unabhängig verschlüsselten Datensatz in einem „äußeren Umschlag“ abgespeichert werden. Für die Stimmenauslesung ist ein weiterer Code notwendig, der auf alle

Mitglieder der Wahlkommission so verteilt ist, dass sie nur gemeinsam den Code verwenden können. Während des Wahlzeitraums kann der Wähler seine Stimme beliebig oft abgeben, nur die letzte Entscheidung zählt. Eine Stimmabgabe an der Urne oder per Brief hat Vorrang vor dem *E-Voting*, so dass die Stimme jeder Wählerin bzw. jedes Wählers am Ende nur einmal gewertet wird. Ein Verstoß gegen die Gleichheit der Wahl – bei der Urnenwahl kann die Wählerin oder der Wähler nur einmal ihre/seine Stimme abgegeben – ist hier hinzunehmen, um die Freiheit und Geheimheit der Wahl zu schützen. Das estnische System genügt jedoch nicht den rechtlichen Voraussetzungen für Parlamentswahlen in der Bundesrepublik Deutschland: Das Verschlüsselungssystem ist nicht öffentlich durch die Wissenschaft nachvollziehbar und genügt daher nicht dem Transparenzgebot. Eine Bestätigung des Inhalts der abgegebenen Stimme verstößt zudem gegen das „Quittungsverbot“.

Neben Estland nutzen auch andere Länder elektronische Systeme zu Wahlen und Abstimmungen. In der Schweiz erfüllten zwei Systeme die dortigen bündesrechtlichen Anforderungen und werden auch aktuell eingesetzt: Das System des Kantons Genf, das auch andere Kantone benutzen, sowie das *E-Voting*-System der Post, das zum Beispiel der Kanton Neuchâtel benutzt. Die nationalen Anforderungen schreiben den Einsatz von modernen mathematischen Verfahren vor, welche gleichzeitig das Stimmgeheimnis garantieren und die Stimmabgabe vollständig nachvollziehbar machen. Die aktuell eingesetzten Systeme verfügen über die individuelle Verifizierbarkeit: Die Stimmberechtigten erhalten Prüfcodes zugestellt, dank denen sie die korrekte Übermittlung ihrer Stimme selbst prüfen können. Diese Prüfcodes werden weiterhin auf einem von der IT unabhängigen Weg – per Post – zugestellt und sind daher besser gegen Manipulationen geschützt.

In den Vereinigten Staaten finden Wahlen auf föderaler Ebene, z. B. zum Präsidenten oder für den Kongress (Senat und Parlament), auf dem Level der Bundesstaaten (Gouverneure, Parlamente) und auf kommunaler Ebene statt. Die meisten Regelungen zu Wahlen sind aber nicht im Bundesrecht zu finden, sondern entspringen dem Recht der fünfzig Bundesstaaten. 1964 wurden erstmals elektronische Wahlgeräte in sieben Wahlbezirken in Kalifornien eingesetzt. In der Regel ist *E-Voting* als Präsenzwahl ausgestaltet. Durch den 1986 eingeführten *Uniformed and Overseas Citizen Absentee Voting Act* müssen die Bundesstaaten in bestimmten Fällen aber auch die Teilnahme an Wahlen auf Bundesebene für Bürger aus dem Ausland (in der Regel Militärangehörige) erlauben. Hieraus ergab sich die Notwendigkeit, Distanzwahlen einzuführen. Der 2009 beschlossene *Military and Overseas Voters Empowerment Act* fordert mindestens eine Variante der elektronischen Stimmabgabe für im Ausland stationierte Militärangehörige (wobei dies auch die Möglichkeit umfassen kann, einen Stimmzettel aus dem Internet herunterzuladen, auszudrucken und dann zu faxen). Die Föderale Wahlkommission erließ 1990 einen Standard für *E-Voting*, an den sich die für die Durchführung der Wahlen zuständigen Bundesstaaten halten müssen. Dieser wurde 2002 modifiziert. Eine nachgeordnete Behörde überprüft die zu verwendenden Wahlgeräte und zertifiziert diese. Beim *E-Voting* in den USA gab es dennoch mehrfach erhebliche Probleme mit den verwendeten Geräten – die Wahlgeräte funktionierten gar nicht, zeigten die Stimm-

abgabe falsch an, ließen sich manipulieren usw. Am Bekanntesten sind die Unklarheiten während der Präsidentschaftswahl 2000 im Bundesstaat Florida. Hier lag der Fehler jedoch nicht im elektronischen Wahlvorgang, sondern es gab Probleme mit den für die Auszählung verwendeten Stimmzetteln aus Papier. Hierbei erfolgte die Anzeige der abgegebenen Stimme durch Ausstanzen des Vorschlags, da die verwendeten Geräte jedoch teils veraltet waren oder nicht korrekt gewartet wurden, setzen die Geräte die Markierungen nicht oder nicht vollständig. Doch auch der elektronische Wahlvorgang als solcher verlief oft nicht einwandfrei: In North Dakota gingen 2004 über 4000 elektronisch abgegebene Stimmen verloren; 2006 zeigte sich, dass die meistgenutzten Geräte in weniger als einer Minute zu *hacken* und manipulieren waren. 2007 ordnete die Kalifornische Regierung eine Überprüfung aller verwendeten Wahlgeräte an, dabei stellten sich flächendeckende erhebliche Sicherheitslücken heraus. Daraufhin wurde *E-Voting* in Kalifornien ausgesetzt. Bei den Zwischenwahlen (*Midterms*) im November 2018 war *E-Voting* in der Hälfte der Bundesstaaten möglich: Per mobiler *App* (West Virginia), über ein *Online-Portal* (Arizona, Colorado, Missouri und North Dakota) sowie per *e-mail* in zwanzig weiteren Bundesstaaten. Hierbei verzichtet die Wählerin bzw. der Wähler bei der Stimmabgabe auf ihr/sein Stimmgeheimnis. Auch bei diesen Wahlen kam es zu zahlreichen Problemen – Wahlgeräte konnten nicht auf das Wählerverzeichnis zugreifen, schalteten sich ab oder zeigten nicht die korrekte Stimmabgabe an. Im Senat wurde ein Gesetzesvorschlag mit dem Ziel eingebracht, die elektronischen Wahlgeräte bis zur Präsidentschaftswahl 2020 sicherer zu machen.

Wie bereits angesprochen spielt *E-Voting* im Rahmen von Wahlen bei Trägern der funktionalen Selbstverwaltung auch in der Bundesrepublik Deutschland eine zunehmende Rolle. Bei Wahlen an Hochschulen wird es bereits seit der Jahrtausendwende praktiziert. An der Universität Osnabrück wurde im Jahre 2000 die erste verbindliche *Online-Wahl* durchgeführt. Einige Landesgesetzgeber haben in ihren Hochschulgesetzen mittlerweile die elektronische Gremienwahl ausdrücklich legitimiert und den Hochschulen hierfür eine Befugnis zur Regelung durch Wahlordnung erteilt. Die in der Wahlordnung der Friedrich-Schiller-Universität Jena eingeführte elektronische Stimmabgabe hat bereits die Billigung der höchstrichterlichen Rechtsprechung gefunden, jedenfalls sofern die Wahlordnung hinreichend bestimmte Regelungen zu den wesentlichen Inhalten des Wahlverfahrens enthält (Bundesverwaltungsgericht 2018; Bätge 2018b). Regelungsbedürftige Inhalte betreffen das Erfordernis einer amtlich geprüften und freigegebenen elektronischen *Software* zur Stimmabgabe und Auszählung, die elektronische Authentifizierung mit Zugangsdaten, die Verhinderung mehrfacher Stimmabgabe, die Anonymisierung der eingegangenen Stimmen, die Möglichkeit der Korrektur bzw. des Abbruches der Stimmabgabe, das Verfahren bei technischen Störungen, die Bestätigung für die Wählerin bzw. den Wähler, die Sicherung gegen Manipulationen und die Regelung der öffentlichen Auszählung. Bei den Wahlen an der Jenaer Universität wird infolgedessen ein von der Bundesanstalt für Sicherheit in der Informationstechnik zertifiziertes System der Wahl verwendet, welches dementsprechende Vorkehrungen aufweist. In einem Erfahrungsbericht zu dieser *Online-Hochschulwahl* wurde deutlich, dass die Wahlbeteiligung erhöht werden, Ressourcen geschont, Kosten für das Wahlmanagement

gesenkt, Termine gestrafft und deutlich komfortabler (wählerfreundlicher) abgestimmt werden konnten (Rüttger 2016). Es ist aber eine differenzierte Betrachtung erforderlich, die vom jeweiligen Einzelfall abhängt. Eine wesentliche Bedeutung kommt der Vorbereitung und Qualitätskontrolle des Onlinesystems zu, da nach dem Start Fehler in der Organisation, bei Stimmzetteln oder im Wählerverzeichnis nicht mehr oder allenfalls mit besonderen Schwierigkeiten korrigiert werden können.

Die für die Wahlen bei Sozialversicherungsträgern geplante Einführung von *E-Voting* ist mehrfach, mindestens bis 2023, verschoben, da nach Ansicht der Träger noch keine elektronischen Wahlsysteme existieren, die auf dieser Ebene ein legales *E-Voting* zuließen. Diesen Bedenken hat sich der Bundesgesetzgeber letztlich angegeschlossen.

Unterhalb der Ebene rechtlicher Verbindlichkeit können als Beispiele freiwillig durchgeföhrter, nicht-verbindlicher elektronischer Partizipationsvorhaben auf kommunaler Ebene angeführt werden:

- Die ausdrücklich im *E-Government-Gesetz* des Landes Nordrhein-Westfalen (§ 18) eingeräumte Möglichkeit für die Kommunen zur Eröffnung einer elektronischen Beteiligung. Für diesen Fall sind die Ergebnisse der Beteiligung bekannt zu geben (Bätge 2018c);
- die gesetzlich vorhandene Möglichkeit zur Durchführung konsultativer Einwohnerbefragungen (vgl. z. B. die Kommunalgesetze von Brandenburg, Niedersachsen oder des Saarlandes) und
- die kommunale Selbstbindung durch eine freiwillige Satzung über das Beteiligungsverfahren auch in elektronischer Form (vgl. z. B. die entsprechenden Satzungen der Städte Bonn und Gießen).

Es wird von Interesse sein, ob sich hieraus etwaige Pilot- oder Vorgänger- bzw. Modellprojekte für ein rechtlich verbindliches *E-Voting* ergeben können.

---

## 4 Künftige Entwicklung

Der Gesetzgeber wird in Zukunft aufgrund des steigenden Digitalisierungsgrades vermehrt auch die rechtlichen Chancen der Einföhrung einer elektronischen Partizipation zu berücksichtigen haben. Hierzu gehören vor allem die möglichen positiven Auswirkungen auf die Wahlbeteiligung, die Vereinfachung und Beschleunigung des Wahlverfahrens (auch für Personen mit Behinderungen oder für im Ausland lebende Wahlberechtigte) sowie die Vermeidung unbewusster falscher Kennzeichnungen und von Zählfehlern. Das BVerfG hat in seiner Wahlcomputerentscheidung die Möglichkeit einer elektronischen Stimmabgabe nicht generell ausgeschlossen, sondern aus dem Öffentlichkeitsgrundsatz entsprechende Anforderungen hierfür an den Gesetzgeber und die Wahlcomputer formuliert.

Es bedarf daher eines interdisziplinären Ansatzes und der Zusammenarbeit von Fachleuten für Datensicherheit, Informatik, Kryptologie, Wahlrecht etc., um entsprechende Lösungen zu erarbeiten, die das erforderliche Mindestmaß an Sicherheit

und Nachvollziehbarkeit gewährleisten. Hierbei empfiehlt es sich, sich zunächst mit den Verfahren zur Wahl von öffentlichen Gremien unterhalb der Parlaments- und Kommunalwahlen zu befassen. In diesem Bereich liegt bereits erste Rechtsprechung vor, die eine weitgehende Satzungsautonomie anerkennt und somit die Einführung elektronischer Wahlen leichter ermöglicht als bei Parlaments- und Kommunalwahlen.

Insbesondere bei Wahlen und Abstimmungen bei Trägern der Selbstverwaltung, wie den Sozialversicherungsträgern und Hochschulen und auf kommunaler Ebene bietet sich für den Gesetzgeber ein schrittweises Vorgehen über gesetzliche Experimentier- und Freistellungsklauseln an. Unabhängig hiervon können die Selbstverwaltungsträger zudem ihre Satzungshoheit nutzen, um freiwillige Gremien auf elektronischem Wege wählen zu können.

Auch jenseits der Selbstverwaltungswahlen könnte der jeweilige parlamentarische Gesetzgeber für behördenerinterne Wahlen unterhalb der politischen Ebenen, wie der Wahl von Personalräten oder Gleichstellungsbeauftragten, elektronische Abstimmungsmöglichkeiten ermöglichen und evaluieren.

Unterhalb der Ebene rechtlicher Verbindlichkeit ergibt sich das breiteste Anwendungsspektrum. Dies kann insbesondere im Rahmen von Pilotprojekten als Möglichkeit genutzt werden, die vorhandenen Verfahren im Echteinsatz zu testen.

---

## Literatur

- Bätge, Frank. 2018a. Legal issues of Online Participation in Municipalities and Universities in the Federal Republic of Germany. In *Proceedings Third International Joint Conference on Electronic Voting E-Vote-ID 2018* [2–5 October 2018, Lochau/Bregenz, Austria], Hrsg. Robert Krimmer, Melanie Volkamer et al., 34–48. Tallinn: TalTech Press.
- Bätge, Frank. 2018b. Rechtswirksamkeit einer Onlinne-Hochschulwahl. *Deutsche Verwaltungspraxis* 2018(11): 458–460.
- Bätge, Frank. 2018c. Wahlen und Abstimmungen in Nordrhein-Westfalen, Loseblatt-Kommentar, Stand: November 2018.
- Bätge, Frank, und Katharina Gerl. 2018. E-Partizipation. Beteiligung in NRW. *Kommune* 21(2): 44–45.
- Bundesverfassungsgericht. 2009. Urteil des Bundesverfassungsgerichts 2 BvC 3/07 und 4/07 vom März 2009 zu Wahlgeräten. [www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2009/03/cs20090303\\_2bvc000307.html](http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2009/03/cs20090303_2bvc000307.html). Zugegriffen am 04.10.2019.
- Bundesverwaltungsgericht. 2018. Beschluss vom 14.03.2018 – 6 BN 3/17. <https://www.bverwg.de/140318B6BN3.17.0>. Zugegriffen am 04.10.2019.
- Rüttger, Marco. 2016. Online-Hochschulwahlen – (m)ein gutes Recht. *Deutsche Universitätszeitung Magazin* 2016(9): 65–67.
- Solvak, Mihkel, und Kristjan Vassil. 2016. *E-Voting in Estonia*.
- Weiler, Thomas. 2015. Können elektronische Wahlen verfassungsmäßig sein? *KommunalPraxis Wahlen* 6(1): 7–19.



# Liquid Democracy

Julia Schwanholz und Lavinia Zinser

## Inhalt

1 Klärung des Konzepts .....	302
2 Theoretische Grundlagen .....	303
3 Praktische Anwendungsfelder .....	306
4 Umsetzungsstand und Auswirkungen .....	307
5 Perspektiven für Staat und Verwaltung .....	310
Literatur .....	311

## Zusammenfassung

*Liquid Democracy* ist ein Alternativkonzept zur repräsentativen und direkten Demokratie, das die Vorteile von Repräsentation und direktdemokratischer Entscheidung integriert. Es bietet eine Möglichkeit, dauerhaft oder von Fall zu Fall die eigene Stimme entweder selbst abzugeben oder an andere zu delegieren. Im Zuge der Verbreitung digitaler Technologien ist *Liquid Democracy* praktisch umsetzbar geworden: Anwendungsbeispiele in Deutschland konzentrieren sich bisher auf Software-Angebote wie *Adhocracy* und *LiquidFeedback*. Während Pilotprojekte eine beachtliche mediale Aufmerksamkeit auf sich ziehen konnten, war die Bürgerbeteiligung eher zurückhaltend. So geht ihr Einsatz in deutschen Kommunalverwaltungen zurück, während international und mithilfe innovativer Angebote wie der *Blockchain*-Technologie schon wieder neue Umsetzungsfelder für *Liquid Democracy* erschlossen werden.

## Schlüsselwörter

Liquid Democracy · Kommunalpolitik · Repräsentation · Delegation · Demokratie

J. Schwanholz (✉) · L. Zinser

Institut für Politikwissenschaft, Georg-August-Universität Göttingen, Göttingen, Deutschland  
E-Mail: [julia.schwanholz@sowi.uni-goettingen.de](mailto:julia.schwanholz@sowi.uni-goettingen.de); [lzinser@gmx.net](mailto:lzinser@gmx.net)

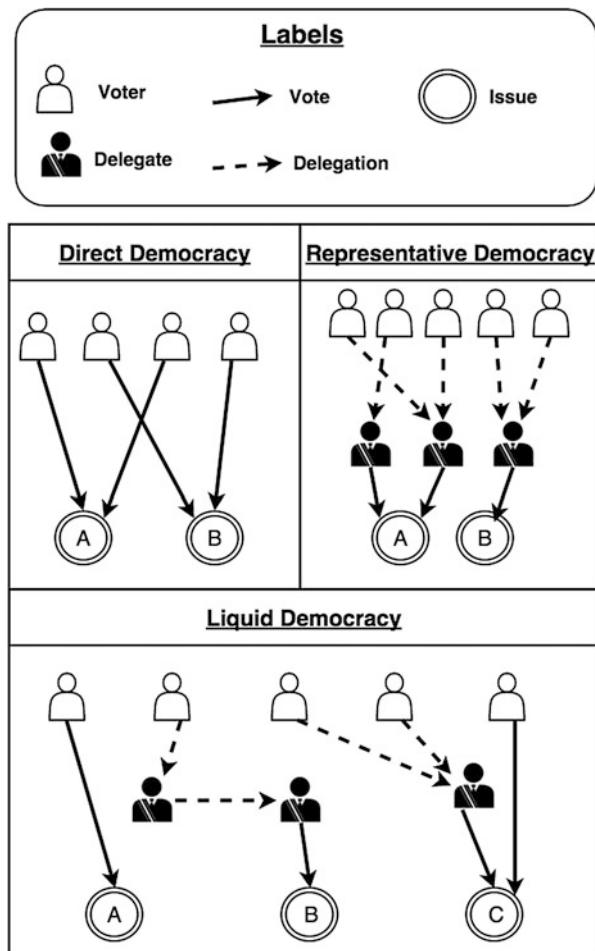
## 1 Klärung des Konzepts

Das Konzept der „Liquid Democracy“ ist ein Alternativvorschlag zur repräsentativen Demokratie. Mit ihrem Kernprinzip demokratischer Selbstbestimmung reagiert die – wörtlich übersetzt – „fließende“ Demokratie auf Defizite des Repräsentationsprinzips, in dem die Gesellschaft in Repräsentierte und Repräsentanten eingeteilt wird und nur letztere legitimiert sind, für alle Bürger bindende Politikentscheidungen zu treffen. Diese Entscheidungen sind weder transparent, noch können die Bürger die für sie geltenden Regeln mitgestalten. Ein Gegenvorschlag zum Repräsentationsprinzip ist die direkte Demokratie, für deren Umsetzung den Bürgern die vollständige Kontrolle über politische Inhalte übertragen wird. Damit wird allerdings gleichzeitig vorausgesetzt, dass alle Bürger sowohl kognitiv in der Lage als auch jederzeit dazu bereit sind, eine Vielzahl an Informationen zu verarbeiten und diese in politische Lösungen zu übersetzen. Aus der Perspektive der *Liquid Democracy* stellt diese Form der Beteiligung aller Bürger jedoch eine Überforderung dar.

In der *Liquid Democracy* sind die Vorteile beider Konzepte kombiniert und in einen neuen Vorschlag integriert worden: Alle kollektiven Entscheidungen sollen mithilfe einer selbstbestimmten Auswahl aus direktdemokratischen und flexibel einsetzbaren repräsentationsdemokratischen Partizipationsmöglichkeiten getroffen werden. In der Umsetzung bedeutet dies, dass jeder Wähler zu jeder Zeit bzw. von Fall zu Fall, entscheidet, ob er seine Stimme direkt abgeben oder sie an eine andere Person delegieren möchte. Auf diese Weise werden die Grenzen zwischen direkter und repräsentativer Demokratie fließend. Da beide Konzepte – also die direkte und die repräsentative Demokratie – entweder als suboptimale Lösung im Sinne proportionaler Repräsentation angesehen werden oder als ungeeignet bewertet werden, um gute Politikentscheidungen zu erzeugen und somit regelmäßig unzufriedene Bürger hinterlassen, erhebt die *Liquid Democracy* den Anspruch, eine vermittelnde Alternative zu sein (Abb. 1).

Der demokratietheoretisch hohe normative Anspruch der *Liquid Democracy*, eine gute Alternative zu den etablierten Demokratiemodellen – wenn nicht sogar das bessere Konzept – zu sein (vgl. Blum und Zuber 2016), steht im Widerspruch zur Komplexität ihrer Umsetzung. Im einfachen Schaubild nicht dargestellt, sind die flexiblen Varianten der *Liquid Democracy*: Neben der Möglichkeit, die eigene Stimme zu delegieren und Stimmen anderer zu erhalten, gibt es auch die Möglichkeit, die erhaltenen Stimmen gesammelt an weitere Delegierte zu übertragen. Es ist zudem auch möglich, die Stimmenübertragung (beispielsweise im Falle von Unzufriedenheit mit dem Abstimmungsverhalten des Delegierten) zu widerrufen. Dies kann sowohl den Einzelfall betreffen, als auch eine ständig thematisch differenzierte Abstimmung (also von Thema zu Thema) zur Folge haben (vgl. Paetsch und Reichert 2012, S. 20). Ohne die informations- und kommunikationstechnischen Voraussetzungen des Internets wäre *Liquid Democracy* praktisch undenkbar. Mithilfe des Internets lässt sich eine netzwerkbasierte Demokratie heute zwar durchaus realisieren (vgl. Reichert und Panek 2014, S. 300). Eingedenk der Tatsache, dass jedoch noch immer nicht alle Mitglieder der Gesellschaft online sind, bleibt das Internet als neu entstandener Raum auch weiterhin nur für die digitale Öffentlichkeit exklusiv. Für die *Liquid Democracy* bedeutet dies, dass bei ihrer Umsetzung ein Teil der Bevölkerung von politischer Partizipation ausgeschlossen bleibt.

**Abb. 1** Direkte, repräsentative und fließende Demokratie im Vergleich.  
(Quelle: Schiener 2015)



## 2 Theoretische Grundlagen

Die Entstehungsgeschichte der *Liquid Democracy* reicht zurück bis ins 19. Jahrhundert. Der britische Schriftsteller Lewis Carroll formulierte den Gedanken von „delegated voting“, d. h. der Übertragung von Stimmrechten bereits im Jahr 1884. Einige Jahre später setzte sich im Bundesstaat Oregon der amerikanische Jurist und politische Aktivist William Simon U'Ren für eine faire, proportionale Repräsentation ein. Er scheiterte allerdings 1912 mit der Forderung eines interaktiven Modells proportionaler Repräsentation, wonach der Einfluss eines gewählten Repräsentanten bei der Verabschiedung eines jeden Gesetzes von der Zahl der von ihm bei seiner eigenen Wahl tatsächlich gewonnenen Stimmen abhängen sollte. Deutlich später als U'Ren entwickelten Gordon Tullock (1967) und James C. Miller (1969) ungefähr zeitgleich ihre Vorschläge für *delegative voting* und *proxy voting*. War U'Ren zu Beginn des

20. Jahrhunderts seiner Zeit noch deutlich voraus, half der technische Fortschritt Tullock und Miller, ihre Visionen einer perfekten proportionalen Repräsentation in eine ernsthafte demokratietheoretische Diskussion zu überführen. Mit der Etablierung des Fernsehens und besonders des Computers wurden komplexe Modelle zur differenzierten Stimmabgabe erstmals auch praktisch denkbar und möglich.

Tullock wollte, dass Wähler Repräsentanten zur Stimmabgabe beauftragen. Wem sie ihre Stimmen geben, sollten sie entlang der Politikthemen flexibel von Fall zu Fall entscheiden können. Dabei sollte es auch möglich sein, sich selbst zu beauftragen. Die Abstimmungsmacht der Repräsentanten orientierte sich in seinem Modell entsprechend am Zuspruch der Wähler. Entscheidend war damit die Anzahl der Stimmen, die für die anstehende Abstimmung an eine Person übertragen wurden. Wollte sich der Wähler selbst repräsentieren, konnte er direkt in das politische Geschehen eingreifen und „*by wire*“ über die entsprechende Politikfrage abstimmen. Seine Abstimmungsmacht war entsprechend seines geringen Stimmengewichts allerdings begrenzt.

Perfekte proportionale Repräsentation bei Miller wird durch eine Integration elektoraler Mechanismen direkter und repräsentativer Demokratie erreicht. Dazu gibt er in seinem Modell den starren Gedanken von Repräsentation auf und führt die Unterscheidung von *proxy* und *direct voting* ein. Sein Ansatz beruht auf vollkommener Freiwilligkeit: Der Wähler entscheidet demnach, ob er seine Stimme dauerhaft an einen Repräsentanten delegieren (*proxy voting*), selbst über politische Sachfragen abstimmen (*direct voting*) oder von Fall zu Fall flexibel abwägen möchte, einen Repräsentanten zu beauftragen bzw. selbst abzustimmen. Aus dem Zeitkontext der 1960er-Jahre blickt Miller in die Zukunft und erwartet binnen weniger Jahrzehnte einen flächendeckenden Zugang aller Haushalte zu Computern. Technische Innovationen, so sein Argument, könnten politische Partizipation erleichtern und die für die Umsetzung seines Konzepts erforderlichen komplexen Abstimmungsmodi ermöglichen.

In der Literatur wurden die Vorschläge von Tullock und Miller aufgegriffen, kritisch diskutiert und teilweise weiterentwickelt. Ihr Ansinnen, die normativen Ideale der direkten und repräsentativen Demokratie in einem vermittelnden Modell zu integrieren, hat zur Fortentwicklung der Demokratietheorie beigetragen. Besondere Beachtung fand zu Beginn des neuen Jahrtausends der Vorschlag einer *delegative democracy* von Bryan Ford (2002). In dem eng an Millers Modellvorschlag angelehnten Konzept kann jeder Bürger zu jeder Politikfrage auch selbst seine eigene Stimme abgeben, einen anderen zur Stimmabgabe im eigenen Namen beauftragen oder auch von anderen als *delegate* (das begrifflich Millers *proxy* entspricht) beauftragt werden. Die Anzahl der Delegierten kann in diesem dynamischen Repräsentationsgeflecht weder von außen vorgegeben noch im Vorhinein festgelegt werden. Denn anders als beim starren Repräsentationsprinzip ändert sich die Zusammensetzung der Gruppe von Repräsentanten bzw. Delegierten ständig, weil der Wähler von Fall zu Fall frei und direkt einen Repräsentanten auswählen und beauftragen kann. An diesem Punkt betont Ford, dass die Legitimation der Delegationskette auf der persönlichen Beziehung zwischen Wähler und Delegiertem beruhe, die wünschenswerterweise von Vertrauen

und Übereinstimmung geprägt sei. Fords Ansatz impliziert, dass alle Wähler bereit sind, sich ständig mit tagespolitischen Themen und Fragen auseinanderzusetzen, um beurteilen zu können, ob sie über die erforderlichen sachpolitischen Kenntnisse für die Entscheidung der anstehenden Politikfrage verfügten oder ihre Stimme an einen Experten delegieren sollten. Dazu müssten sich Bürger wieder vermehrt mit Politik auseinandersetzen, was das Verhältnis von Wählern und Repräsentanten stärken könnte. Auch lässt sich fehlende sachpolitische Expertise vor jeder Entscheidung über das Delegationsprinzip ausgleichen. Gegenüber diesen positiven Motiven ist die Komplexität des Modells der *delegative democracy* allerdings problematisch. Die flexible Übertragung und Kumulation von Stimmen bewirkt, dass die Delegierten nicht wissen, in wessen Namen sie eigentlich abstimmen. Gleichzeitig stimmen sie aber öffentlich ab, damit die Delegierenden sie kontrollieren können. Im Falle von Unzufriedenheit können sie somit bei nächster Gelegenheit die eigene Stimme an eine andere Person übertragen oder alternativ selbst abstimmen.

In der deutschsprachigen Literatur (vgl. Dobusch und Pick 2012) wird erstens beklagt, dass das, was in der repräsentativen Demokratie als defizitär kritisiert wird, nämlich ein Mangel an Transparenz, Verantwortlichkeit und Kontrolle, in der fließenden Demokratie noch viel weniger zu realisieren sei. Wenn jeder Bürger zwar nach Belieben partizipieren dürfe, unter den Bedingungen des sog. *digital divide* aber gar nicht partizipieren könne, so wird ein Folgeproblem offenkundig. Mit *digital divide* ist die Spaltung zwischen Internet-Nutzern und Nicht-Internet-Nutzern gemeint, für die es unterschiedliche Gründe geben kann: Der Zugang zum Internet ist beispielsweise noch immer altersabhängig. So ist die jüngere Generation, die sog. *digital natives*, wie selbstverständlich und ständig *online*, während zwar mehr und mehr, aber weiterhin nicht alle älteren Menschen das Internet nutzen. Es kann zudem von finanziellen Ressourcen abhängen, ob Menschen über einen Internetzugang und die erforderliche *Hardware* verfügen. Auch ist die Infrastruktur und Netzbdeckung ein Hinderungsgrund, nach eigenem Belieben online sein zu können. Schließlich sind ideologische Gründe anzuführen, wie eine Enthaltsamkeit zum Schutz der eigenen Daten und Privatsphäre, weshalb sich Menschen der virtuellen Welt verschließen. Für die Umsetzung eines *delegative democracy*-Modells blieben also aufgrund des Technikeinsatzes zahlreiche Menschen außen vor.

Es wird in der Literatur zweitens bezweifelt, welche Politikfelder mithilfe von *Liquid Democracy* überhaupt entschieden werden können (vgl. Merkel 2015). Offenkundig gibt es politische Fragen, wie etwa jene nach Krieg und Frieden, die nicht dem Prinzip unüberschaubarer, mehrfacher Stimmdelegation und -kumulation unterworfen werden sollten, wenn am Ende unsicher ist, ob das Abstimmungsergebnis die ursprüngliche Intention derjenigen, die ihre Stimmen delegiert haben, auch tatsächlich entspricht. Gleches gelte ebenso für sog. *high politics* wie Innen-, Finanz- und Wirtschaftspolitik.

Jüngere Beiträge der einschlägigen Literatur distanzieren sich vom ursprünglichen Ansinnen, das Konzept der *Liquid Democracy* als ein Staatskonzept zu etablieren und ziehen sich auf Minimaldefinitionen zurück, die einerseits den deliberativen Charakter des Konzepts betonen und es andererseits von digitalem

Verwaltungshandeln (*E-Government*) abgrenzen. Flüssige Demokratie wird damit als ein onlinegestütztes Verfahren zur intensiveren diskursiven Auseinandersetzung und Deliberation erfasst, das das Ziel verfolgt, einen „*Direkten Parlamentarismus*“ und eine Beteiligungsdemokratie zu realisieren (vgl. Adler 2018).

---

### 3 Praktische Anwendungsfelder

Im deutschen Kontext zeigen sich Anwendungsbeispiele für Liquid Democracy, seitdem diese über *Software*-Angebote umsetzbar geworden ist. Entsprechende Projekte existieren seit 2009 (vgl. Brabanski und Kettner 2015, S. 21): Sowohl der Verein *Liquid Democracy e.V.* wurde in diesem Jahr gegründet, als auch *Liquid-Feedback* wurde im selben Jahr vom Verein *Public Software Group e.V.* (später Interaktive Demokratie e.V.) veröffentlicht. Anwendung findet *Liquid Democracy* gegenwärtig vor allem bei innerparteilichen Prozessen (wofür nach eigenen Angaben die *Software*-Hersteller ihre Anwendungen ursprünglich entwickelt hatten), wohingegen es im Bereich der öffentlichen Verwaltung, der im Zentrum dieses Handbuches steht, noch relativ wenige Umsetzungsbeispiele gibt. Dies hat vor allem auch damit zu tun, dass sich das im US-amerikanischen Kontext als *delegative democracy* entwickelte Konzept einer *Liquid Democracy* nur bedingt auf Deutschland übertragen lässt und re-kontextualisiert werden muss. Die politischen Systeme der USA und Deutschlands unterscheiden sich deutlich voneinander und können nicht ohne weiteres miteinander verglichen werden. Grundlegende Kontextbedingungen zwischen den Ländern stimmen nicht überein: Das Delegationsprinzip kommt in Deutschland in Verbänden, Vereinen oder politischen Parteien zur Anwendung, nicht aber in der staatlichen Verwaltung. Insofern eine Übertragung eins zu eins erfolgt, würde man für die Praxis der *Liquid Democracy* in Deutschland erwarten, dass Experimente in Kommunalverwaltungen und politischen Institutionen weit weniger erfolgreich verlaufen, als dies in den USA der Fall ist. Rückt man hingegen vom Prinzip der Delegation als Markenkern der *Liquid Democracy* ab und betont stärker ihren deliberativen Charakter, so ändert sich auch der Bewertungsmaßstab für den Stand der Umsetzung. Die Aufmerksamkeit liegt in dem Fall auf diskursiver Beteiligung und nicht so sehr auf dem Ausgang des Verfahrens, der Entscheidung oder dem Ergebnis. Jüngere Beiträge empfehlen diese Sichtweise auf *Liquid Democracy* für den bundesrepublikanischen Kontext (vgl. Adler 2018). Ihnen wollen wir folgen.

*Liquid Democracy* wird in Deutschland über zwei *Software*-Angebote umgesetzt: *Adhocracy* und *LiquidFeedback*. Der Verein *Liquid Democracy e.V.* hat *Adhocracy* als *Software*-Lösung entwickelt und dabei den Schwerpunkt auf den Diskurs und nicht auf Stimmendelegation gelegt. Dies zeigt sich anschaulich in der Umsetzung der *Software*, wo repräsentativ- und deliberativ-demokratische Elemente gegenüber direktdemokratischen klar überwiegen. So bietet die *Software* die Möglichkeit an, einen Diskussionsverlauf chronologisch zu dokumentieren und jede Textänderung festzuhalten. Ablesbar in einem sich ständig wandelnden Textkorpus, verschmelzen über diesen Weg Diskurs und Abstimmung ineinander und reifen zu einem fertig

---

ausformulierten und im Prozess sukzessive verabschiedeten Dokument. *Adhocracy* wird in der Regel von politischen Parteien und Vereinen, seltener von Kommunen eingesetzt, um einen Konsens oder Mehrheitsbeschluss über Textvorschläge (etwa Satzungen oder Gesetzesvorschläge) herzustellen.

Der Verein *Interaktive Demokratie e.V.* (vormals Public Software Group e.V.) betreibt die *Software-Lösung LiquidFeedback*. Ihr Ansatz integriert direkt- und repräsentativdemokratische Elemente. *LiquidFeedback* wird vor allem von kommunalen Verwaltungen eingesetzt und ist über verschiedene Phasen organisiert, in denen Initiativen eingebracht und diskutiert werden können. Am Ende steht zumeist eine digitale Abstimmung, die ein Stimmungsbild vor der verbindlichen Endabstimmung in einem entsprechenden repräsentativ-demokratisch besetzten Gremium erzeugen soll.

Der Einsatz von *Software* in Deutschland soll transparente politische Entscheidungsprozesse bewirken und Bürgerbeteiligung erhöhen. Während dies eine kostengünstige Möglichkeit bietet, um Diskussions- und Abstimmungsforen einzurichten und für bestimmte Verwaltungszwecke zu nutzen, sind die Folgen, wie etwa der Personalaufwand für den Betrieb und die Pflege der Foren, kostenintensiv. Welche Anwendungsbeispiele es für *Liquid Democracy* und die beiden vorgestellten *Software*-Lösungen gibt, wird im Folgenden veranschaulicht.

---

## 4 Umsetzungsstand und Auswirkungen

Das prominenteste Anwendungsbeispiel der *Software Adhocracy* war ihr Einsatz in der Enquête-Kommission „Internet und digitale Gesellschaft“ im Deutschen Bundestag. Im Jahr 2011 hat der Bundestag mit *enquetebeteiligung.de* erstmalig eine *Online*-Beteiligungsplattform in Betrieb genommen. Vorausgegangen waren Monate kontroverser Diskussionen zwischen direkt beteiligten und angrenzenden Akteuren der Bundestagsverwaltung, des Ältestenrates und Enquête-Mitgliedern über die Relation von Kosten und Ertrag sowie die Möglichkeiten und Grenzen der Beteiligung (v. a. die Gefahren von Ausgrenzung). Schließlich wurde die Partizipationsplattform nicht wie ursprünglich angedacht von offizieller Stelle über die Bundestagsverwaltung angeboten, sondern als kostenfreies Portal vom Verein *Liquid Democracy e.V.* organisiert und betrieben. Die Enquête-Kommission bestand aus 17 Bundestagsabgeordneten (und 17 Stellvertretern) sowie 17 unabhängigen Sachverständigen. Die Plattform *enquetebeteiligung.de* diente gewissermaßen als 18. Sachverständige. Über sie sollten interessierte Bürger, Organisationen und Interessensgruppen in die Projektgruppenarbeit einbezogen werden. Monatlich besuchten rund 30.000 Besucher die Plattform; 3299 Besucher waren insgesamt registriert und können als Nutzer gezählt werden. Die Aktivität dieser registrierten Nutzer war entlang der unterschiedlichen Projektgruppen der Enquête-Kommission divers und rangierte zwischen neun und 82 eingebrachten Vorschlägen pro Themengruppe. Insgesamt wurden über die Plattform 493 Vorschläge eingebracht, zu denen 2353 Kommentare und 14.603 Stimmen abgegeben wurden.

Ein zweites Beispiel für die Nutzung von *Adhocracy* ist *OffeneKommune.de*. Die mittlerweile nicht mehr aktiv geschaltete Beteiligungsplattform stand allen Kommunen in Deutschland offen und bot Bürgern, Amtsträgern, Vereinen und Unternehmen die Möglichkeit zur Anmeldung im Portal ihrer Stadt (unter *NamederKommune.offenekommune.de*). Die Idee der Plattform war es, Abstimmungen, Initiativen und Vorschläge von allen Nutzern *online* einbringen und auch abstimmen lassen zu können. Dabei konnten Mandatsträger über sich selbst und ihre politische Funktion mittels eines Etiketts (sog. *Badge*) informieren. Auf *OffeneKommune.de* waren insgesamt 52.370 Nutzer (aus potenziell allen Kommunen Deutschlands) angemeldet, was eine im Vergleich zur Gesamtzahl potenzieller Nutzer aller Kommunen Deutschlands sehr geringe Zahl ist. Während die Plattform mittlerweile eingefroren ist, ist die *Adhocracy-Software* als *Open-Source*-Lösung weiterhin nutzbar.

Die Beteiligungsplattform *mein.berlin.de* ist als ein drittes Anwendungsbeispiel anzuführen. *Meinberlin.de* stellt eine Weiterentwicklung der *Adhocracy-Software* dar. Über die von der Senatsverwaltung finanzierte Plattform können alle Verwaltungen des Landes Berlin die Bürger seit August 2015 informieren oder zur Beteiligung an Onlineverfahren aufrufen. Die niedrigschwellige Akkreditierung (Benutzername, E-Mail-Adresse und Passwort) vereinfacht eine Partizipation. In der Literatur wird das Beispiel als Beteiligungsinfrastruktur gelobt (Adler 2018, S. 168), die einen direkten Parlamentarismus ermögliche. Der modulare Aufbau der *Software* gestattet die Integration weiterer *Liquid-Democracy*-Aspekte, wie ein Identitäts-Management der Wähler, die Sicherung von Abstimmungsdaten (in Form von Datenbank-Speicherungen) oder eine Stimmendelegation.

Die zweite *Software* *LiquidFeedback* wird in der Regel von Verwaltungen eingesetzt. Ein Jahr nachdem die Enquête-Kommission „Internet und digitale Gesellschaft“ im Deutschen Bundestag damit begonnen hatte, mit *Adhocracy* zu experimentieren, schaltete der Landkreis Friesland seine Plattform *LiquidFriesland* über die *Software* *LiquidFeedback online*. Damit erhielten die Bürger ab 2012 mehr Möglichkeiten zur Partizipation und direkter Beteiligung an politischen Entscheidungen. Konkret konnten alle in Friesland gemeldeten Bürger ab 16 Jahren Anträge über die *Online*-Plattform einreichen. Der Landkreis Friesland war damit Vorreiter unter allen Kommunalverwaltungen Deutschlands. Parallel dazu konnte auch die Kreisverwaltung Themen setzen und über diese abstimmen lassen. Anträge, die ein Quorum erreichten, wurden zur Kommentierung und Änderung zugelassen. Anträge, die mit der Mehrheit der abgegebenen Stimmen beschieden wurden, wurden anschließend im Kreistag behandelt. Zwar konnten einige Anträge so ihren Eingang in den Kreistag finden, aber erst dort wurden sie im repräsentativ-demokratischen Verfahren verbindlich abgestimmt und entschieden. Anliegen, die vorher Unterstützung in der Bevölkerung gefunden hatten, konnten entsprechend im Kreistag durchfallen, wenn sie von den Abgeordneten abgelehnt wurden. Das *LiquidFriesland*-Onlinebeteiligungsprojekt hat vor allem aufgrund seiner Vorreiterrolle für die deutschen Kommunalverwaltungen eine hohe mediale Aufmerksamkeit erfahren. Und doch war die Bürgerbeteiligung eher schwach: Binnen dreieinhalb Jahren (bis zur Abschaltung der Plattform Anfang 2016 aufgrund zu geringer Aktivität) wurden nur 76 Initiativen von 30 Bürgern sowie 14 Initiativen von der

Kreisverwaltung eingereicht und zur Abstimmung gestellt. Die Beteiligung am Diskurs blieb mit weniger als 600 von rund 83.000 wahlberechtigten Einwohnern sehr überschaubar. Seit Ende 2016 hat der Landkreis unter *liquidfriesland.de* ein reduziertes Portal zur Einreichung von Vorschlägen eingerichtet. Es bietet jedoch keine Möglichkeit für Onlinediskussionen und Abstimmungen, sondern zielt ausschließlich auf die Artikulation gesellschaftlich relevanter Themen ab. Mit rund 35 eingereichten Vorschlägen zwischen 2016 und 2018 wurde auch dieses neue Portal des Landkreises Friesland kaum genutzt. Ob sich die Akzeptanz hierdurch erhöht, ist fraglich.

Die Plattformen des Landkreises Rotenburg (Wümme), *Bürgerplattform ROW*, und die der niedersächsischen Städte Seelze, *SeelzeDirekt*, und Wunstorf, *wunstorf-direkt*, sind weitere Beispiele für die Anwendung von Liquid Democracy auf Kreisebene in Deutschland. Alle drei wurden im Jahr 2015 als eigene Beteiligungsplattformen gestartet und nutzten die Open-Source-Software LiquidFeedback. Dabei unterschieden sie sich nur geringfügig voneinander. Zu den berechtigten Teilnehmern zählten alle Bürger mit einem Mindestalter von 16 Jahren, die sich über den Verifikationsprozess (Klarnamenpflicht, Validierung über das Einwohner-Melderegister und Freischaltung über Aktivierungs-Code) angemeldet hatten. Die eingebrachten Themen wurden den Ausschüssen der kommunalen Gremien zugeordnet. Die Beteiligungsquoten waren schließlich auch bei diesen Anwendungsbeispielen mit rund einem Dutzend Nutzern – abgesehen von positiven Ausnahmen – gering und wurden schließlich eingestellt.

Für die Fallbeispiele *Offenekommune.de*, *Meinberlin.de*, *LiquidFriesland*, *Bürgerplattform ROW*, *SeelzeDirekt* und *wunstorf-direkt* lässt sich festhalten, dass eine geringe Partizipation an den kommunalen Angeboten nach kurzer Zeit deren Absetzung und Einstellung begründete. Abgesehen von zu geringer Beteiligung kann der Vorreiter *LiquidFriesland* unter ihnen am ehesten als ein gelungenes Beispiel für *Bottom-up*-Partizipation beurteilt werden. Bürger hatten ihre Vorstellungen und Meinungen als Diskussionsbeiträge, Zustimmungen, Enthaltungen oder Ablehnungen zu den eingebrachten Politikanträgen schriftlich artikuliert. Die politischen Entscheidungsträger konnten auf diese Weise, einen Eindruck von gesellschaftlichen Stimmungen gewinnen, auch wenn das Ergebnis nicht repräsentativ war.

Das Pilotprojekt im Deutschen Bundestag stellt insofern eine Ausnahme unter den vorgestellten Fallbeispielen dar, als dass es nicht kommunal und zudem von Beginn an auf die Dauer der Arbeit der Enquête-Kommission beschränkt angelegt, also zeitlich befristet war. Die eingesetzte Plattform wurde nicht vom Deutschen Bundestag, sondern kooperativ vom Verein Liquid Democracy e.V. (also von außen) bereitgestellt und betrieben. Im Verlauf traten technische, administrative und rechtliche Probleme auf, die aufgrund des Pilotcharakters im Vorfeld kaum zu antizipieren waren (darunter der Verzicht auf Klarnamenpflicht bei der Registrierung). Die mediale Beachtung und Beobachtung war national wie international hingegen enorm. So kann am Ende zwar keine Rede von einem durchschlagenden Partizipationserfolg sein, weil die aktive Beteiligung auf der Plattform quantitativ zwar vergleichsweise am höchsten, aber absolut betrachtet doch eher gering war. Die Qualität der Beiträge hätte zudem erhöht werden können, wenn die unterwegs aufgetretenen Defizite flexibel und unmittelbar

behoben worden wären. Und dennoch hat das Experiment gezeigt, dass eine Beteiligung von Bürgerinnen und Bürgern an der Parlamentsarbeit von außen möglich ist, was national wie international ein Novum war und in einer sehr positiven medialen Berichterstattung gewürdigt wurde.

Die ersten Versuche, *Liquid Democracy* im bundesrepublikanischen Kontext umzusetzen, sind damit differenziert zu beurteilen: Erstens kann festgehalten werden, dass alle Fallbeispiele ambitionierte Beteiligungsversuche dokumentieren, die das Ziel verfolgten, eine modernere (onlinegestützte), transparentere und bürger-nähre (Kommunal-)Politik umzusetzen. Zweitens wurden die *Liquid Democracy*-Lösungen an das jeweilige Anforderungsprofil der Anwendungen angepasst (vgl. Adler 2018, S. 190–191): In den *LiquidFeedback*-Anwendungen konnten falsche oder missbräuchliche Nutzerangaben etwa als Ordnungswidrigkeit geahndet werden. Die Mandatsträger in den Kreistagen oder Stadt- und Ortsräten sowie Mitarbeitende in den Fachbereichen der Verwaltung waren zur Teilnahme – anders als bei *Adhocracy* – nicht zugelassen. Die Angebote hatten drittens in keinem Fall bindende Wirkungen, sondern können nur als *Feedback*-Instrumente und Beteiligungsmöglichkeiten zum Einfangen situativer Meinungs- und Stimmungsbilder der Bürger betrachtet werden. Auf Delegationsmechanismen, wie ein solcher im Kernkonzept der *delegative democracy* angelegt ist, wurde in allen Anwendungen bewusst verzichtet, wobei das Erreichen einer notwendigen Abstimmungsbeteiligung für die weitere Behandlung in den offiziellen Gremien der Institutionen als Ansatz für ein Delegationsquorum zu werten ist. Schließlich hat sich viertens übereinstimmend gezeigt, dass Bürgerbeteiligung kein Selbstläufer ist. Alle Beteiligungsergebnisse waren zu gering, um die Angebote in einem vernünftigen Kosten-Nutzen-Verhältnis dauerhaft zu etablieren.

---

## 5 Perspektiven für Staat und Verwaltung

Die Anwendungsbeispiele haben gezeigt, wie *Liquid Democracy* in Deutschland bisher umgesetzt worden ist. In deutschen Kommunalverwaltungen müssen Vorteile und Nachteile gegeneinander abgewogen werden. Bisher genutzte und in diesem Beitrag behandelte Software-Lösungen basieren auf *Open-Source*-Projekten, die von gemeinnützigen Vereinen getragen werden. Sie sind im Vergleich zu kommerziellen Angeboten kostengünstiger und dabei individuell einsetzbar. Allerdings haben sie auch Nachteile wie etwa Supportdefizite oder einen hohen Schulungsaufwand für die Nutzer bei regelmäßiger technischer Weiterentwicklung. Zudem ist der personelle Aufwand für die Betreiber einer Plattform bedeutsam. Stehen Aufwand und Ertrag in keinem vernünftigen Verhältnis, so lässt sich eine Umsetzung kaum längerfristig rechtfertigen. In den Ertrag müssen die Nutzerzahlen eingerechnet werden: Das wohl größte Problem der Plattformen ist die (zu) geringe Partizipationsquote. Die Mehrheit der Internetnutzer sieht keine Vorteile in einer Beteiligung an *Liquid Democracy* und enthält sich stattdessen den angebotenen Formaten. Dabei spielen für den Wert von Plattformen gerade Netzwerkeffekte eine zentrale Rolle, d. h. ihr Wert hängt entscheidend von der Nutzerzahl ab.

Aus demokratietheoretischer Sicht ist zu bedenken, dass der bisherige *Output* nie bindend für politische Gremien und deren Entscheidungen gewesen ist. Das Delegationsprinzip wurde also bislang nicht angewendet. Die Akzeptanz von *Liquid Democracy* (als alternatives oder ergänzendes Angebot zur repräsentativen Demokratie) könnte vor allem dadurch erhöht werden, dass eine Verbindung zwischen den Abstimmungsergebnissen auf den Plattformen und den späteren konkreten politischen Inhalten hergestellt wird.

Außerhalb Deutschlands wird *Liquid Democracy*, nachdem es durch die weltweite Verbreitung digitaler Technologien praktisch umsetzbar geworden ist, zügig weiterentwickelt. Neue Anwendungsfelder werden in den USA unter dem Label „Crypto-Democracy“ im Kontext der *Distributed-Ledger*-Technologie (z.B. *Blockchain*) erschlossen. Neben den bereits bekannten Feldern der Kryptowährungen wird die *Distributed-Ledger*-Technologie dazu auch für digitales Wählen eingesetzt. So kann die Identität von Wählern vollständig geheim gehalten und trotzdem unveränderlich zugeordnet und damit nachprüfbar gemacht werden. Bisher werden solche Projekte, die teilweise oder vollständig mit *Blockchain*-Technologien arbeiten, in der kommunalen Verwaltung (z. B. *DemocracyOS* in der Stadtverwaltung von Buenos Aires) oder auf Parlamentsebene (z. B. *United. vote* im US-Bundesstaat Kalifornien) eingesetzt. Zeitverzögert schwappen diese Projekte auch nach Europa herüber (z. B. für die Notarisierung öffentlicher Daten durch *Blockchain* in der Wiener Stadtverwaltung), während die deutsche Verwaltung allerdings längst noch nicht so weit ist, derartige Technologien in entsprechenden Pilotprojekten zu erproben. Mit den in diesem Beitrag beschriebenen *Software*-Lösungen lassen sich überprüfbare Identitäten nicht darstellen und auch die Geheimhaltung von Wahlen ist nicht widerspruchsfrei umzusetzen. Die bisher umgesetzten *Liquid-Democracy*-Projekte in Deutschland genießen zwar national Vorreiterpositionen, sind aber angesichts der Fülle neuer Angebote im globalen Vergleich kaum mehr innovativ, wenn es darum geht, Bürger *online* an politischen Entscheidungen zu beteiligen. Dass die Angebote überdies kaum angenommen wurden, unterstreicht einmal mehr empirisch die deutsche Skepsis gegenüber *Liquid Democracy*.

---

## Literatur

- Adler, Anja. 2018. *Liquid Democracy in Deutschland. Zur Zukunft digitaler politischer Entscheidungsfindung nach dem Niedergang der Piratenpartei*. Bielefeld: transcript.
- Blum, Christian, und Christina Isabel Zuber. 2016. Liquid democracy. potentials, problems, and perspectives. *The Journal of Political Philosophy* 24(2): 162–182.
- Brabanski, Oskar, und Matthias Kettner. 2015. Chancen und Risiken von Liquid Democracy für die politische Kommunikation. In *Cyber-Sicherheit. Studien zur Inneren Sicherheit 18*, Hrsg. Hans-Jürgen Lange und Astrid Bötticher, 19–38. Wiesbaden: Springer.
- Dobusch, Leonhard, und Yussi Pick. 2012. *Parteidemokratie #4: Liquid Democracy in Theorie und Praxis (Update)*. <http://blog.sektionacht.at/2012/06/parteidemokratie-4-liquid-democracy-in-theorie-und-praxis/>. Zugegriffen am 29.10.2019.
- Ford, Bryan. 2002. *Delegative democracy*. <http://www.brynosaurus.com/deleg/deleg.pdf>. Zugegriffen am 29.10.2019.

- Merkel, Wolfgang. 2015. *Nur schöner Schein? Demokratische Innovationen in Theorie und Praxis, OBS-Arbeitsheft 80*. Frankfurt a. M.: Otto Brenner Stiftung.
- Paetsch, Jennifer, und Daniel Reichert. 2012. Liquid Democracy. Neue Wege der politischen Partizipation. *vorgänge* 51(4): 15–26.
- Reichert, Daniel, und Eva Panek. 2014. Alles ist im Fluss – die fließenden Ebenen einer Liquid Democracy. In *Internet und Partizipation. Bottom-up oder Top-down? Politische Beteiligungsmöglichkeiten im Internet*, Hrsg. Katrin Voss, 299–310. Wiesbaden: Springer VS.
- Schiener, Dominik. 2015. *Liquid democracy: True democracy for the 21st century*. <https://medium.com/organizer-sandbox/liquid-democracy-true-democracy-for-the-21st-century-7c66f5e53b6f>. Zugriffen am 29.10.2019.



---

# Elektronische Gesetzgebung

Axel Piesker, Patrick Schweizer und Carolin Steffens

## Inhalt

1 Klärung des Begriffs .....	313
2 Theoretische Grundlagen .....	315
3 Praktische Anwendung .....	317
4 Künftige Entwicklung .....	321
Literatur .....	323

---

## Zusammenfassung

Elektronische Gesetzgebung bezeichnet ein durchgängig elektronisches Verfahren vom Textentwurf bis zur Verkündung eines Gesetzes, das Format- und Medienbrüche vermeiden und sowohl den Aufwand als auch die Fehleranfälligkeit einzelner Prozessschritte verringern soll. Sie kann – abhängig von ihrer konkreten Ausgestaltung und ihrer Akzeptanz durch die am Verfahren beteiligten Akteure – zu einer Verbesserung der Qualität der Gesetzgebung beitragen.

---

## Schlüsselwörter

Verwaltungsmodernisierung · E-Government · Bessere Rechtsetzung ·  
Gesetzgebungsverfahren · Elektronische Verkündung

---

## 1 Klärung des Begriffs

Der Gesetzgebung kommt in der Demokratie eine zentrale Rolle zu, da Gesetze die Lebensverhältnisse von Menschen gestalten und ihr sicheres Zusammenleben in einem Staat gewährleisten. Das Bundesverfassungsgericht hat die grundlegende

---

A. Piesker (✉) · P. Schweizer · C. Steffens  
Deutsches Forschungsinstitut für öffentliche Verwaltung, Speyer, Deutschland  
E-Mail: [piesker@foev-speyer.de](mailto:piesker@foev-speyer.de); [schweizer@foev-speyer.de](mailto:schweizer@foev-speyer.de); [steffens@foev-speyer.de](mailto:steffens@foev-speyer.de)

Bedeutung des förmlichen Gesetzes und damit auch der Gesetzgebung durch seine Wesentlichkeitstheorie unterstrichen, nach der alle wesentlichen Entscheidungen per Gesetz getroffen werden müssen (Fliedner 2013, S. 20–21).

Am Gesetzgebungsverfahren, das von den ersten Überlegungen zur Erarbeitung eines Gesetzentwurfs bis zur Verkündung des verabschiedeten Gesetzes im Bundesgesetzblatt reicht, sind in Deutschland auf Bundesebene verschiedene Verfassungsorgane und Akteure beteiligt. Der Bundestag berät und beschließt die aus seiner Mitte, von der Bundesregierung oder vom Bundesrat eingebrochenen Gesetzentwürfe. Der Großteil der im Bundestag behandelten und beschlossenen Gesetze stammt von der Bundesregierung, die aufgrund der in der Ministerialverwaltung vorhandenen fachlichen Expertise eine wichtige Rolle bei der Gesetzesvorbereitung spielt. Gemäß der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO) ist die Einbeziehung weiterer Akteure (z. B. Verbände, Gewerkschaften, kommunale Spitzenverbände, Nationaler Normenkontrollrat) vorgesehen.

Der Bundesrat kann ebenfalls selbst Gesetzentwürfe einbringen, zu den ihm zugeleiteten Gesetzentwürfen eine Stellungnahme abgeben oder muss über zustimmungspflichtige Vorhaben abstimmen. Weitere am Gesetzgebungsverfahren auf Bundesebene beteiligte Akteure sind der Vermittlungsausschuss, der bei Uneinigkeiten im Gesetzgebungsverfahren zwischen Bundestag und Bundesrat vermitteln soll, sowie der Bundespräsident, der für die Ausfertigung aller vom Deutschen Bundestag beschlossenen Gesetze zuständig ist.

Die Gestaltung des formalen Gesetzgebungsverfahrens ist an unterschiedlichen Stellen geregelt. Während das Grundgesetz Aufgaben, Befugnisse und Zusammenwirken der an der Gesetzgebung beteiligten Verfassungsorgane (Art. 76–78 und 82 GG) festlegt, erfolgt eine weitere Konkretisierung des Verfahrens in den Geschäftsordnungen der Bundesministerien, des Bundestags, des Bundesrats und der Bundestagsfraktionen. Diese Regelungen bilden im Wesentlichen die Grundlage für die formale Gesetzgebungsarbeit. Neben den dort festgelegten Verfahrensschritten existieren jedoch auch informale Prozesse im Gesetzgebungsverfahren, die mit informalem Politik- und Verwaltungshandeln einhergehen. Dieses zeichnet sich dadurch aus, dass es nicht rechtlich geregelt und auf keine Rechtsfolgen, sondern auf tatsächliche Erfolge gerichtet ist (Ismayr 2008, S. 389; Bohne 2018, S. 238). Hierbei handelt es sich beispielsweise um politische und administrative Aushandlungs- und Abstimmungsprozesse, die im Laufe des Gesetzgebungsverfahrens stattfinden.

Im Zusammenhang mit Maßnahmen zur Verwaltungsmodernisierung und zum Bürokratieabbau gab es in den vergangenen Jahren auf staatlicher Seite verschiedene Digitalisierungsbemühungen, die unter dem Oberbegriff *E-Government* oder mittlerweile auch *Smart Government* zusammengefasst werden können. Obwohl es sich bei der Gesetzgebung um das wichtigste verfassungsorganübergreifende Verfahren handelt, wurde sie im Rahmen der deutschen *E-Government*-Aktivitäten bisher eher „stiefmütterlich“ behandelt. Bereits heute werden verschiedene Softwarelösungen und Plattformen an verschiedenen Stellen des Gesetzgebungsprozesses genutzt, ein umfassender Ansatz fehlt bislang jedoch. Erst im Rahmen des Regierungsprogramms „Digitale Verwaltung 2020“ aus dem Jahr 2014 griff die Bundesregierung

das Thema der Digitalisierung des Gesetzgebungsverfahrens auf und rief das Projekt „elektronisches Gesetzgebungsverfahren“ („eGesetzgebung“) ins Leben (Bundesministerium des Innern 2014). Obwohl es sich um ein Programm der Bundesregierung handelt, sieht das Projekt die Entwicklung eines Unterstützungsangebots für alle am Gesetzgebungsverfahren beteiligten Akteure vor.

Elektronische Gesetzgebung im Sinne des Regierungsprogramms soll den Gesetzgebungsprozess von der Entwurfserstellung bis zur Verkündung des Gesetzes durch moderne Informationstechnologie unterstützen, der dadurch vollständig elektronisch, medienbruchfrei und interoperabel wird. Bisher bestehende Medienbrüche im Prozess innerhalb der Bundesregierung, des Bundestags, des Bundesrats, des Vermittlungsausschusses und des Bundespräsidialamts sowie zwischen diesen Institutionen sollen damit abgebaut werden. Zudem soll dies zu einer Arbeitsentlastung und zu einer Verbesserung der Qualität der Regelungsentwürfe führen (Bundesministerium des Innern 2014, S. 37–38). Durch die Aufnahme des Projekts eGesetzgebung in das Arbeitsprogramm „Bessere Rechtsetzung und Bürokratieabbau 2018“ unterstreicht die Bundesregierung die Bedeutung der Maßnahme. Insbesondere wird hier auf innovative und bedarfsgerechte Unterstützungsangebote (z. B. elektronische Textabstimmung, digitalisierte Arbeitshilfen) hingewiesen, die im Gesetzgebungsprozess fortlaufend zur Verfügung gestellt werden sollen (Bundeskanzleramt 2018, S. 4).

---

## 2 Theoretische Grundlagen

Das Gesetzgebungsverfahren ist durch vielfältige Koordinierungs-, Beteiligungs- und Abstimmungsprozesse gekennzeichnet, an denen verschiedene Verfassungsgänge und Akteure beteiligt sind. Dadurch ergibt sich eine Reihe von Schnittstellen, an denen es zu einem Austausch von relevanten Informationen und Dokumenten zum Gesetzesvorhaben zwischen verschiedenen Stellen kommt.

Bei Gesetzentwürfen der Bundesregierung, die den größten Anteil der eingebrachten Gesetzesinitiativen ausmachen, können Beteiligungs- und Abstimmungsprozesse auf drei unterschiedlichen Ebenen ablaufen. Auf intraministerieller Ebene ist es beispielsweise erforderlich, dass das für die Ausarbeitung eines Gesetzentwurfs zuständige Referat gemäß § 15 Abs. 1 GGO alle Arbeitseinheiten innerhalb des Ressorts, deren Zuständigkeiten durch das Vorhaben berührt sind, beteiligt (sog. Hausabstimmung). Bei Einwänden anderer Referate werden weitere Abstimmungen auf den nächsthöheren Hierarchieebenen notwendig (z. B. Einbindung der (Unter-) Abteilungsleiter- und Staatssekretärsebene). Umfangreichere Änderungen im Verlauf des Gesetzgebungsverfahrens erfordern in der Regel eine erneute Hausabstimmung vor der Einbringung des Gesetzentwurfs in das Kabinett (Bundesministerium des Innern 2012, S. 69).

Auf interministerieller Ebene gibt es ebenfalls verschiedene Abstimmungs- und Beteiligungsprozesse. Zu nennen ist hier die gemäß § 45 Abs. 1 GGO durchzuführende Beteiligung der betroffenen Ressorts sowie der Beauftragten der Bundesregierung und der Bundesbeauftragten. Zudem sind Beteiligungs- und Abstimmungs-

prozesse mit weiteren Verfassungsorganen und Akteuren vorgeschrieben. So sollen – sofern die Belange der Länder und Kommunen berührt sind – gemäß § 41 GGO vor Abfassung eines Entwurfs die Auffassungen der Länder sowie der kommunalen Spitzenverbände eingeholt werden. Bei Gesetzesvorhaben der Bundesregierung ist auch der Nationale Normenkontrollrat (NKR) zu beteiligen, der zum ermittelten Erfüllungsaufwand, der durch ein geplantes Gesetz verursacht wird, Stellung nehmen kann. Die Beteiligung des NKR erfolgt zur gleichen Zeit wie die der Ressorts (Bundesministerium des Innern 2012, S. 70–74). Nachdem der Gesetzentwurf vom Kabinett beschlossen wurde, erfolgt die Einbeziehung des Bundesrats, der eine Stellungnahme abgeben kann (erster Durchgang). Diese wird durch die ressort- und fachbezogen arbeitenden Ausschüsse vorbereitet und im Plenum des Bundesrats beschlossen. Im Falle der Abgabe einer Stellungnahme kann die Bundesregierung sich hierzu äußern. Die Bundeskanzlerin bringt den Gesetzentwurf mit der Stellungnahme des Bundesrates sowie der Gegenäußerung der Bundesregierung in den Bundestag ein (Bundesministerium des Innern 2012, S. 75–85).

Im Bundestag erfolgt die parlamentarische Beratung zu einem Gesetzentwurf in der Regel in drei Lesungen, wobei die fachliche Bearbeitung und politische Feinabstimmung der Vorlage im federführenden Ausschuss, der dem Plenum am Ende seiner Beratung eine Beschlussempfehlung vorlegt, stattfinden. Das Plenum entscheidet abschließend darüber, ob eine Vorlage endgültig abgelehnt, noch einmal geändert, ganz oder teilweise an die Ausschüsse zurückverwiesen oder beschlossen wird. Nach Beschluss eines Gesetzes durch den Bundestag wird dieses durch den Bundestagspräsidenten unverzüglich dem Bundesrat zugeleitet.

Im Bundesrat wird der Gesetzesbeschluss des Bundestags in den zuständigen Ausschüssen beraten (zweiter Durchgang). Am Ende der Beratung steht eine Empfehlung, dem Gesetzesbeschluss zuzustimmen bzw. nicht zuzustimmen oder den Vermittlungsausschuss anzurufen bzw. nicht anzurufen (Bundesministerium des Innern 2012, S. 89–106).

Ist ein Gesetz zustande gekommen, wird das federführende Ressort unterrichtet, das bei der Schriftleitung des Bundesgesetzblatts die Herstellung der Urschrift des Gesetzes veranlasst. Das federführende Ressort trägt dafür Sorge, dass die Urschrift von den zuständigen Mitgliedern der Bundesregierung gegengezeichnet wird. Nach Übersendung der Urschrift durch das Bundeskanzleramt an das Bundespräsidialamt prüft der Bundespräsident das verfassungskonforme Zustandekommen des Gesetzes und ob es sonstige, offenkundige Verstöße gegen Bestimmungen des Grundgesetzes gibt. Ergibt die Prüfung, dass das Gesetz verfassungskonform ist, unterzeichnet er die Urschrift und übermittelt diese zur Verkündung an die Schriftleitung des Bundesgesetzblatts. Zudem unterrichtet er die beteiligten Ressorts über die Ausfertigung des Gesetzes. Die Schriftleitung veranlasst die Verkündung des Gesetzeswortlauts im Bundesgesetzblatt. Sie unterrichtet das Bundeskanzleramt und das federführende Ressort darüber und übergibt die Urschrift zur Archivierung an das Bundesarchiv (Bundesministerium des Innern 2012, S. 107–108).

Trotz der hervorgehobenen Rolle der Gesetzgebung ist sie erst in den letzten Jahren Gegenstand von Digitalisierungsüberlegungen geworden. Aufgrund ihrer Verbindlichkeit und besseren Erfassbarkeit werden diejenigen Schritte des Gesetz-

gebungsverfahrens digital umgesetzt, die durch formales Handeln gekennzeichnet sind. Informale Prozesse sind hingegen nur sehr schwer zu erfassen und eignen sich daher nur bedingt für die Digitalisierung. Zudem würde eine Digitalisierung informaler Prozesse, die eine wichtige Ergänzung zu formalen Prozessen darstellen, zu einer in der Regel nicht beabsichtigten Formalisierung führen.

---

### 3 Praktische Anwendung

Die Grundidee der elektronischen Gesetzgebung ist es, das Verfahren vom Textentwurf bis zur Verkündung eines Gesetzes vollständig elektronisch abzubilden. Durch die Vermeidung von Medienbrüchen sowie die standardisierte Erfassung und Weitergabe von Informationen zu einem Gesetzesvorhaben ist es möglich, das Verfahren zu vereinfachen, den Arbeitsaufwand zu reduzieren und Fehler zu vermeiden. Bevor allerdings das Gesetzgebungsverfahren vollständig digitalisiert werden kann, bedarf es der Überwindung einiger Hindernisse. Neben (verfassungs-)rechtlichen Fragen sowie Fragen der IT-Sicherheit, die im Zusammenhang mit der verstärkten Nutzung von IT-Lösungen im staatlichen Bereich noch zu klären sind, ist auch die Akzeptanz dieser Angebote durch die Nutzerinnen und Nutzer ein wichtiger Aspekt. Aus diesem Grund ist sowohl die Einbeziehung der Nutzerinnen und Nutzer bei der Entwicklung solcher Lösungen als auch ihre umfassende Schulung im Umgang mit den neuen Instrumenten eine wichtige Voraussetzung für den Umsetzungserfolg. Zusätzlich besteht die Schwierigkeit darin, die Prozessabläufe und IT-Systeme in einem gemeinsamen System zusammenzuführen, ohne jedoch die Autonomie der beteiligten Institutionen einzuschränken. So betont beispielsweise der Bundestag unter Verweis auf das Verfassungsprinzip der Gewaltenteilung die Eigenständigkeit seiner informationstechnischen Systeme. Auf Ebene der Exekutive hat das Ressortprinzip, das die eigenverantwortliche Leitung eines Geschäftsbereichs durch die jeweilige Ministerin oder den jeweiligen Minister festlegt, in der Vergangenheit die Einführung gemeinsamer IT-Strukturen und -Standards innerhalb der Bundesregierung häufig erschwert (Bernhardt 2018, S. 18–19; Brosius-Gersdorf 2010).

Anwendungsmöglichkeiten für die elektronische Gesetzgebung ergeben sich in Deutschland auf Bundes- und Landesebene, da auf diesen beiden Ebenen Gesetze erarbeitet und verabschiedet werden. Grundsätzlich ist die Übertragung dieser Funktionalitäten auf das Verfahren zur Erstellung untergesetzlicher Regelungen ebenfalls möglich. Allerdings gibt es bislang noch kein durchgängig elektronisches Gesetzgebungsverfahren, sondern lediglich einzelne Softwarelösungen. Beispielsweise unterstützt das Planungs- und Kabinettmanagement-Programm (PKP) die ressortspezifische und -übergreifende Planung von Regelungsvorhaben sowie die Planung des Kabinetts- und Gesetzgebungsverfahrens. Das *Microsoft Word Add-In eNorm* bietet Dokumentvorlagen für verschiedene Arten von Regelungsvorhaben sowie eine Qualitätsprüfung, die anhand festgelegter Kriterien Fehler kennzeichnet. Insgesamt ist die IT-Unterstützung des Gesetzgebungsprozesses innerhalb der verschiedenen Verfassungsorgane noch unzureichend.

Die Wichtigkeit und Notwendigkeit der Bereitstellung einer verfassungsorganübergreifenden elektronischen Anwendung wurde durch den Abschluss einer Verwaltungsvereinbarung zur Umsetzung des Projekts „eGesetzgebung“ unterstrichen, die von Bundesregierung, Bundesrat, Bundestag, Bundespräsidialamt sowie der Geschäftsstelle des Vermittlungsausschusses und dem Nationalen Normenkontrollrat am 4. September 2017 unterzeichnet wurde. In dieser Vereinbarung definieren die Beteiligten die Projektorganisation und das Ziel eines interoperablen und modularen Systems für die Gesetzgebung. Dabei sollen organinterne Abstimmungsprozesse geschützt und Schnittstellen zu Bestandssystemen hergestellt werden. Bislang wurden im Rahmen des Projekts mehrere prototypische Anwendungen und Demonstratoren entwickelt, wie zum Beispiel die elektronische Nachhaltigkeitsprüfung (eNAP), die eine digitale Unterstützung bei der Beschreibung der Auswirkungen auf eine nachhaltige Entwicklung anbietet. In einem nächsten Schritt sollen weitere Unterstützungsangebote auf einer gemeinsamen Arbeitsplattform bereitgestellt werden. Dieser Umsetzungsstand macht deutlich, dass die Entwicklung eines vollständig elektronischen Gesetzgebungsverfahrens in Deutschland noch am Anfang steht. Grundsätzlich sind jedoch verschiedene Anwendungsmöglichkeiten denkbar, die die Nutzerinnen und Nutzer an verschiedenen Stellen im Gesetzgebungsprozess bei ihrer Arbeit unterstützen.

Im Gesetzgebungsverfahren können Funktionen zur Zeit- und Vorhabenplanung sowie zur Vorbereitung und Durchführung von Sitzungen und Abstimmungen einen reibungsloseren Ablauf gewährleisten und die Planungsprozesse verbessern. In den Sitzungen selbst könnten Nutzerinnen und Nutzer über eine elektronische Sitzungsplanung und -durchführung (z. B. Kabinett, Parlament, Ausschüsse) Tagesordnungen sowie Informationen und Dokumente zu den einzelnen Tagesordnungspunkten einsehen und versenden. Alle im System vorhandenen Dokumente und Prozessinformationen zu den zu behandelnden Regelungsvorhaben könnten angezeigt werden und die Stimmabgabe könnte direkt im System erfolgen. Für die Bundesregierung bietet das Planungs- und Kabinettsmanagement-Programm (PKP) einen Teil dieser Funktionalitäten an. Es ermöglicht unter anderem die (zeitliche) Planung eines Vorhabens im federführenden Ressort bzw. die übergreifende Koordinierung und die Kabinettszeitplanung durch das Bundeskanzleramt sowie den Versand von Dokumenten.

Die Arbeit am Text eines Gesetzesvorhabens kann ebenfalls durch den Einsatz moderner Informationstechnologien erleichtert werden. So könnte den Nutzerinnen und Nutzern frühzeitig eine Vorlage zur Verfügung gestellt werden, welche den formalen Gestaltungsanforderungen entspricht und damit die Erstellung eines Gesetzentwurfs nach den Vorgaben der GGO schnell und einfach ermöglicht. Auf Bundesebene wird hierfür in der Regel „eNorm“ genutzt, das vom Bundesministerium der Justiz und für Verbraucherschutz zur Verfügung gestellt und schrittweise weiterentwickelt wird. Darauf hinaus bieten sich innerhalb der elektronischen Gesetzgebung neue Möglichkeiten der kollaborativen Textarbeit. Insbesondere durch Änderungs- und Kommentarfunktionen könnten Gesetzentwürfe zeitgleich bearbeitet und zu unterschiedlichen Zeitpunkten mit unterschiedlichen Kreisen (ressortintern, ressortübergreifend etc.) abgestimmt werden. Daneben kann die IT-

Unterstützung das Vergleichen und Zusammenführen von Änderungsversionen erleichtern, indem automatisiert Synopsen erstellt werden. Zudem könnte eine automatisierte Texterkennung dabei helfen, die Gesetzessprache durch die automatische Überprüfung redaktioneller Aspekte (z. B. Abkürzungen und Zitierweise) und die Anzeige von Verbesserungsvorschlägen zu vereinheitlichen. Darüber hinaus wäre es denkbar, aus Fassungsvergleichen automatisiert Änderungsbefehle zu Änderungsgesetzen zu generieren, sodass die Textarbeit hauptsächlich am avisierten Regelungstext erfolgen kann. Hier könnten sowohl Arbeitsaufwand eingespart als auch redaktionelle Fehler minimiert werden. Im Bereich der automatischen Texterkennung wäre es denkbar, dass referenzierte Rechtsvorschriften erkannt und eingeblendet werden sowie bereits bei der Texterstellung selbstständig auf vorhandene Definitionen eines Begriffs in anderen Regelungen hingewiesen wird. Die Vermeidung von parallel existierenden Definitionen ein und desselben Begriffs würde die Verständlichkeit und Konsistenz des Rechts erheblich verbessern. Für diese Funktion ist jedoch ein amtlicher elektronischer Normenbestand notwendig, den es bisher im Bund noch nicht gibt.

Eine elektronische Anwendung kann die Nutzerinnen und Nutzer auch bei der Durchführung von in der GGO festgelegten Schritten im Gesetzgebungsprozess unterstützen. So sieht § 44 GGO vor, dass für Gesetzentwürfe der Bundesregierung eine Gesetzesfolgenabschätzung durchgeführt werden soll. Eine elektronische Gesetzgebung kann hierfür digitale *Tools* bereitstellen, mit denen die Gesetzesfolgen in den jeweiligen Bereichen (z. B. Erfüllungsaufwand, Auswirkungen auf die öffentlichen Haushalte) erfasst werden können. Die Unterstützung könnte die Bereitstellung von Informationen (z. B. über die Anbindung von Datenbanken), strukturierten Prüfschemata und Berechnungshilfen sowie die Aufbereitung von Inhalten umfassen. Durch die übersichtliche Aufbereitung der zahlreich vorhandenen Materialien bliebe mehr Zeit für die inhaltlichen Überlegungen und somit könnte letztlich auch die Qualität der Gesetzesfolgenabschätzung gesteigert werden. Eine bessere Verfügbarkeit von Informationen könnte darüber hinaus evidenzbasierte Entscheidungen fördern und somit zur Erarbeitung besserer Regelungsentwürfe führen. Ein erster Schritt in diese Richtung wurde mit der Umsetzung von eNAP als erste funktionsfähige digitale Anwendung unternommen.

In Österreich existiert dagegen bereits ein vollumfängliches „elektronisches Werkzeug zur wirkungsorientierten Folgenabschätzung“ (WFA IT-Tool), dessen Ergebnisdokument Gesetzentwürfen verpflichtend beizulegen ist. Die für ein Regelungsvorhaben zuständigen Rechtsetzungsreferentinnen und -referenten können die Auswirkungen von Regelungsvorhaben in verschiedenen Wirkdimensionen anhand von Fragen und Berechnungen identifizieren und beschreiben. Dabei werden sie durch eine gezielte Nutzerführung, umfangreiche Hilfetexte und regelmäßig aktualisierte Kennzahlen für Berechnungen unterstützt.

Auch die Verbändeanhörung und die Abgabe von Stellungnahmen (z. B. des Bundesrats oder des NKR) können elektronisch erfolgen. Hierfür sind verschiedene Stufen der technischen Unterstützung bzw. der Standardisierung von Stellungnahmen möglich. Über die medienbruchfreie Entgegennahme von Stellungnahmen hinaus könnte die Weiterverarbeitung durch die Ministerialverwaltung durch eine

*Online*-Plattform vereinfacht werden, auf der die Texte und Angaben zur Person bzw. Organisation über eine Maske erfasst werden. Dies könnte auch in Form eines Fragebogens geschehen, bei dem ein Ministerium gezielt Fragen zum geplanten Regelungsvorhaben stellt, die dann *online* beantwortet werden können. Diesen Weg beschreitet beispielsweise die EU-Kommission mit ihren *Online*-Konsultationen. Über eine zentrale Webseite können neben Interessengruppen, Verbänden und Nichtregierungsorganisationen auch Bürgerinnen und Bürger ihre Bewertung neuer EU-Initiativen und bestehender Rechtsvorschriften abgeben. Für die Konsultationen werden *Online*-Fragebögen mit standardisierten Fragen und Texteingabefeldern genutzt. Zudem können Stellungnahmen als Anlage hochgeladen werden. Denkbar ist auch eine größere Orientierung an der Struktur des Entwurfs für den Gesetzestext: So könnten Verbände oder Institutionen wie der NKR ihre Anmerkungen auch direkt einzelnen Textpassagen zuordnen. Eine in dieser Weise strukturierte Erfassung von Stellungnahmen würde die anschließende Weiterverarbeitung und Auswertung durch die Ministerialverwaltung erleichtern.

Schließlich sieht eine vollständig elektronische Gesetzgebung auch die elektronische Verkündung von Gesetzen vor, die einen einfachen und unmittelbaren Zugang zu Verkündigungsblättern und zur amtlich verbindlichen Version der Gesetze ermöglicht. Eine elektronische Verkündung ist zudem Voraussetzung für die Schaffung eines amtlich verbindlichen elektronischen Normbestands. Durch eine Integration des elektronischen Normbestands in die elektronische Gesetzgebung stünden den Nutzerinnen und Nutzern immer alle erforderlichen Rechtsgrundlagen durchsuch- und sortierbar zur Verfügung. Bisher sind Gesetze im Internet lediglich in nicht-amtlicher Fassung abrufbar. Neben den technischen Voraussetzungen sind auch rechtliche Anforderungen im Zusammenhang mit der elektronischen Verkündung zu beachten. Erstens muss ein dauerhafter Zugriff auf die Gesetze im Internet gewährleistet sein. Zweitens müssen die Bürgerinnen und Bürger, die über keinen Internetzugang verfügen, Einblick in die Gesetze nehmen können. Drittens muss garantiert werden, dass die Verkündung nur durch die dazu legitimierte Person erfolgen kann und Änderungen am Gesetzestext nur durch den erforderlichen Hoheitsakt vollzogen werden können. Eine elektronische Verkündung erfordert nach derzeitigem Stand eine Änderung des Grundgesetzes. Brandenburg, das Saarland und Bremen haben inzwischen ihre Landesverfassungen entsprechend geändert und verkünden ihre Gesetze ausschließlich auf elektronischem Wege. Auf europäischer Ebene hat neben der EU u. a. Österreich eine ausschließlich elektronische Verkündung von Gesetzen und Rechtsverordnungen eingeführt. Beide haben einzelne Elemente einer elektronischen Gesetzgebung implementiert, verfügen bislang jedoch über kein integriertes elektronisches System für den gesamten Gesetzgebungsprozess.

Um die zuvor genannten Funktionalitäten vollumfänglich nutzen zu können, ist ein umfassendes Rollen- und Berechtigungskonzept erforderlich. Durch diese Authentifizierungspflicht würde sichergestellt, dass einerseits alle Nutzerinnen und Nutzer der elektronischen Gesetzgebung die Aufgaben wahrnehmen können, die ihnen zugeordnet worden sind, und andererseits Informationen erst dann anderen Personen zur Verfügung stünden, wenn diese vorher freigegeben wurden. Dies ist vor allem deshalb wichtig, damit es nicht zu einer Missachtung der von der Verfassung garantierten Grundsätze (z. B. Ressortprinzip, Gewaltenteilung) kommt.

Ein Beispiel für ein umfangreiches elektronisches Gesetzgebungsverfahren mit vielen der hier geschilderten Funktionen bietet Estland, das weltweit einen Vorreiterstatus im Bereich *E-Government* einnimmt. Die Abstimmung von Gesetzentwürfen zwischen den Ministerien und im Parlament wird vollständig elektronisch im „e-Consultation System“ abgewickelt, das die verschiedenen Institutionen in einem Netzwerk verbindet und über das Internet auch die Beteiligung der Öffentlichkeit ermöglicht. Das System ist verbunden mit einer web-basierten *Software*, die zur Vorbereitung und Durchführung der Kabinettsitzungen genutzt wird. Berechtigte Nutzerinnen und Nutzer können auf das System mit Hilfe ihres elektronischen Ausweises oder ihrer mobilen ID zugreifen. Über das Informationssystem haben die Ministerinnen und Minister Zugang zu allen Beratungsgegenständen und Tagesordnungen der Kabinettsitzungen und können Kommentare hinterlassen sowie vorläufig über Beratungsgegenstände abstimmen. Alle Gesetzentwürfe werden in der Online-Datenbank „e-Law“ veröffentlicht und nach ihrer Verabschiedung *online* im Gesetzblatt verkündet. Eine einfache Übernahme des estnischen Ansatzes ist wegen der sehr unterschiedlichen Rahmenbedingungen jedoch nur schwer denkbar. Während es sich bei Estland um einen relativ kleinen Zentralstaat mit einer Bevölkerung von rund einer Million Einwohnern handelt, steht Deutschland als Föderalstaat mit rund 80 Millionen Einwohnerinnen und Einwohnern vor ganz anderen Herausforderungen (Bernhardt 2018, S. 4).

---

## 4 Künftige Entwicklung

Die elektronische Gesetzgebung befindet sich in Deutschland in einer frühen Entwicklungsphase. Erste Umsetzungsschritte sind erfolgt. Es ist jedoch zu früh, um Auswirkungen auf das Gesetzgebungsverfahren feststellen zu können. Der Abbau von Medienbrüchen und die IT-gestützten Arbeitsprozesse können allerdings zu einer Zeitersparnis und zu Arbeitserleichterungen und dadurch zu mehr Zeit für die inhaltliche Arbeit führen. Hierfür sind die rechtlichen Voraussetzungen im Bund weitgehend geschaffen. Lediglich für die elektronische Verkündung von Gesetzen ist eine Grundgesetzänderung erforderlich. Hingegen ist nicht damit zu rechnen, dass sich die informalen Prozesse, die mit dem Gesetzgebungsverfahren einhergehen, durch die elektronische Gesetzgebung grundlegend ändern werden. Die Aushandlungs- und Abstimmungsprozesse jenseits formalisierter Verfahrensvorgaben werden auch weiterhin möglich sein.

Die elektronische Gesetzgebung bietet aber auch Weiterentwicklungsmöglichkeiten. Zu nennen ist hier z. B. eine elektronische Beteiligung von Bürgerinnen und Bürgern am Gesetzgebungsverfahren, die zeit- und ortsunabhängig sowie mit einem geringen Aufwand verbunden wäre. Die Einführung einer E-Partizipation würde sich auf den Ablauf des Gesetzgebungsverfahrens und das Zusammenspiel der an ihm beteiligten Akteure auswirken und kann zu einer höheren Akzeptanz von Gesetzen bei den Bürgerinnen und Bürgern beitragen. Allerdings fehlen auf Bundesebene hierfür die rechtlichen Voraussetzungen. Auch wenn Informations- und Kommunikationstechnologien hier neue Möglichkeiten bieten, bleibt es eine politische Entscheidung, wie diese genutzt werden.

Ein Bereich, in dem technologische Innovationen der Gesetzgebungsarbeit langfristig neue Impulse geben können, ist die Gesetzesvorbereitung, die hauptsächlich in der Ministerialverwaltung erfolgt. Bisher stehen hier die Arbeit am Gesetzestext und weniger die mit einem Regelungsvorhaben verbundenen Prozesse im Mittelpunkt. Beispielsweise werden oft Dokumente zu abgeschlossenen Regelungsvorhaben überarbeitet oder es werden Formatvorlagen verwendet. Dieses Vorgehen erschwert, dass Problemlösungen offen und zunächst unabhängig von bestehenden Regelungstexten gedacht werden, und schränkt damit die Handlungsspielräume bereits im Vorfeld ein. Moderne IT-Lösungen können eine offenere, prozessorientierte Herangehensweise unterstützen, die sich von der individuellen Textarbeit löst und stärker auf die Erstellung von Regelungsentwürfen in interdisziplinären Teams setzt.

Von zentraler Bedeutung für eine prozessorientierte Herangehensweise ist die Verknüpfung von Gesetzestext und Prozessdarstellung. Um die dafür erforderliche Verbindung zwischen Text und seiner inhaltlichen Bedeutung automatisiert herstellen zu können, ist eine Systematik erforderlich, durch die Begriffen oder Textpassagen inhaltliche Bedeutungen zugeordnet werden können. Beispielsweise könnte der Formulierung „auf Antrag“ das Prozesselement „Antragstellung“ zugeordnet werden, das weitere Informationen zum typischen Ablauf einer Antragstellung enthalten könnte (Off et al. 2016, S. 39). Mithilfe einer Datenbank von Standardprozessen könnte dann ein erster Entwurf einer Prozessdarstellung aus einem Regelungstext erzeugt werden. Könnten Änderungen in beide Richtungen – sowohl vom Text zur Prozessdarstellung als auch von der Prozessdarstellung zum Text – vollzogen werden, könnte dies die Nutzung eines prozessorientierten Ansatzes in der Gesetzgebungsarbeit wesentlich erleichtern und einen besseren Überblick über die konkreten Konsequenzen einzelner Regelungsbestandteile verschaffen. Die Änderung eines geplanten Prozesses würde sich dann automatisch im Gesetzestext niederschlagen und umgekehrt. Darüber hinaus könnten durch einen Abgleich der Prozesse weitergehende Beziehungen zwischen einem aktuellen Regelungsentwurf und bereits vorhandenen Regelungen aufgezeigt werden. Damit ließen sich Vereinfachungspotenziale in einer geplanten Regelung identifizieren.

Der Aufbau eines umfassenden Wissensmanagementsystems und dessen intelligente Vernetzung mit einer elektronischen Gesetzgebung stellen eine weitere Entwicklungsmöglichkeit dar, die sich jedoch voraussichtlich erst mittel- oder langfristig realisieren lässt. Dadurch könnten an unterschiedlichen Stellen vorhandene Daten- und Wissensbestände gebündelt und für die Erarbeitung eines Regelungsvorhabens genutzt werden. Hierbei könnten integrierte Datenbanken (sog. *Data-Warehouses*), Dokumentenmanagementsysteme, digitale Bibliotheken oder *Wikis* zum Einsatz kommen. Die zusätzliche Sicherung von Wissen in einem Wissensmanagementsystem – unabhängig von einzelnen Wissensträgern – gewährleistet die dauerhafte Bereitstellung von Informationen, die zur Lösung von Aufgaben benötigt werden, auch wenn die dafür zuständigen Personen wechseln. In einem solchen System kann vorhandenes Wissen ständig mit neuen Informationen angereichert und neu strukturiert werden. Dies ermöglicht einen umfassenden und schnellen Zugang zu Wissen, das beispielsweise für die Erarbeitung eines Regelungsentwurfs (z. B. für

die Durchführung der Gesetzesfolgenabschätzung) relevant ist und würde über die verbesserte Sammlung und Weitergabe von Informationen die Arbeit im Gesetzgebungsprozess erleichtern.

Erste Erfahrungen mit einem IT-gestützten prozessorientierten Ansatz, verknüpft mit Wissensmanagement-Elementen, konnten bereits bei der Erarbeitung eines Gesetzentwurfs für die Strukturreform des Versorgungsausgleichs im Bundesministerium der Justiz und für Verbraucherschutz gesammelt werden. In dem Pilotprojekt stellten die Nutzerinnen und Nutzer die Regelungsinhalte prozesshaft dar und ordneten diesen dann gezielt Informationen zu. Erst am Ende dieses Prozesses erfolgte die Formulierung neuer Normen und die Ausarbeitung eines Gesetzentwurfs. Die Visualisierung ermöglichte ein besseres Verständnis der komplexen Regelungsmaterie und eine leichtere Identifizierung von Optimierungspotenzialen (Breidenbach und Schmid 2018).

Die Verknüpfung einer prozessorientierten Arbeitsweise mit Wissensmanagementansätzen könnte – unterstützt durch die zunehmende Verbreitung von IT-gestützten Visualisierungstools – in Zukunft häufiger zur Anwendung kommen. Dies würde die Erarbeitung von Regelungsentwürfen nachhaltig verändern und die Einbeziehung verschiedener fachlicher Spezialistinnen und Spezialisten erleichtern.

---

## Literatur

- Bernhardt, Wilfried. 2018. Digitalisierung im Spannungsfeld der grundgesetzlichen Kompetenzträger. In *Digitalisierung im Spannungsfeld von Politik, Wirtschaft, Wissenschaft und Recht*, Hrsg. Christian Bär, Thomas Grädler und Robert Mayr, 1–24. Berlin: Springer Gabler.
- Bohne, Eberhard. 2018. *Verwaltungswissenschaft. Eine interdisziplinäre Einführung in die Grundlagen*. Wiesbaden: Springer VS.
- Breidenbach, Stephan, und Matthias Schmid. 2018. Gesetzgebung und Digitalisierung – Digitale Instrumente der Erarbeitung von Gesetzentwürfen. In *Rechtshandbuch Legal Tech*, Hrsg. Stephan Breidenbach und Florian Glatz, 169–188. München: C.H. Beck.
- Brosius-Gersdorf, Frauke. 2010. Verfassungsrechtliches Ressortprinzip als Hindernis staatlicher Innovationen? In *Innovationen im und durch Recht*, Hrsg. Hermann Hill und Utz Schliesky, 23–55. Baden-Baden: Nomos.
- Bundeskanzleramt. 2018. Arbeitsprogramm Bessere Rechtsetzung und Bürokratieabbau 2018. Kabinettbeschluss vom 12. Dezember 2018. <https://www.bundesregierung.de/resource/blob/997532/1560386/a5004f6046edb6a8ce916b411c8c3e43/2018-12-12-arbeitsprogramm-bessere-rechtsetzung-data.pdf?download=1>. Zugegriffen am 05.11.2019.
- Bundesministerium des Innern. 2012. *Handbuch zur Vorbereitung von Rechts- und Verwaltungsvorschriften*. Köln: Bundesanzeiger.
- Bundesministerium des Innern. 2014. Digitale Verwaltung 2020 – Regierungsprogramm 18. Legislaturperiode. <https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/moderne-verwaltung/regierungsprogramm-digitale-verwaltung-2020.html>. Zugegriffen am 05.11.2019.
- Fliedner, Ortlieb. 2013. *Rechtsetzung in Deutschland*. Baden-Baden: Nomos.
- Ismayr, Wolfgang, Hrsg. 2008. Gesetzgebung im politischen System Deutschlands. In *Gesetzgebung in Westeuropa*, 383–429. Wiesbaden: Springer VS.
- Off, Thomas, Hannes Kühn, und Tino Schuppan. 2016. Semantikbasierte und prozessorientierte E-Gesetzgebung zur Vollzugsoptimierung. In *Digitale Transformation. Methoden, Kompetenzen und Technologien für die Verwaltung*, Hrsg. Detlef Rätz, Michael Breidung, Dagmar Lück-Schneider, Siegfried Kaiser und Erich Schweighofer, 35–50. Bonn: Kölken.



---

# Soziale Medien (Social Media)

Mathias König und Wolfgang König

## Inhalt

1 Klärung des Begriffs .....	326
2 Theoretische Grundlagen .....	326
3 Praktische Anwendungsfelder .....	330
4 Umsetzungsstand und Auswirkungen .....	332
5 Perspektiven für Staat und Verwaltung .....	335
Literatur .....	336

---

## Zusammenfassung

Weltweit hat die Nutzung von *Social Media* im Zeitverlauf grundsätzlich an Bedeutung gewonnen. In Deutschland ist sie im Vergleich zum Jahr 2013 um 13 Prozentpunkte auf 31 Prozent im Jahr 2018 gestiegen (Newman et al. 2018). Staat und Verwaltung sind folglich zunehmend mit der öffentlichen Erwartungshaltung konfrontiert, via *Social Media* (insb. *Facebook* und *Twitter*) eine bessere Kommunikation (schneller, transparenter, responsiver, unbürokratischer) mit Bürgern zu realisieren. Bei genauer Betrachtung zeigt sich allerdings, dass die erhoffte kommunikative Bürgernähe weitgehend ausbleibt. Professionelle Kommunikation wird primär in jenen Bereichen forciert, in denen Staat und Verwaltung auf Bürger als Ressource zurückgreifen möchten (z. B. Mithilfe bei Onlinefahndung, Personalrekrutierung, Legitimationsbeschaffung).

---

## Schlüsselwörter

Social Media · Twitter · Online-Partizipation · Regierungskommunikation · Bürgerbeteiligung

---

M. König (✉) · W. König

Institut für Kommunikationspsychologie und Medienpädagogik & Institut für Sozialwissenschaften, Universität Koblenz-Landau, Landau in der Pfalz, Deutschland  
E-Mail: [mathias.koenig@gmail.com](mailto:mathias.koenig@gmail.com); [wolfgang.koenig@gmail.com](mailto:wolfgang.koenig@gmail.com)

## 1 Klärung des Begriffs

In der Forschung gibt es keinen Konsens bezüglich einer allgemeingültigen Definition von *Social Media*. Grundsätzlich ist der Begriff *Social Media* eng mit den Möglichkeiten des Internets verbunden, seine Meinung und Ansichten mit anderen zu teilen und dadurch quasi selbst zum Medium werden. Bezogen auf das massenöffentliche Verbreiten von Botschaften ermöglichte das Internet 1.0 in der Regel nur eine *One-Way-Kommunikation*, weil das Betreiben einer *Homepage* oder eines *Blogs* technisches Wissen und ggf. finanzielle Ressourcen erforderte. Um die Jahrtausendwende emanzipierte sich das Internet hin zum sogenannten Web 2.0. Nunmehr kann jeder Nutzer ohne finanzielle Ressourcen und ohne größeres technisches Verständnis zum Sender öffentlicher Botschaften werden, indem er *Social Media-Dienste* nutzt. Das Attribut „sozial“ bezieht sich auf das Potenzial des interpersonalen Austauschs, der zumeist in *Online-Communities* (z. B. *Facebook*) mehr oder weniger öffentlich stattfindet. Für die soziale Teilhabe an öffentlichen Debatten bietet sich zudem unangefochten der *Micro-Blogging-Dienst Twitter* an, da hier primär Akteure des politisch-medialen Systems oder Prominente (z. B. Sportler und Schauspieler) erreicht werden können. Die technische Infrastruktur, die durch die *Social Media-Dienste* bereitgestellt wird, impliziert letztlich gleichberechtigte Kommunikationschancen – unabhängig von Rolle, Amt oder sonstigem Status. Kurz: Eine Bürgernähe auf Augenhöhe.

Teilweise wird in der Literatur *Social Media* aber auch als *Catch-All-Term* verwendet. Beispielsweise werden hierdurch klassische Beteiligungsformate wie z. B. Bürgerhaushalte oder auch *E-Government* als „neu“ etikettiert. Diese gehören aber nicht zum Kern von *Social Media*, weil sie völlig unabhängig im Internet betrieben werden können. Diskussionen über einen konkreten Bürgerhaushalt können hingegen – wie jeder andere öffentliche Diskurs – aber durchaus in sozialen Medien geführt werden.

---

## 2 Theoretische Grundlagen

Wie bereits skizziert, ist der Begriff *Social Media* empirisch eine Sammelbeschreibung verschiedener Internet-Kommunikations-Dienste. Dass hierdurch die soziale interpersonale Kommunikation teilweise verändert und intensiviert wird, zeigt beispielsweise eine Studie zur Bundestagswahl 2017 (vgl. König und König 2018). Die theoretische Debatte zum Wandel der Kommunikation zwischen Staat, Verwaltung und Bürger lässt sich analytisch in zwei unterschiedliche Stränge differenzieren, die aber meist miteinander vermischt werden: einen kommunikations-konzeptionellen und einen gesellschaftlich-normativen. Der Anspruch des kommunikations-konzeptionellen Strangs ist es, die neue Vielfalt der Möglichkeiten anhand verschiedener Kommunikationsdimensionen analytisch zu erfassen, während der gesellschaftlich-normative Strang versucht, die soziale Richtung der Veränderung zu untersuchen.

Die Essenz des konzeptionellen Strangs lässt sich in Anlehnung an Lindsay Hoffman (2012) anhand von drei Dimensionen der Kommunikationsinteraktion synthetisieren:

1. Eindimensionale Kommunikation: Klassische *One-Way*-Kommunikation (z. B. *Homepage*)
2. Zweidimensionale Kommunikation: Wechselseitige (*Two-Way*-)Kommunikation (z. B. *E-Mail* oder *Messenger*)
3. Dreidimensionale Kommunikation: *Soziale Medien*, die ein- und zweidimensionale Kommunikation ermöglichen sowie ergänzende Vernetzungsmöglichkeiten, die auf der Basis von Nutzer-Profilseiten (z. B. *Online-Community*, *Micro-Blogging*) möglich sind.

Werden exemplarisch *Social Media*-Dienste anhand der möglichen Kommunikationsinteraktion und Nutzungsweise betrachtet, dann unterscheiden sich *Messenger*, *Online Communities* oder *Blogs* bzw. *Micro-Blogs* voneinander.

1. *Messenger* wie *WhatsApp* werden überwiegend zur zweidimensionalen und nicht-öffentlichen Kommunikation genutzt, wobei auch in Gruppenchats diskutiert werden kann. Zur öffentlichen Diskussion sind sie nicht geeignet.
2. *Online-Communities* wie *Facebook* ermöglichen das Betreiben einer eigenen öffentlichen oder auch privaten Profil-Seite, die umfangreich gestaltet werden kann. Neben dieser klassisch eindimensionalen Kommunikation liegt das Kommunikationsziel aber in der dreidimensionalen Kommunikation. Beiträge anderer Nutzer können verbreitet (*share*n) oder bewertet (*like*n) werden. Für Institutionen gibt es die Möglichkeit so genannte *Fan-Pages* anzulegen. Hier können diverse Informationen bereitgestellt werden. Nutzer können gleichzeitig Fan einer solchen Seite werden und erhalten dann automatisch die Nachrichtenupdates oder Veranstaltungshinweise. Für die massenhafte Verbreitung von Nachrichten sind *Online-Communities* oft nicht geeignet, da Nachrichten nutzerspezifisch gefiltert werden (Stichwort *Filterbubble* bzw. *Echokammer*) oder nur in der jeweiligen *Online-Community* öffentlich sichtbar sind (abhängig ist dies auch von den Privatsphäre-Einstellungen der Nutzer).
3. *Blogs* (z. B. [blogger.com](#)) ermöglichen in jedem Fall eine eindimensionale Kommunikation. Die Kommunikation kann theoretisch auch mehrdimensional erfolgen, falls die Kommentarfunktion freigeschaltet wird. In der Regel müssen sich Kommentatoren von Blogbeiträgen aber anmelden. Dies erschwert die mehrdimensionale Kommunikation strukturell.
4. Beim *Micro-Blogging* handelt es sich ursprünglich um ein Phänomen, das auf Kurzbeiträgen (280 Zeichen z. B. bei *Twitter*) basiert. Nutzer sind angehalten kurze Texte zu aktuellen Entwicklungen zu schreiben, ähnlich wie in einem Nachrichten-Ticker. Der Arbeitsaufwand für eine Kurzbotschaft ist sehr gering und folglich ist die Beteiligung und Nutzerinteraktion höher als bei normalen *Blogs*. Eine öffentliche transparente dreidimensionale Kommunikation ist strukturell nur für angemeldete Nutzer gegeben. Beim *Micro-Blogging* ist weltweit *Twitter* (bis auf China) der zentrale Dienst geworden. Nutzer können kurze Botschaften (*Tweets*) über die eigene Profilseite in Echtzeit in der Regel massen-

öffentlich publizieren (Mittlerweile können auch Videos und Bilder direkt publiziert werden). Letztlich wird jeder Nutzer zu seinem eigenen Nachrichtendienst. *Twitter*-Seiten oder *Tweets* sind problemlos ohne Anmeldung nutzbar und ermöglicht dadurch immer auch eine eindimensionale Kommunikation. Eine Kooperation mit dem Suchmaschinenbetreiber *Google* sorgt dafür, dass relevante Botschaften direkt in den Ergebnissen einer *Google*-Suche platziert werden. Außerdem sind zahlreiche Politiker, Medien und Journalisten bei *Twitter* aktiv. Dadurch ist *Twitter* für die schnelle massenmedial verwertbare Informationsverbreitung der präferierte *Social Media*-Kanal. Gleichzeitig können die klassischen Gatekeeper (Journalisten) bei der Nachrichtenverbreitung umgangen werden. Besonders in Wahlkampfzeiten wird *Twitter* von Politikern (z. B. Donald Trump), Journalisten aber auch von Wählern genutzt, um öffentlich sichtbar für alle zu diskutieren. Ein *Tweet*-Aufkommen von mehreren tausend *Tweets* binnen weniger Stunden bei Wahlen ist dabei keine Seltenheit. Neuere Dienste wie z. B. *Instagram* oder *Snapchat* spielen bei der politischen Informationsnutzung in Deutschland noch keine entscheidende Rolle (Newman et al. 2018).

Die Grenzen der Trennung der *Social Media*-Angebote nach *Messenger*, *Online-Community*, oder (*Micro-)**Blogging* wird allerdings immer fließender, weil die Betreiber der Anwendungen versuchen, immer mehr Nutzer anzusprechen und entsprechend die Anwendungen in ihren Möglichkeiten erweitern. Trotzdem weisen *Social Media*-Dienste einen entsprechend *Bias* bei der Kommunikationsdimension und der öffentlichen Sichtbarkeit auf. Nachfolgende Tabelle gibt einen ausgewählten Überblick (Tab. 1).

Bei der gesellschaftlich-normativen Betrachtung geht es darum, die soziale Richtung der Kommunikationsentwicklung theoretisch zu beleuchten und auf dieser Basis Vergleiche zu ziehen bzw. *Benchmarks* aufzustellen. Bei klassischen Medien wird hier zwischen Unterhaltungswert und informativ-gesellschaftlichem Nutzwert differenziert, wobei im Kontext des demokratischen Staates der informativ-gesellschaftliche Nutzwert von zentraler Bedeutung ist.

Bei sozialen Medien werden als Ausgangsbasis die Demokratisierungsprozesse in Tunesien als Ideal herangezogen, da durch die sozialen Medien (insb. *Facebook* und *Twitter*) die dortigen Systemmedien umgangen werden konnten (vgl. König und König 2016). Soziale Medien waren letztlich der zentrale alternative Publikationskanal der demokratischen Öffentlichkeit bzw. Opposition in Tunesien. Obwohl bzw. weil die sozialen Medien gegen den autoritären Staat und seine Verwaltung gerichtet waren und gerade nicht auf eine bessere Kommunikation mit ihm zielten, haben soziale Medien ihren Weg in die theoretischen Debatten gefunden, die „gute“ Kommunikation als wesentlichen Garant der funktionierenden westlichen Demokratie sehen. Diese Debatte wird von einer cyberutopischen *Impact*-Hypothese geprägt, die insbesondere durch die Grundwerte der Transparenz, Rechenschaftspflicht und Responsivität des Verwaltungshandelns repräsentiert wird und mehr oder weniger implizit in die Konzeption eines herrschaftsfreien Diskurses in Annäherung an Jürgen Habermas münden. Hierbei wird die Hoffnung geweckt, via *Social Media* gerade öffentliche Diskurse und damit die demokratische Öffentlichkeit zu revitali-

**Tab. 1** Social Media-Diensten im Überblick

Social Media-Dienst	Primärfunktion	Primäre Kommunikationsdimension	Primäre Publizitätsdimension
Blogger.com	Blogging	Eindimensional	Massenöffentlich
Facebook	Online-Community	Dreidimensional	Community-Öffentlich
Facebook-Messenger	Messenger	Zweidimensional	Beteiligte Nutzer
Flickr	Foto-Blogging	Dreidimensional	Massenöffentlich
Instagram	Foto- und Video-Blogging	Dreidimensional	Massenöffentlich
Pinterest	Foto-Blogging	Eindimensional	Community-Öffentlich
Sina Weibo (nur China)	Micro-Blogging	Dreidimensional	Massenöffentlich (ggf. durch chinesische Regierung censiert)
Snapchat	Foto-Video-Blogging	Eindimensional	Community-Öffentlich
Telegram	Messenger	Zweidimensional	Beteiligte Nutzer
Twitter	Micro-Blogging	Dreidimensional	Massenöffentlich
Vimeo	Video-Blogging	Dreidimensional	Massenöffentlich
Whatsapp	Messenger	Zweidimensional	Beteiligte Nutzer
Youtube	Video-Blogging	Dreidimensional	Massenöffentlich

Quelle: Eigene Zusammenstellung

sieren, weil es sehr leicht geworden ist, seine Meinung zu äußern und sich an öffentlichen Diskussionen zu beteiligen. Die Vermachtung der öffentlichen Meinung, durch die *Gatekeeper*-Funktion der Staatsmedien, lasse sich hierdurch nämlich überwinden, wie das Beispiel Tunesien beeindruckend zeige. Die Kommunikation zwischen Bürgern und Verwaltung im demokratischen Staat könnte – so die demokratietheoretische Hypothese – entsprechend der erwähnten Grundwerte verbessert werden.

Insbesondere verweist der Wert der Responsivität auf die Chance einer bürgernahen Verwaltungskommunikation. Die zunehmende Beliebtheit von *Social Media* in der Gesellschaft setzte die Verwaltungskommunikation unter Modernisierungsdruck – so die normative Hypothese. Damit würden nahezu alle Erwartungen einer modernen Verwaltung erfüllt, bei der Bürger nicht als Untertanen, sondern als mündige Bürger verstanden werden: Interessierte Bürger könnten nämlich durch *Social Media* schneller, transparenter, komfortabler, vielfältiger und verständlicher mit der Verwaltung kommunizieren. Gleicher gilt für die staatsinterne Kommunikation der Verwaltungsmitarbeiter untereinander (Stichwort: Kollaboration), da zusätzlich die hierarchische Kommunikationsstruktur überwunden werden könnte (Stichwort „kurzer Dienstweg“).

Zusammengefasst zeigt sich, dass der theoretische Diskurs das Modernisierungspotential von *Social Media* normativ im Sinne gesellschaftlich-sozialer Utopien stark überdehnt und empirisch nachweisbare negative Tendenzen eher ausblendet

werden. Hierdurch muss sich der Diskurs der Kritik aussetzen, dass er zur PR missbraucht wird, bei der *Social Media* als „Allheilmittel“ der Kommunikationspraxis vermarktet wird, um beliebige Ziele zu forcieren. Twitter-Star US-Präsident Donald Trump (Chef der amerikanischen Bundesverwaltung), gilt beispielsweise als Negativbeispiel für die Verrohung der Sitten bei der öffentlichen *Social Media*-Kommunikation. Seine Twitter-Kommunikation fällt durch öffentliche Entgleisungen, Beleidigungen, Maßregelungen und Entlassungen von Mitarbeitern auf. Die Kommunikation mit den Bürgern ist populistisch, wobei eher mit persönlicher Meinung und „alternativen Fakten“ argumentiert wird (vgl. Henze 2017).

Neben dem dominierenden rauen und satirischen Umgangston zeigen zahlreiche internationale Studien, dass sich die demokratiefördernden Hoffnungen nicht erfüllen. Das Beispiel des gescheiterten militärischen Putschversuches in der Türkei, bei dem mit Hilfe eines Messengerdienstes eine demokratisch gewählte Regierung gestürzt werden sollte, zeigt, dass *Social Media*-Technologien keinen demokratiefreundlichen *Bias* haben. Demokratisierende Effekte sind selbst in gut funktionierenden Demokratien nicht zwangsläufig zu erwarten. Dies hat zwei Gründe: Erstens entwickeln sich die *Social Media*-Dienste mit intransparenten Algorithmen selbst zu Gatekeepern. Zweitens können inhaltlich *Fake-News* oder *Social-Bots* sachliche öffentliche Diskussionen stören. Als prominentes Beispiel gilt hierbei der US-Präsidentschafts-Wahlkampf 2016, bei dem Russland vorgeworfen wird, über *Social-Bots* und *Fake-News* das amerikanische demokratische System manipuliert zu haben.

---

### 3 Praktische Anwendungsfelder

Inwieweit die Nutzung von *Social Media*-Diensten die Kommunikation zwischen Bürger, Staat und Verwaltung in Deutschland überhaupt Anwendung finden kann, hängt mit mehreren Faktoren zusammen. Zunächst zeigen die geringen Nutzerzahlen, dass die Deutschen derzeit eher als *Social Media*-Muffel einzuschätzen sind, wenn es um die Kommunikation außerhalb des persönlichen Umfeldes geht. Im Jahr 2017 belegt die ARD-ZDF-Onlinestudie, dass besonders *WhatsApp* und *Facebook* die am meisten genutzten *Social Media*-Dienste seitens der Bevölkerung sind. Deutlich wird, dass *WhatsApp* am meisten genutzt wird und ein Nutzerwachstum verzeichnet, allerdings ist der Dienst für eine öffentliche Diskussion ungeeignet. Anders ist es bei *Facebook*, das aber leicht rückläufige Nutzerzahlen aufweist. *Twitter* spielt eine geringe Rolle, außer in den jüngeren Altersklassen. Eine öffentliche mehrdimensionale Kommunikation mit den Bürgern ist folglich rein strukturell nur bei *Facebook* möglich.

Komplementär zu der Frage, wo Bürger aktiv sind; stellt sich die Frage nach der Aktivität von Staat und Verwaltung in *Social Media*. Grundsätzlich zeigt sich der Trend, dass Politiker, Parteien und Fraktionen vor allem *Facebook* und *Twitter* nutzen, um mit den Bürgern zu kommunizieren. Dies war gerade auch im Bundestagswahlkampf 2017 zu beobachten. Hier zeigen sich verschiedene Kommunikationspotenziale mit Politikern und Parteien, die aber nicht zur Verwaltungskommunikation zählen.

Wird die Verwaltungskommunikation betrachtet, dann sind zuvörderst die rechtlichen Rahmenbedingungen für das Nutzen von sozialen Medien relevant: Bis November des Jahres 2017 war in Deutschland nicht definiert, wie staatliche Institutionen *Social Media*-Dienste aus Sicht des Datenschutzes überhaupt nutzen dürfen. Die Neue Richtlinie des Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) zur Nutzung von Sozialen Netzwerken durch öffentliche Stellen aus Baden-Württemberg (2018) gilt seither bundesweit als Richtschnur. Zentral ist vor allem die Feststellung, dass unabhängig vom Betreiben von *Social Media*-Kanälen immer auch alternative Kommunikationskanäle und Informationsquellen betrieben werden müssen.

Vor dem Hintergrund der Datenschutzgrundverordnung (DSGVO) argumentiert der Landesbeauftragte aus Baden-Württemberg (2017), dass das Betreiben von *Social Media*-Kanälen zulässig ist, weil beispielsweise in *Twitter* keine Klarnamenspflicht besteht. Trotzdem bleiben datenschutzrechtliche Fragen. Problematisch ist die Nutzeridentifikation bzw. Anonymisierung bei den *Social Media*-Diensten für die Kommunikation zwischen Bürgern und Verwaltung. So können beispielsweise *E-Government*-Dienstleistungen oder tiefergehende öffentliche Nachfragen nur dann bearbeitet werden, wenn der Nutzer identifizierbar (ID-Technologie) ist, aber wenn er dies ist, dann greifen datenschutzrechtliche Schranken, die den Einsatz von *Social Media* verhindern.

Ein Sonderfall stellen polizeiliche *Social Media*-Aktivitäten dar, um die in der Bundesrepublik ein intensiver kontroverser Diskurs geführt wird. Bereits im Jahr 2015 befasste sich der Wissenschaftliche Dienst des Deutschen Bundestages mit der Frage, ob polizeiliches Echtzeit-*Twittern* rechtswidrig ist (Deutscher Bundestag – Wissenschaftlicher Dienst 2015). Ohne das Vorliegen eines Gefahrverdachts ist beispielsweise das Erheben und *Twittern* von Fotos durch die Polizei als Gefahrenabwehrbehörde rechtswidrig. Bei der Öffentlichkeitsfahndung der Polizei gelten die gesetzlichen Vorschriften, die auch *offline* zum Tragen kommen. In einem weiteren Gutachten des Wissenschaftlichen Diensts des Deutschen Bundestages aus dem Jahr 2018 wird festgestellt, dass die Polizei unliebsame Nutzer nicht einfach blockieren darf (Deutscher Bundestag – Wissenschaftlicher Dienst 2018). Wird die Kommentiermöglichkeit von Beiträgen z. B. für einen bestimmten Nutzer eingeschränkt, dann kann dies dessen Meinungsfreiheit verletzen (Art. 5 Abs. 1 GG). Die Polizei kann folglich nicht den Zugang eines Nutzers allein wegen einer missliebigen Meinung beschränken, die durch die Meinungsfreiheit gedeckt ist. In der Kritik steht die Polizei auch beim Einsatz von sogenannter *Social-Listening-Software*, bei der die *Social Media*-Kommunikation nach bestimmten potenziellen Gefahrenbegriffen durchsucht wird. Diese Techniken werden für die präventive Polizeiarbeit wichtiger, wobei gleichzeitig die Grenze zwischen geheimdienstlichen Methoden verschwimmt. Mittlerweile experimentiert die Polizei (z. B. in Rheinland-Pfalz) auch mit *Instagram*. Ziel ist hierbei die Nachwuchsrekrutierung. Gleiches gilt auch für die Bundeswehr.

Besonders die politische Verwaltungsspitze nutzt *Social Media*-Kanäle teilweise viel umfangreicher, weil eine Trennung zwischen Amts- und Privatperson in der Praxis nicht immer eindeutig ist. Ein Beispiel ist Bundeswirtschaftsminister Peter

Altmaier, der sich wie folgt in seinem *Twitter*-Profil beschreibt: „Bundesminister für Wirtschaft und Energie. Mitglied des Deutschen Bundestages, CDU. Alle Tweets von mir und meine Meinung.“

Bilanzierend zeigt sich in der praktischen Anwendung primär eine zunehmende Professionalisierung in jenen Bereichen, in denen Staat und Verwaltung auf Bürger als Ressource zurückgreifen möchten. Ebenfalls wird deutlich, dass die *Social Media*-Kommunikation ein vordringliches Anwendungsfeld der politischen Kommunikation ist und dadurch strukturell die Pressestellen der Verwaltungen sowie die politischen Verantwortlichen der jeweiligen Verwaltungen im Zentrum stehen.

---

## 4 Umsetzungsstand und Auswirkungen

Gerade die politisch besetzte Verwaltungsspitze (Wahlbeamte) nimmt bei der Umsetzung von *Social Media* eine Vorreiterrolle ein, da sie *Social Media* als zusätzlichen Kanal zur Pressestelle versteht, um schnell und direkt auf Themen und Ereignisse reagieren zu können. Privates *Twittern* von „einfachen“ Verwaltungsmitarbeitern über ihre konkreten Verwaltungstätigkeiten ist in Deutschland nicht exakt geregelt, aber in der Tendenz unerwünscht. In der Presseberichterstattung wird sporadisch auf Fehlverhalten von Verwaltungsmitarbeitern beim Umgang mit *Social-Media* verwiesen (z. B. SWR 2018).

Letztlich betreiben zahlreiche deutsche staatliche Institutionen mittlerweile „offizielle“ *Social Media*-Kanäle. Der Dienstleister Pluragraph.de zählte im Juni 2018 fast 3000 staatliche Organisationen. Eine Gesamtbetrachtung aller ist aber in diesem Beitrag nicht möglich. Folgende Tabelle gibt einen ausgewählten Überblick der Verwaltungsbereiche und ihren *Social Media*-Aktivitäten auf der Bundesebene, da auf dieser Verwaltungsebene teilweise besonders umfangreich auf *Social Media* gesetzt wird und einige Kanäle eine besonders hoher Resonanz (Anzahl der *Follower*, Fans oder Abonnenten) aufweisen. Allerdings gibt es auch ‚Totalverweigerer‘ (Tab. 2).

Bilanzierend zeigt sich, dass *Social Media*-Repräsentanzen der Bundesverwaltung(en) in Deutschland überwiegend auf *Facebook* und *Twitter* zu finden sind. Die *Facebook*-Kanäle weisen fast immer auch die meisten Fans (Synonym zu *Follower*) auf, im Vergleich zu den Fans bzw. Abonnenten anderer *Social Media*-Dienste. Einzige Ausnahme ist der *Twitter*-Kanal der Bundesregierung. Dieser ist kein klassischer Verwaltungsauftritt in *Twitter*, sondern der persönliche *Twitter*-Kanal des Regierungssprechers. Die Bundesregierung bzw. die Bundesministerien sowie Polizei und Bundeswehr sind gemessen an den *Follower*-Zahlen am erfolgreichsten mit ihren Angeboten. Die anderen Bundesverwaltungen sind weit weniger erfolgreich. In einigen Fällen sind deren *Social Media*-Kanäle noch nicht einmal *verifiziert*, d. h. sie sind nicht als echt gezeichnet. Bemerkenswert ist aber auch, dass das Bundespräsidialamt und die Bundestagsverwaltung keine *Social Media*-Repräsentanzen betreiben, während der Bundesrat hingegen erfolgreich *twittert*.

Werden Landes- oder Kommunalverwaltungen betrachtet, dann sind die *Social Media*-Repräsentanzen sehr heterogen aufgestellt. In der Tendenz wird auch hier vor

**Tab. 2** Überblick der Social Media-Repräsentanzen bei der Bundesverwaltung

Institution	Facebook	Twitter	Instagram	Youtube
Bundespräsidialamt	–	–	–	–
Bundesverfassungsgericht	–	+ (20 Tsd. Follower)	–	–
Bundestag	–	–	–	–
Bundesrat	–	+ (89 Tsd. Follower)	–	–
Bundesregierung	+ (520 Tsd. Fans)	+ (916 Tsd. Follower)	+ (602 Tsd. Follower)	+ (22,3 Tsd. Abonnenten)
Bundesamt für Migration und Flüchtlinge	+ (96 Tsd. Follower)	+ (30,4 Tsd. Follower)	+ (0,2 Tsd. Follower)	–
Bundeswehr	+ (425 Tsd. Fans)	+ (68,4 Tsd. Follower)	+ (193 Tsd. Follower)	+ (0,3 Tsd. Abonnenten)
Bundespolizei	+ (75 Tsd. Fans)	+ (46 Tsd. Follower)	+ (46 Tsd. Tsd. Follower)	+ (17 Tsd. Abonnenten)
Bundeskriminalamt	+ (70 Tsd. Fans)	+ (36,6 Tsd. Follower)	+ (3,6 Tsd. Follower)	–
Bundesamt für Bauwesen und Raumordnung	–	–	–	–
Bundesagentur für Arbeit	–	+ nicht verifiziert (5,4 Tsd. Follower)	–	–
Bundesamt für Verbraucherschutz und Lebensmittelsicherheit	–	+ nicht verifiziert (1,1 Tsd. Follower)	–	–
Bundesamt für Verfassungsschutz	–	+ (4,7 Tsd. Follower)	–	–
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	–	+ (15,4 Tsd. Follower)	–	–

(Fortsetzung)

**Tab. 2** (Fortsetzung)

Institution	Facebook	Twitter	Instagram	Youtube
Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen	–	+(6,8 Tsd. Follower)	–	–
Bundesversicherungsamt	–	–	–	–
Bundesverwaltungsamt	–	–	–	–
Bundeszentralamt für Steuern	–	–	–	–
Deutsche Patent- und Markenamt	–	–	–	–
Umweltbundesamt	+ (22,3 Tsd. Fans)	+(0,8 Tsd. Follower)	+(3,8 Tsd. Follower)	+(0,8 Tsd. Abonnenten)
Bundesamt für Justiz	–	–	–	–

Datenbasis: Juni 2018

allem auf *Twitter* gesetzt. Danach folgt *Facebook*. Hauptsächlich besteht das Problem, dass die *Social Media*-Repräsentanzen der Landes- oder Kommunalverwaltungen oft nicht verifiziert sind. Dies ist sogar unabhängig von der Anzahl der *Follower*. So betreibt beispielsweise der Stadtstaat Hamburg eine der erfolgreichsten *Twitter*-Repräsentanzen in Deutschland. Der *Twitter*-Kanal (@hamburg\_de) besteht seit dem Jahr 2007 und verfügt über mehr als 230 Tsd. *Follower*. Trotzdem ist er von *Twitter* nicht verifiziert. Das bedeutet, dass *Twitter* diesen Kanal nicht als „echt“ kennzeichnet. Mit anderen Worten könnte es theoretisch auch ein *Fake-Account* sein. (Warum eine Verifizierung seitens *Twitter* nicht erfolgt kann an dieser Stelle nicht beantwortet werden, weil *Twitter* beim Verifizierungsverfahren nicht transparent agiert (König und König 2016b)). Problematisch ist für die Kommunikation mit dem Bürger folglich, dass in der Regel oft nicht deutlich wird, ob er wirklich mit der echten Verwaltung kommuniziert. Dies betrifft gerade die kommunalen Verwaltungsebenen, mit denen der Bürger am ehesten in Kontakt steht.

Neben diesen strukturellen Bedingungen der *Social Media*-Kommunikation stellen sich aber auch inhaltliche Fragen der Kommunikation mit dem Bürger. Exemplarisch wird nachfolgend die Kommunikationsstrategie des Bundespressesamtes skizziert, das mit einer dafür eigens eingerichteten *Social Media*-Redaktion verschiedene *Social Media*-Kanäle im Namen der gesamten Bundesregierung betreut. Diese Redaktion wird neben hauptamtlichen Mitarbeitern auch von einer privaten Kommunikationsagentur unterstützt. Inhaltlich besteht ein qualitativer Unterschied bei der Zielgruppenkommunikation. *Facebook*, *Youtube* und *Instagram* richten sich in erster Linie an politisch interessierte Bürger. Hierbei steht der Dialog mit der jüngeren Zielgruppe im Vordergrund (vgl. Recherche von NDR.de 2016): Die *Facebook*-Seite der Bundesregierung (über 501 Tsd. Fans) bietet beispielsweise allgemeine Informationen zu Terminen und Veranstaltungshinweisen. Außerdem werden teilweise Fragen von Bürgern zu bestimmten Beiträgen öffentlich sichtbar vom *Social Media*-Team beantwortet. Allerdings sind diese Antworten nicht immer qualitativ hochwertig. Die Frage der Seriosität stellt sich zunehmend dort, wo der informative Nutzerwert durch einen Unterhaltungswert abgelöst wird. Beispiele-

weise themisierte der Satiriker Jan Böhmermann im Frühjahr 2018 das „flapsige“ Antwortverhalten der Bundesregierung in seiner TV-Show.

Der *Twitter*-Account des Regierungssprechers richtet sich dagegen vorrangig an die politisch interessierte Öffentlichkeit (z. B. Journalisten). Stellvertretend für die Bundesregierung *wittert* Regierungssprecher Steffen Seibert (@RegSprecher) persönlich seit dem Jahr 2011. Mit über 900 Tsd. *Followern* betreibt er den erfolgreichsten *Twitter*-Kanal der Verwaltung in Deutschland.

---

## 5 Perspektiven für Staat und Verwaltung

Letztlich zeigt sich, dass die *Social Media*-Kommunikation bisher vor allem rein rechtlich nur ein ergänzender Kommunikationskanal von Staat und Verwaltung sein kann. Ein exklusiver Informationswert ist daher auch zukünftig nicht zu erwarten.

Zahlreiche staatliche Institutionen betreiben *Social Media*-Kanäle, aber in der Kommunikationspraxis werden die mehrdimensionalen Kommunikationsmöglichkeiten der neuen Technologien nicht genutzt. Vielmehr dominiert die eindimensionale Kommunikation aus Bürgersicht. Auf *Social Media*-Diskussionen mit der Verwaltung wird der Bürger in der Regel erst durch das Aufgreifen dieser Diskussionen seitens der klassischen Medien aufmerksam. Daher ist auch in Zukunft eine zunehmende digitale Transformation der klassischen Öffentlichkeitsarbeit zu erwarten. Die Verwaltung versucht sich hierbei als „positiv modern“ (im PR-Jargon: „positives Markenumfeld“) zu präsentieren. Die Kommunikation wird zunehmend professioneller, je eher Verwaltung und Staat auf den Bürger als Ressource zurückgreifen möchten.

Umgekehrt zeigt sich gerade aus der Perspektive der Dienstleistung am normalen Bürger ein deutlich unausgeschöpftes Potenzial. Wenn beispielsweise *Facebook*-Angebote bestehen, bei denen mehrdimensionale Kommunikationsmöglichkeiten explizit angeboten werden, dann stellen diese entsprechend meist ein Kommunikationsangebot zwischen Bürgern und der Pressestelle bzw. speziellen *Social Media*-Teams dar. Gerade hier könnte der informative Nutzerwert noch erhöht und der Unterhaltungswert reduziert werden. Die Antworten sind nämlich oftmals nicht mit denen einer Fachverwaltung vergleichbar, sondern dienen bestenfalls einer ersten Lotsenfunktion, um dann mit zuständigen Mitarbeitern in Kontakt zu kommen. Belastbare Bürgerbeteiligung oder ein Bürgerdialog findet zudem aus rechtlichen Gründen nicht in *Social Media*-Kanälen statt. Vielmehr werden interessierte Bürger über *Social Media*-Kanäle hin zu Bürgerbeteiligungsplattformen gelotst.

Gerade bei *Twitter* scheint es so, dass das puristische *Twittern* von *Links* zunehmend zur Suchmaschinen-Optimierung eingesetzt wird.

Als grundsätzlich eher hemmend für die zukünftige Entwicklung einer bürgernahen *Social Media*-Kommunikation erweist sich nach wie vor das intransparente Verifizierungssystem der *Social Media*-Dienste, die oft ein einfaches Erkennen echter Verwaltungsangebote nicht ermöglichen. Zudem stellen sich neben Datenschutzfragen bei der *Social Media*-Kommunikation auch Grundsatzfragen in Bezug auf Bürgerrechte, falls die Verwaltung beispielsweise unliebsame Nutzer in *Social Media* blockiert oder *Social Listening*-Technologien einsetzt.

## Literatur

- Deutscher Bundestag (Wissenschaftlicher Dienst). 2015. Öffentlichkeitsarbeit von Polizeibehörden in sozialen Medien. <https://www.bundestag.de/blob/405538/c90e0606186c97afa54b9694a865e026/wd-3-157-15-pdf-data.pdf>. Zugegriffen am 19.03.2017.
- Deutscher Bundestag (Wissenschaftlicher Dienst). 2018. Zugang zur Öffentlichkeitsarbeit der Polizei in sozialen Medien („Twitter“). <https://www.andrej-hunko.de/start/download/dokumente/1110-gutachten-des-wissenschaftlichen-dienstes-im-bundestag-zugang-zur-oeffentlichkeitsarbeit-der-polizei-in-sozialen-medien>. Zugegriffen am 19.03.2018.
- Henze, Arnd. 2017. Trumps Twitterei. In 140 Zeichen zur Weltkrise?. <https://www.tagesschau.de/ausland/trump-twitter-111.html>. Zugegriffen am 03.11.2018.
- Hoffman, Lindsay H. 2012. Participation or Communication? An Explication of Political Activity in the Internet Age. *Journal of Information Technology & Politics* 9(3): 217–233.
- König, Mathias, und Wolfgang König. 2016. Web 2.0 und der SPD-Mitgliederentscheid zur „GroKo“. Twitter-Kommunikation als Qualitätsmerkmal digitaler Demokratie? *Zeitschrift für Vergleichende Politikwissenschaft* 10(2): 151–178.
- König, Mathias, und Wolfgang König. 2016b. #MythosTwitter. Chancen und Grenzen eines sozialen Mediums (OBS-Arbeitspapier 24). [https://www.otto-brenner-stiftung.de/fileadmin/user\\_data/stiftung/02\\_Wissenschaftsportal/03\\_Publikationen/AP24\\_Twitter\\_Koenig\\_2016\\_10\\_05.pdf](https://www.otto-brenner-stiftung.de/fileadmin/user_data/stiftung/02_Wissenschaftsportal/03_Publikationen/AP24_Twitter_Koenig_2016_10_05.pdf). Zugegriffen am 03.11.2018.
- König, Wolfgang, und Mathias König. 2018. Digitale Öffentlichkeit. Facebook und Twitter im Bundestagswahlkampf 2017. <http://www.bpb.de/dialog/podcast-zur-bundestagswahl/264748/digitale-oeffentlichkeit-facebook-und-twitter-im-bundestagswahlkampf-2017>. Zugegriffen am 22.05.2016.
- Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI). 2017. Neue Richtlinie des LfDI zur Nutzung von sozialen Netzwerken durch öffentliche Stellen. [https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2017/11/2017\\_11\\_02\\_Richtlinie-zur-Nutzung-sozialer-Netzwerke-durch-%C3%B6ff-Stellen.pdf#](https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2017/11/2017_11_02_Richtlinie-zur-Nutzung-sozialer-Netzwerke-durch-%C3%B6ff-Stellen.pdf#). Zugegriffen am 19.03.2018.
- Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI). 2018. Twitter-Datenschutzfolgenabschätzung. <https://www.baden-wuerttemberg.datenschutz.de/twitter-datenschutzfolgenabschaetzung>. Zugegriffen am 27.06.2018.
- NDR.de. 2016. Social Media der Bundesregierung. <https://www.ndr.de/nachrichten/netzwelt/Social-Media-der-Bundesregierung,bundespresseamt102.html>. Zugegriffen am 27.06.2018.
- Newman, Nic, Richard Fletcher, Antonis Kalogeropoulos, und David A. L. Levy. 2018. *Reuters institute digital news report 2018*. Oxford: Reuters Institute for the Study of Journalism/University of Oxford. <http://media.digitalnewsreport.org/wp-content/uploads/2018/06/digital-news-report-2018.pdf?x89475>. Zugegriffen am 03.11.2018.
- SWR. 2018. Ordnungsamt-Mitarbeiter der Stadt Worms: Keine Ermittlungen nach Rassismus-Vorfall. <https://www.swr.de/swraktuell/rp/ordnungsamt-mitarbeiter-der-stadt-worms-keine-ermittlungen-nach-rassismus-vorfall/-/id=1682/did=20932958/nid=1682/qclqx4/>. Zugegriffen am 03.11.2018.



---

# Civic Tech (digitale Bürgerzentrierung)

Stefan Baack, Christian Djeffal, Juliane Jarke und Hendrik Send

## Inhalt

1 Klärung des Begriffs .....	338
2 Theoretische Grundlagen .....	339
3 Praktische Anwendung .....	340
4 Umsetzungsstand und Diskussion .....	342
5 Fazit: Künftige Entwicklung .....	344
Literatur .....	345

---

## Zusammenfassung

*Civic Tech* beschreibt Anwendungen, durch die Bürger\*innen sich einfacher engagieren und informieren können. Neu an *Civic Tech* ist die potenzielle Nutzerreichweite und die Bandbreite an Anwendungsfällen durch die Nutzung offener Daten. *Civic Tech* als Leitbild der Verwaltungsdigitalisierung impliziert, dass die Verwaltung stärker bürgerzentriert arbeitet und die Entwicklung von Softwareanwendungen im Sinne von *Civic Tech* unterstützt, etwa durch offene Daten.

---

S. Baack (✉)

Weizenbaum Institut, Berlin, Deutschland

E-Mail: [sbaack@zedat.fu-berlin.de](mailto:sbaack@zedat.fu-berlin.de)

C. Djeffal

Munich Center for Technology in Society, Technische Universität München, München, Deutschland

E-Mail: [christian.djeffal@tum.de](mailto:christian.djeffal@tum.de)

J. Jarke

ifib: Institut für Informationsmanagement Bremen GmbH, Universität Bremen, Bremen, Deutschland  
E-Mail: [jjarke@ifib.de](mailto:jjarke@ifib.de)

H. Send

Alexander von Humboldt Institut für Internet und Gesellschaft, Berlin, Deutschland

Fachbereich Wirtschaft, Hochschule Anhalt, Bernburg, Deutschland  
E-Mail: [hendrik.send@hiig.de](mailto:hendrik.send@hiig.de)

## Schlüsselwörter

Partizipation · Offene Daten · Bürgergenerierte Daten · Informationsfreiheit · Zivilgesellschaft

### 1 Klärung des Begriffs

Im deutschsprachigen Raum werden „Civic-Tech-Anwendungen“ häufig als „digitale Werkzeuge für Bürger\*innen“ beschrieben, die sie in der Ausübung ihrer demokratischen Rechte unterstützen und Bürgerbeteiligung sowie Transparenz staatlicher Prozesse fördern (siehe bspw. <https://codefor.de/>). In dieser Definition spiegelt sich die Essenz von „Civic Tech“: Es geht um digitale Anwendungen, die sich primär an den Bedürfnissen von Bürger\*innen orientieren und es ihnen in unterschiedlichen Formen erleichtern sollen, sich stärker an politischen Prozessen zu beteiligen, öffentliche Dienstleistungen wahrzunehmen oder von ihren Rechten Gebrauch zu machen. Bekannte Beispiele in Deutschland sind *Abgeordnetenwatch.de*, welches es Nutzer\*innen u. a. einfacher macht, ihre Bundes- oder Landtagsabgeordneten zu finden und zu kontaktieren, oder *FragDenStaat.de*, welches das Verfassen und Versenden von Informationsfreiheitsanfragen vereinfacht.

Das wirklich Neue an *Civic Tech* ist dabei weniger der Grundgedanke, Bürger\*innen stärker die Möglichkeit zum Engagement zu bieten und einzubinden, als die Skalierung entsprechender technischer Lösungsansätze unter Nutzung von offenen oder bürger generierten Daten. Das Aufkommen von *Civic Tech* ist entsprechend eng mit der Idee und Umsetzung von *offenen Daten* und *Informationsfreiheit* verbunden, da beides zentrale Voraussetzung für die Entwicklung von *Civic-Tech*-Anwendungen ist. Einerseits können durch Daten stärker individualisierte und benutzerfreundliche Services entwickelt werden, andererseits können durch das Sammeln von Daten neue Formen der Transparenz hergestellt werden. Die Anwendung *FixMyStreet.com* aus Großbritannien, mit der Nutzer\*innen lokale Infrastrukturprobleme wie Schlaglöcher an zuständige Behörden melden können, veranschaulicht beides. Einerseits nutzt *FixMyStreet* hierfür Daten über die Zuständigkeitsbereiche der Behörden, andererseits sammelt die Anwendung aber auch die von Nutzer\*innen gemeldeten Probleme und visualisiert sie auf einer Karte. Hierdurch können Bürger\*innen nachvollziehen, wo besonders viele Probleme bestehen und wie lange die zuständigen Behörden für die Bearbeitung benötigen.

*Civic Tech* zeichnet sich vor allem durch einen technologiegetriebenen Ansatz und eine ausgeprägte Bürgerorientierung aus; der Begriff wird aber sehr unscharf verwendet. Das hat einerseits zu seiner Popularität beigetragen, da viele unterschiedliche Gruppen unter dem Stichwort *Civic Tech* zusammenfinden, die sich alle im weitesten Sinne mit der Entwicklung von digitalen Anwendungen für Bürger\*innen beschäftigen. Andererseits erschwert diese Offenheit aber auch eine klare Abgrenzung gegenüber verwandten Konzepten wie „Co-Creation“. *Civic Tech* ist am besten als übergeordneter Sammelbegriff zu verstehen, dem viele unterschiedliche Kon-

zepte zugeordnet werden können. So kann *Civic Tech* durchaus Anwendungen im Bereich der Co-Creation umfassen, insofern sich diese Anwendungen primär an Bürger\*innen richten. Darüber hinaus können *Civic-Tech*-Anwendungen von unterschiedlichen Akteuren entwickelt und bereitgestellt werden. Dazu zählen gemeinnützige und nicht-profitorientierte Organisationen, Unternehmen und natürlich auch Verwaltungen, die (bestimmte) Bürger\*innen als Zielgruppe ihrer Anwendung haben, diese aber nicht explizit in den Entwicklungsprozess einbeziehen.

Der Fokus dieses Artikels liegt auf *Civic Tech* in seiner primären Ausprägung: als von *Non-profit*-Organisationen entwickelte digitale Anwendungen, die als Schnittstellen zwischen Verwaltung und Bürger\*innen fungieren. *Non-profit*-Organisationen rund um *Civic Tech* bilden inzwischen ein weltweites Netzwerk, welches durch internationale Austauschprogramme („Fellowships“), Konferenzen und transnational operierenden Organisationen wie ‚Code for All‘ gestützt wird. Finanziert werden solche Organisationen und Netzwerke vor allem durch Stiftungen, staatliche Fördergelder, große IT-Unternehmen und private Spenden.

*Civic-Tech*-Anwendungen aus dem *Non-profit*-Bereich bezwecken nicht in erster Linie, der Verwaltung Arbeit abzunehmen. Stattdessen geht es darum, die Nutzung von Verwaltungsdienstleistungen durch Bürger\*innen zu vereinfachen und die Arbeit der Behörden für sie transparenter zu machen. So kann das o. g. Beispiel *FragDenStaat.de* als Plattform verstanden werden, die die Kommunikation zwischen Behörden und Bürger\*innen vereinfacht und gleichzeitig den Umgang von Behörden mit Anfragen transparent macht, da die Reaktion auf Informationsfreiheitsanfragen von *FragDenStaat.de* dokumentiert wird. Den zivilgesellschaftlichen Akteuren geht es hier nicht nur um technologische Lösungen, sondern weitergehend um einen kulturellen Wandel im Verhältnis von Verwaltung und Bürger\*innen: eine Entwicklung hin zu einer größeren Offenheit, Transparenz und Kooperationsbereitschaft von Politik und Verwaltung und zum Teil auch eine stärkere Einbindung von Bürger\*innen in Entscheidungsprozesse der öffentlichen Verwaltung. *Civic Tech* als Leitbild setzt die Verwaltungsdigitalisierung also in einen größeren kulturellen Kontext, der sich nicht nur auf die Verwaltung, sondern auch auf das Engagement und Selbstverständnis von Bürger\*innen bezieht: Verwaltungen sollen Weichen stellen und die Entwicklung von *Civic-Tech*-Anwendungen ermöglichen, aber Bürger\*innen sollten diese Angebote auch wahrnehmen, mitgestalten oder selbst anregen.

---

## 2 Theoretische Grundlagen

Historisch betrachtet vereint *Civic Tech* unterschiedliche Konzepte, die vor allem aus dem anglo-amerikanischen Raum stammen: „offene Daten“, „Open Government“ und Informationsfreiheit. Grob gesagt ist *Civic Tech* eine Zusammenführung von zwei unterschiedlichen Offenheitskonzepten. Einerseits umfasst *Civic Tech* eine durch das Recht geförderte Offenheit im Sinne der Informationsfreiheit. Informationsfreiheitsrechte räumen Bürger\*innen das Recht ein, bislang unveröffentlichte Dokumente von der Regierung einzufordern. Andererseits näherte sich dieser juris-

tisch verankerte Offenheitsbegriff mit dem Aufkommen und der Verbreitung des Internets langsam dem Offenheitsbegriff der *Open-Source-Kultur*, der auf freiem Austausch und Kollaboration im Hinblick auf *Software* oder andere Produkte beruht (Yu und Robinson 2012).

Diese Annäherung wurde sowohl von stärker technologie-fokussierten *Open-Source-Communities* als auch von eher an Informationsfreiheit interessierten Gruppen vorangetrieben. Letztere sahen in der erweiterten Konnektivität und dem vereinfachten Zugriff auf Daten eine Art ‚natürliche Erweiterung‘ der den Informationsfreiheitsgesetzen zugrunde liegenden Ideen von Offenheit und Transparenz. Anhänger der *Open-Source*-Idee legten den Fokus hingegen stärker auf neue Möglichkeiten der Kollaboration beruhend auf einer weitergehenden Form der Transparenz. Der Begriff der Beteiligung wird im Bereich *Civic Tech* dabei weit verstanden und umfasst Handlungen von Bürger\*innen, die sich freiwillig durch die Nutzung von digitalen Plattformen und Anwendungen mit politischen oder gesellschaftlichen Themen aus-einandersetzen (Theocharis 2015).

Indem *Civic Tech* Bürger\*innen auf verschiedenen Ebenen in den Mittelpunkt stellt, steht es im Kontrast zu einer effizienz- und kostengetriebenen Verwaltungsdigitalisierung. Im Vergleich dazu ist etwa der Begriff des „E-Government“ zweck-offen und wird in verschiedenen Richtungen verwandt: von Bürgerorientierung bis Effizienzsteigerung. Als Leitbild kann *Civic Tech* dem Teil des *E-Government* eine Kontur geben, der strikt Bürger\*innen in den Mittelpunkt des Verwaltungshandels stellt. *Civic Tech* überträgt Leitbilder der Bürgerzentrierung und Bürgerbeteiligung weiter auf die Verwaltungsdigitalisierung und bildet so ein eigenes spezifisches Leitbild der Verwaltungsdigitalisierung aus. Die technologische Komponente dieses Leitbilds bezieht sich auf unterschiedliche Formen der Offenheit der Verwaltung. Nach diesem Leitbild können Bürger\*innen durch Anwendungen, die offene Daten für sie nutzbar und zugänglich machen, besser verstehen, was in der Verwaltung vor sich geht, und dies auch in verschiedenen Graden mitbestimmen. Daher zielt *Civic Tech* auf das Bild engagierter Bürger\*Innen, die in ihrem Gesichtskreis Verantwortung übernehmen. Studien zur Nutzung von *Civic-Tech*-Anwendungen in Großbritannien zeigen, dass sich Nutzer\*innen oft als ‚Sprachrohr‘ ihrer Gemeinschaften verstehen (Cantijoch et al. 2016). Aus dieser Zusammenschau ergibt sich eine neue Verwaltungskultur der Zusammenarbeit zwischen Verwaltung und Bürger\*innen, bei der die Interessen der Bürger\*innen im Mittelpunkt stehen.

---

### 3 Praktische Anwendung

Als Leitbild der Verwaltungsdigitalisierung stellt *Civic Tech* die technischen und juristischen Weichen, die es *Non-profit*-Organisationen ermöglichen, *Civic-Tech*-Anwendungen zu entwickeln. Es geht aber auch um einen kulturellen Wandel innerhalb der Verwaltungen. Bei der Umsetzung dieses Leitbilds lassen sich grundsätzlich vier Interaktionsmodelle zwischen Verwaltung und Bürger\*innen unterscheiden (Sieber und Johnson 2015).

**Data Publishing:** In diesem Modell stellen Verwaltungen offene Daten kostenfrei zur Verfügung, die anderen Akteuren dazu dienen, Anwendungen zu entwickeln. Gemäß den Anforderungen der *Open Knowledge Foundation* (2014) sollten offene Daten über keine Kontrollmechanismen wie restriktive Lizzenzen verfügen und für jedermann frei verfügbar und wiederverwendbar sein und weiterverbreitet werden dürfen. Die Verwaltung verfügt beispielsweise über Daten zu Auftragsvergaben, zur Qualität der Gesundheitsversorgung, zur Verkehrsentwicklung und Unfällen sowie über umfangreiche Statistiken wie z. B. Kriminalstatistiken. Werden diese Daten strukturiert und mit einem brauchbaren Lizenzmodell zur Verfügung gestellt, kann die Zivilgesellschaft sie in einer Vielzahl von Kontexten nutzen und informierter entscheiden. Hierbei ist die öffentliche Verwaltung jedoch lediglich Datenlieferantin und nicht Ideengeberin; sie erteilt keine Aufträge an NGOs, sondern diese entwickeln eigene Ideen, wie offene Daten sinnvoll und im Interesse von Bürger\*innen genutzt werden können. So nutzen in vielen Städten Initiativen wie z. B. „Transportation Alternatives“ in New York Unfalldaten der Vergangenheit, um Fahrradfahrer\*innen problematische Routen und Orte zu zeigen. In Deutschland nutzen zum Beispiel die *OK-Labs* der *Open Knowledge Foundation* in mehreren Großstädten offene Verwaltungsdaten, um Verwaltungshandeln oder andere Informationen zu ihren Städten zu visualisieren (<https://codefor.de/>).

**Code-Austausch:** In diesem Modell fördern Regierung oder Verwaltung ausdrücklich die Entwicklung von innovativen Anwendungen, die auf offenen Daten basieren. Die Bereitstellung von Daten wird von unterstützenden Aktivitäten wie „App-Wettbewerben“ begleitet. Es ist eine Art *Outsourcing* der App-Entwicklung durch die Verwaltung. Verschiedene öffentliche Organisationen haben in der Vergangenheit sogenannte „Hackathons“ veranstaltet, in denen digitale Anwendungen auf Basis offener Daten prototypisch umgesetzt werden, wie der EU-Hackathon des Europäischen Parlaments.

**Civic Issue Tracker:** In diesem Modell wird die Richtung der Interaktion umgekehrt. NGOs oder Verwaltungen fordern Bürger\*innen auf, Probleme wie Schlaglöcher oder Lärmbeschwerden zu melden oder *Feedback* zu veröffentlichen. Daten und Dokumenten zu geben. Die Daten werden hier also von den Bürger\*innen generiert. Dieses Modell kann unabhängig von den beiden anderen Modellen angewendet werden, kann aber auch kombiniert werden, wenn die Bürger\*innen als „Sensoren ihrer Umgebung“ eingeladen werden und Daten über Phänomene, denen sie physisch nahestehen, in einem *Crowdsourcing*-Ansatz zusammentragen. Ein Beispiel für die Sammlung von wichtigen Informationen durch Bürger\*innen ist in Großbritannien das bereits oben beschriebene *FixMyStreet.com*. Auf Basis der Technologie eines privaten Anbieters haben viele Kommunen in Brandenburg mit der App und Plattform Maerker einen ähnlichen Dienst aufgesetzt. Die Kommunen profitieren von der Übersicht und Sammlung von Problemstellen und vermeiden unnötige Anrufe, weil Bürger\*innen sehen können, wenn ein Straßenschaden bereits gemeldet ist. Gleichzeitig üben die Dokumentation des Meldezeitpunkts und der Rückmeldungen durch zuständige Behörden einen gewissen Druck auf die Verwaltung aus, das Problem zügig zu lösen.

**Partizipative offene Daten:** Hier werden offene Daten reziprok, d. h. sowohl durch Verwaltungen als auch zivilgesellschaftliche Akteure erstellt und genutzt. Nach der Bereitstellung von Daten können zusätzliche Daten angefordert und durch bürgergenerierte Daten ergänzt werden, die die Erbringung von Dienstleistungen unterstützen und einen neuen Kanal für Diskussionen über die Politik eröffnen. Dies umfasst die laufende gemeinsame Erstellung von Rohdaten zwischen Verwaltungen und Behörden sowie die gemeinsame Produktion von Dienstleistungen. Ein bemerkenswertes Beispiel für *Civic Tech* war der *Promise Tracker* von São Paulo, bereitgestellt vom Center for Civic Media am MIT. Bürger\*innen der Stadt hatten für die Dauer des Projektes die Möglichkeit, öffentlich sichtbar die Wahlkampfversprechen des Bürgermeisters Haddad zu überwachen und dabei die demokratischen Ideale – Transparenz und Verantwortlichkeit – praktisch zu erproben.

Als Leitbild kann *Civic Tech* alle diese Interaktionsmodelle umfassen. Jedes Modell beinhaltet Chancen und Risiken, wie wir im Folgenden genauer erläutern.

---

## 4 Umsetzungsstand und Diskussion

In Deutschland ist *Civic Tech* vor allem durch die *Open Knowledge Foundation Deutschland* vertreten, die die bekanntesten und meistgenutzten *Civic-Tech*-Anwendungen bereitstellt. Neben dem o. g. *FragDenStaat.de* gehören dazu u. a. *OffenesParlament.de* oder *OffenerHaushalt.de*. Darüber hinaus gibt es eine Vielzahl lokaler Initiativen wie *Frankfurt-Gestalten.de* oder *Muenchen-Transparent.de*. Im internationalen Vergleich hinkt Deutschland insgesamt sowohl bei der Informationsfreiheit als auch bei der Bereitstellung von offenen Daten hinterher (*Open Knowledge 2017*). Dies zu ändern und *Civic Tech* als Leitbild der Verwaltungsdigitalisierung stärker in den Fokus zu rücken, birgt sowohl Risiken als auch Chancen, die man gut anhand der oben beschriebenen Interaktionsmodelle veranschaulichen kann.

Die Modelle *Data Publishing* und *Code-Austausch* sind durch die Forderung nach Transparenz auf der Grundlage der Informationsfreiheit und der Bereitstellung von Ressourcen für die wirtschaftliche Entwicklung motiviert. Das dritte Modell, *Civic Issue Tracker*, ist in der Sorge um ein besseres Verhältnis der Regierung zu ihren Bürger\*innen begründet, während das vierte Modell, Partizipative Offene Daten, eine grundlegende Veränderung der Rolle von Verwaltung zeigt und eine gewisse Flexibilität erfordert, die bisher kaum zu finden ist. Ein Grund hierfür dürfte auch sein, dass dieses Modell den von *Civic-Tech*-Organisationen geforderten Kulturwandel am stärksten umsetzt. Sieber und Johnson (2015) unterstützen dieses Modell ausdrücklich, da die ersten beiden Modelle das Risiko bergen, dass Verwaltungen ihre Aufgaben ‚outsourcen‘. Kritiker\*innen haben in diesem Zusammenhang die Mehrdeutigkeit von *Civic Tech* hervorgehoben, durch die die Möglichkeit besteht, unter diesem Label eine neoliberalen Politik durchzusetzen, bei der die Verwaltungen lediglich als Datenlieferanten fungieren und die Tätigkeiten der Verwaltung an private Dienstleister ausgelagert werden.

Aus der Sicht von Sieber und Johnson (2015) ist das Modell der Partizipativen Offenen Daten eine notwendige Reaktion auf die laufenden Veränderungen der

digitalen Welt und im Einklang mit den Prinzipien der *Open Government Partnership*. Dabei handelt es sich um einen informellen Zusammenschluss verschiedener Länder und der Zivilgesellschaft, um durch konkrete Maßnahmen Inklusion, Verantwortung und Responsivität in Regierung und Verwaltung zu stärken. Aber auch dieses Modell ist nicht ohne Risiken und steht im Widerspruch zu etablierten Strukturen der repräsentativen Demokratie und der Rechtsstaatlichkeit. Wenn Bürger\*innen als Mitgestalter\*innen eingeladen werden, erwarten sie, dass Verwaltungen auf ihre Vorschläge und Beiträge eingehen. Es ist jedoch offen, wie man mit widersprüchlichen Forderungen umgeht und stillen Mehrheiten eine Stimme gibt. Diejenigen, die sich als Mitgestalter\*innen engagieren, haben kein Mandat von ihren Mitbürger\*innen, sondern können ihre individuellen Interessen verfolgen. Ferner sind auch die Bestimmungen des Haushalts- und Vergaberechts einzuhalten.

Hinzu kommt, dass *Civic-Tech*-Anwendungen bestehende Ungleichheiten reproduzieren und eventuell sogar verstärken können. Zum Beispiel werden Issue Tracker in den Stadtteilen, in denen Menschen mit höherem sozioökonomischem Status leben, häufiger genutzt. Studien haben gezeigt, dass nach der Einführung von Issue Trackern diese Stadtteile eher von den Verwaltungen beachtet werden. Die Britische *Civic-Tech*-Organisation *mySociety* hat in einer Studie über die Nutzer\*innen ihrer Anwendungen festgestellt, dass die meisten Anwender\*innen aus Großbritannien über 56 Jahre alt, männlich, weiß, im Schnitt höher gebildet und größtenteils vollbeschäftigt sind (Rumbul 2015).

Gleichzeitig birgt *Civic Tech* aber auch Chancen für eine Erneuerung des Verhältnisses zwischen Bürger\*innen und Verwaltung. Die oben genannten Risiken sind keine zwangsläufige Folge von *Civic Tech*, sondern eine Frage der Ausgestaltung. Obwohl jedes der oben beschriebenen Modelle Risiken birgt, kann eine gewisse Experimentierfreudigkeit auf Verwaltungsseite helfen, den Bedürfnissen von Bürger\*innen besser gerecht zu werden und kooperativ Lösungen für Probleme zu finden. Statt eines *Outsourcings* kann *Civic Tech* dann auch eine Stärkung der Verwaltung und des öffentlichen Sektors zur Folge haben.

Allerdings kann es auf unterschiedlichen Wegen zu experimentierfreudigen, neuartigen Lösungen kommen. Wenn man zukünftige Handlungsmöglichkeiten generell zu zwei Handlungsalternativen verdichten wollte, könnte man zwischen Kooperation und Konkurrenz unterscheiden. Diese Handlungsalternativen stehen sowohl der Verwaltung als auch der Zivilgesellschaft offen – die Verortung zwischen den beiden Polen spielt aber für die künftige Entwicklung eine große Rolle. Das Kooperationsverhältnis basiert auf gegenseitiger Öffnung, insbesondere der Verwaltung. Diese Öffnung kann technisch, organisatorisch und verfahrensmäßig gefördert werden. In jeder Form macht die Verwaltung ihre Daten und ihr Handeln transparent. Eine technische Öffnung kann erfolgen, wenn entsprechende Schnittstellen geschaffen werden, die im Falle von bestimmten IT-Systemen die Integration von Anwendungen erlauben. So wurden etwa Schnittstellen für verschiedene Datenbanken für Inhalte des Parlaments des Vereinigten Königreichs geöffnet, sodass Initiativen mit den Daten Zusatzdienste entwickeln konnten. Organisatorisch kann die Öffnung insbesondere dann gelingen, wenn im Rahmen von Regierung und Verwaltung Zuständigkeiten für die Zusammenarbeit mit der Zivilgesellschaft geschaffen wer-

den. Dies geschah in Deutschland nach dem Beitritt zur *Open Government Partnership*, wo diese Zuständigkeiten im Innenministerium geschaffen wurden, die in der 19. Legislaturperiode ins Kanzleramt übergangen sind. Verfahrensmäßig öffnet sich die Verwaltung, wenn Prozesse zum Austausch mit der Zivilgesellschaft aufgesetzt werden. Eine größere Offenheit kann aber auch in konkrete Verfahren einbezogen werden, etwa bei der Aufstellung von Plänen oder bei sogenannten frühen Öffentlichkeitsbeteiligungen (d. h. nicht-förmlichen Verfahren, in dem Bürger\*Innen frühzeitig in die Planung von Großprojekten einbezogen werden).

Im Falle der Zivilgesellschaft kommt es besonders auf das Verständnis ihrer Rolle an. *Civic-Tech*-Initiativen können auf eine enge Zusammenarbeit untereinander zu bestimmten Themen ausgerichtet sein. Sie können sich aber auch stärker als Konkurrenten verstehen, die die Verwaltung mit eigenen Anwendungen unter Druck setzen. Der *Chatbot DoNotPay*, der von einem jungen Studierenden programmiert wurde, kann als Beispiel angeführt werden. Ursprünglich wollte er die Verwaltungen in New York und London unter Druck setzen, weil sie oft unberechtigte Parkbußen gegen Bürger\*innen verhängten. Später arbeitete er aber mit verschiedenen lokalen Verwaltungen zusammen und entwickelte unter anderem einen Service für Bürger\*innen, die obdachlos geworden waren und Leistungen beantragen wollten. In anderen Konstellationen geht es mehr um Beaufsichtigung und Monitoring der Verwaltung. Sowohl Kooperationen als auch Konkurrenz können dementsprechend die Experimentierfreudigkeit befördern.

---

## 5 Fazit: Künftige Entwicklung

Eine stärkere Verankerung von *Civic Tech* im Sinne größerer Bürgerbeteiligung, Nutzerorientierung und damit einhergehend einem Kulturwandel, der den öffentlichen Sektor stärkt, kann nur im Zusammenspiel von Zivilgesellschaft, Wirtschaft und Verwaltung geschehen. Die Frage nach den Möglichkeiten von Einbindung und Transparenz stellt sich insbesondere in Zeiten von wachsender Politikverdrossenheit und aufkeimendem Populismus. In diesem Sinne ist *Civic Tech* als ein Leitbild der Verwaltungsdigitalisierung eine Möglichkeit, um Integration, Partizipation und Zusammenhalt zu stärken. Für den Fall, dass Staat und Gesellschaft sich stärker gegenseitig öffnen, wird das grundlegende Änderungen nach sich ziehen. Denn *Civic Tech* hat einen anderen normativen Fokus als andere Leitbilder wie New Public Management, schlanker Staat oder aktivierender Staat: Bürger\*innen stehen im Mittelpunkt der Aufmerksamkeit. Ferner geht *Civic Tech* von einer offenen Verwaltung aus, die einen partnerschaftlichen Ansatz verfolgt und mit der Zivilgesellschaft stärker auf Augenhöhe verhandelt. Außerdem würde *Civic Tech* einen starken normativen Rahmen für den staatlichen Technologieeinsatz bedeuten.

Ob es aber in den deutschsprachigen Ländern zu einer solchen Entwicklung kommen wird, lässt sich nicht sicher sagen. Eine große Herausforderung bei *Civic-Tech*-Anwendungen, die von *Non-profit*-Organisationen entwickelt werden, ist die Nachhaltigkeit, insbesondere im Hinblick auf Aktualisierung von Daten, Daten-Schnittstellen sowie die Weiterentwicklung. Hier fehlt es Initiativen oft an Stetigkeit

und Mitteln, um im Wandel der Zeit zu überstehen. Lösungsstrategien waren bisher, die Anwendung in die Obhut der Verwaltung zu geben, die Initiativen stetig aus öffentlichen Mitteln zu fördern oder die Anwendung zumindest teilweise mit einem Geschäftsmodell zu unterlegen.

Auch die Art und Weise, wie *Civic Tech* als Konzept und *modus operandi* stärkeren Anklang findet, hängt stark von den handelnden Akteur\*innen ab. Generell ist es jedoch wünschenswert, wenn die Verwaltung *Civic Tech* nicht prinzipiell ablehnend gegenübersteht, sondern auf Kooperation setzt und die Chancen für eine Stärkung von Zivilgesellschaft und öffentlicher Verwaltung nutzt.

---

## Literatur

- Cantijoch, Marta, Silvia Galandini, und Rachel Gibson. 2016. „It's not about me, It's about my community“. A mixed-method study of civic websites and community efficacy. *New Media & Society* 18(9): 1896–1915. <https://doi.org/10.1177/1461444815616225>.
- Open Knowledge. 2014. *What is Open?* <https://okfn.org/opendata/>. Zugegriffen am 31.10.2019.
- Open Knowledge. 2017. *Global Open Data Index 2016/2017*. <https://index.okfn.org/>. Zugegriffen am 31.10.2019.
- Rumbul, Rebecca. 2015. Who benefits from civic technology? *mySociety Research*. <https://www.mysociety.org/research/who-benefits-from-civic-technology/>. Zugegriffen am 31.10.2019.
- Sieber, Renee E., und Peter A. Johnson. 2015. Civic open data at a crossroads. Dominant models and current challenges. *Government Information Quarterly* 32(3): 308–315. <https://doi.org/10.1016/j.giq.2015.05.003>.
- Theocharis, Yannis. 2015. The conceptualization of digitally networked participation. *Social Media + Society* 1(2): 1–14. <https://doi.org/10.1177/2056305115610140>.
- Yu, Harlan, und David G. Robinson. 2012. The new ambiguity of ‚Open government‘. In *59 UCLA L. Rev. Disc.* 178 (2012). <https://doi.org/10.2139/ssrn.2012489>.



---

# Co-Creation von digitalen öffentlichen Dienstleistungen

Juliane Jarke und Herbert Kubicek

## Inhalt

1 Klärung der Begriffe .....	348
2 Konzeptionelle Elemente .....	350
3 Anwendungen und Umsetzungsstand .....	355
4 Zukunftsperspektiven: .....	357
Literatur .....	358

---

## Zusammenfassung

Die Beteiligung zukünftiger Nutzer\*innen an der Entwicklung von digitalen Informationssystemen ist in Organisationen nicht neu, aber im Rahmen von *E-Government*-Diensten noch selten. Die für *E-Government* zuständigen Minister\*innen der EU Mitgliedstaaten sehen in einer stärkeren Beteiligung von Bürger\*innen an der Entwicklung digitaler Dienste einen entscheidenden Faktor, um die bisher geringe Nutzung zu überwinden. Bereits 2009 wurde in einem *Benchmark Report* ein Modell der Reifegrade der Entwicklung von *E-Government*-Diensten vorgestellt (European Commission 2009): Auf die Stufe einer Orientierung an den Bedürfnissen zukünftiger Nutzer\*innen als verwaltungsgesteuerte Nutzerbeteiligung („government-driven“) folgt als der

---

J. Jarke (✉)

ifib: Institut für Informationsmanagement Bremen GmbH, Universität Bremen, Bremen, Deutschland

E-Mail: [jjarke@ifib.de](mailto:jjarke@ifib.de)

H. Kubicek

ifib: Institut für Informationsmanagement Bremen GmbH, Universität Bremen, Bremen, Deutschland

E-Mail: [kubicek@ifib.de](mailto:kubicek@ifib.de)

höchste Reifegrad eine nutzer-gesteuerte Nutzerbeteiligung („user-driven“). Die Europäische Kommission verwendet in ihrem Forschungs- und Innovationsprogramm *Horizon 2020* für diese Stufe den Begriff „Co-Creation“. Er kommt in mehr als 70 Ausschreibungstexten des EU *Horizon 2020* Forschungsförderprogramms vor, wird jedoch meistens nicht genauer definiert. Es ist nicht klar, ob und wie sich Co-Creation von Begriffen wie Kooperation im Rahmen von „Open Government“, von der „kollaborativen Verwaltung“ oder von „Co-Produktion“ und „Co-Design“ unterscheidet. Der Artikel versucht, diese Frage durch eine begriffliche Einordnung, die Herausarbeitung zentraler Elemente und eine Bestimmung geeigneter Anwendungsbereiche zu beantworten.

---

### Schlüsselwörter

Co-Creation · E-Government · Open Government · Co-Produktion · Partizipation · Co-Design

---

## 1 Klärung der Begriffe

### 1.1 Kooperation und Zusammenarbeit

In dem auf US Präsident Barack Obama zurückgeführten Konzept des „Open Government“ ist Kooperation (oder „Collaboration“) neben Transparenz und Partizipation eine der drei tragenden Säulen, die auf offenen Verwaltungsdaten aufbauen und in deutscher Übersetzung zu einem offenen Regierungs- und Verwaltungshandeln führen sollen (Wewer 2013). Dabei wird nicht näher definiert, was unter „Collaboration“ zu verstehen ist bzw. wie diese ausgestaltet werden kann. In der Begriffsverwendung gibt es zumindest zwei unterschiedliche Schwerpunkte. Zum einen wird anknüpfend an die Hervorhebung offener Verwaltungsdaten als Fundament ein Fokus auf deren kooperative Nutzung für die Entwicklung von digitalen Diensten insbesondere in Form von Apps gelegt.

Zum anderen geht es um die Zusammenarbeit von Regierung und Verwaltung mit allen Bereichen der Zivilgesellschaft. In der internationalen „Open Government Partnership“ (OGP) haben sich mehr als 90 nationale und regionale Regierungen verpflichtet, offener zu werden und in Zusammenarbeit mit zivilgesellschaftlichen Organisationen alle zwei Jahre einen nationalen Aktionsplan (NAP) mit Projekten zur Umsetzung von *Open Government* zu entwickeln. In Deutschland wurde 2016 der erste NAP in diesem Sinne kooperativ entwickelt. 14 von 15 darin enthaltenen Maßnahmen beziehen sich auf die Öffnung von Verwaltungsdaten, eine auf Partizipation im Umweltbereich. Die Zentralstelle der internationalen OGP hat unter dem Titel: „OGP Partizipation and Co-creation Toolkit“ (Open Government Partnership 2018) einen Leitfaden für die kollaborative Entwicklung von NAPs veröffentlicht, der viele Beispiele für Kooperationsprojekte aus allen Teilen der Welt als Vorbilder beinhaltet.

## 1.2 Co-Produktion

Die Zusammenarbeit der Verwaltung mit zivilgesellschaftlichen Organisationen ist nichts Neues. Dies gilt sowohl für die Planung von Vorhaben, z. B. mit Runden Tischen, Planungszellen, Bürgergutachten u. ä., als auch für die Erbringung von Dienstleistungen. Wie Aichholzer und Strauss (2015) bemerken, umfassen kooperative Formen der Beteiligung alle Phasen der Projekt- und Dienstleistungsplanung, das Design und die Erbringung und betreffen sowohl Bürger\*innen als auch Organisationen wie NGOs oder Unternehmen. Die Beteiligung von Bürger\*innen an der Gestaltung und Erbringung öffentlicher Dienstleistungen wird oft als „Co-Produktion“ bezeichnet. Voorberg et al. (2015) stellen in einer umfassenden Literaturanalyse fest, dass die Begriffe Co-Produktion und Co-Creation häufig synonym verwendet werden. Zur Abgrenzung kann man sagen, dass Co-Produktion häufig in Verbindung mit der physischen Welt und Face-to-Face-Dienstleistungen verwendet wird, etwa bei Projekten im Bereich Infrastruktur und Transport, Bildung, Gesundheit und sozialer Daseinsvorsorge, während Co-Creation zumeist auf die Entwicklung und Implementierung von digitalen Dienstleistungen bezogen wird und sich hier mit dem Begriff „Co-Design“ und partizipativer Software- und Systementwicklung überschneidet.

## 1.3 Co-Design und Partizipative Systemgestaltung

Auch die Beteiligung von Nutzer\*innen an der Entwicklung von Informationssystemen hat eine lange Tradition. Seitdem die Verarbeitung von Informationen in den Büros in Wirtschaft und Verwaltung durch Computer unterstützt oder teilautomatisiert wird, kann die Entwicklung dieser Werkzeuge auch auf Softwareentwickler\*innen verlagert werden, die die fachlichen Inhalte der zu unterstützenden Tätigkeiten nicht kennen. So entsteht eine Lücke zwischen dem technischen Wissen professioneller Softwaresystementwickler und dem fachlichen Wissen der nach wie vor verantwortlichen Sachbearbeiter\*innen, die nun Nutzer\*innen genannt werden. Im Sinne der partizipativen Softwaregestaltung soll die so geschaffene Wissensklufl durch die Einbindung zukünftiger Anwender\*innen in das *Software-Design* überbrückt werden, indem diese ihr Wissen über ihre Arbeitsprozesse in die Anforderungsanalyse einbringen. Obwohl die Beteiligung von Nutzer\*innen in der Regel mit höheren Kosten verbunden ist, besteht Einigkeit darüber, dass das Ergebnis einer solchen Beteiligung zu fachlich besseren Lösungen und zu einer höheren Nutzerzufriedenheit und Akzeptanz führt (Bratteteig und Wagner 2016).

Nachdem partizipative Designprozesse schon lange innerhalb von Unternehmen durchgeführt werden, kommen mit der Verbreitung digitaler Kunden- und Bürgerdienste im *E-Commerce* und *E-Government* Nutzer\*innen außerhalb von Unternehmen und Verwaltungen hinzu. Dies hat zu neuen Herausforderungen für die Zusammenarbeit zwischen Softwareentwickler\*innen und potenziellen Nutzer\*innen geführt, die nicht Mitglied einer bestimmten Organisation und daher schwieriger einzubinden sind. Gleichwohl ist das Verständnis des zukünftigen Nutzungskontext-

tes und der Nutzungspraktiken für die Systementwickler\*innen unverzichtbar, weil die externen Nutzer\*innen zumindest bisher einfach auf die Verwendung der digitalen Angebote verzichten und die Dienstleistungen nach wie vor papiergebunden oder im *Face-to-Face*-Kontakt erledigen.

Aus Sicht der Verwaltung als Anbieter eines Dienstes und/oder eine beauftragten Softwareentwicklers ist keineswegs klar, welche potenziellen Nutzer\*innen zur Beteiligung eingeladen werden sollen. Und für die adressierten Bürger\*innen ist keineswegs klar, ob sich eine solche Beteiligung lohnt, wenn sie die meisten Dienste der Verwaltung nur selten nutzen, die Teilnahme jedoch Zeit erfordert und eine Zusammenarbeit mit Menschen mit sich bringt, die sich in der Regel nicht kennen und vielleicht auch nicht verstehen. Hinzu kommt, dass Softwaregestaltung ein Themengebiet ist, mit dem die meisten Menschen nicht vertraut sind und auch kaum Interesse haben es zu lernen. Viele haben schon Schwierigkeiten digitale Dienste kompetent zu nutzen. Insofern ist Co-Design und Co-Creation zwar insbesondere ein von der EU-Kommission und den *E-Government*-Minister\*innen favorisierter und beworbener Ansatz, um die Nutzung von digitalen Diensten zu fördern, indem diese selbst nutzergerechter werden. Ob und wie dies gelingt, ist jedoch noch offen. Von daher ist es angemessen, dass Co-Creation zurzeit vor allem in geförderten Forschungs- und Entwicklungsprojekten in verschiedenen Variationen erprobt und evaluiert wird.

---

## 2 Konzeptionelle Elemente

Aus eigenen Erfahrungen in einem EU-Forschungs- und Entwicklungsprojekt zu Co-Creation-Ansätzen zur Entwicklung öffentlicher digitaler Dienstleistungen für ältere Menschen (*MobileAge*) sowie einer Analyse von Berichten aus anderen Co-Creation-Projekten und verschiedenen Modellen in der Literatur können einige konzeptionelle Elemente oder Bausteine identifiziert werden. Zu diesen Elementen gehören

- die Bestimmung geeigneter Arten digitaler öffentlicher Dienste, insbesondere in Abhängigkeit von der Interaktionsform zwischen Dienstleistungserbringer und Nutzenden und der Art der Erbringer bzw. Anbieter,
- eine Identifizierung relevanter Akteure oder *Stakeholder* und eine Systematisierung der verschiedenen Rollen, die insbesondere die mitwirkenden Bürger\*innen übernehmen können,
- eine Systematisierung der Arten von Teilprozessen, Phasen und Aktivitäten,
- Beispiele für innovative Methoden.

### 2.1 Bestimmung geeigneter digitaler öffentlicher Dienste

Zwar wird Co-Creation prominent von den *E-Government*-Minister\*innen in der EU und der EU-Kommission beworben, man darf jedoch zweifeln, ob alle *E-*

*Government*-Dienste dazu gleichermaßen geeignet sind. *E-Government*-Dienste werden nach der Art der Interaktion unterschieden in Informationsdienste, Kommunikationsdienste und Transaktionsdienste. Letztere können nach Art der Integration noch weiter in horizontal und vertikal integrierte Dienste unterschieden werden. Jede dieser Arten zeichnet sich durch unterschiedliche technische, organisationale und rechtliche Anforderungen aus. Eine horizontale Integration wird erreicht, wenn verschiedene Dienste integriert werden, die in einer bestimmten Lebenssituation regelmäßig gemeinsam genutzt werden: Ziehen beispielsweise Menschen von einem Ort zum anderen, so müssen sie typischerweise bei mehreren Stellen gleichzeitig Adressänderungen vornehmen. Bei der horizontalen Integration müssen sie die neuen Daten nur einmal eingeben. Vertikal integrierte Dienste erfassen automatisch Daten aus zentralen Registern und entlasten die Nutzer\*innen von der Eingabe dieser Daten. Beide Wege erfordern Interoperabilität zwischen den verschiedenen Diensten. Wenn sie von verschiedenen Verwaltungseinheiten durchgeführt werden, besteht ein Bedarf an interorganisatorischer Koordination. Es ist schwer vorstellbar, dass einzelne Bürger\*innen bei der (Weiter-)Entwicklung einer solchen Dienstleistungsintegration eine Hilfe sein können, da es sich um Entscheidungen über jeweils innerbetriebliche Prozesse und Zuständigkeiten handelt. Im Gegensatz dazu scheinen Informationsdienste zwischen Dienstleistungserbringern und potenziellen Nutzer\*innen besser für die Co-Creation geeignet zu sein. Hier wissen Softwareentwickler\*innen und oft auch die Verwaltung nicht, welche Informationen welche Bürger\*innen zu einem bestimmten Themengebiet benötigen. Co-Creation kann diese Wissenskluft überbrücken und zu wirklich nutzerrelevanten Informationsdiensten führen.

Eine weitere Unterscheidung öffentlicher Dienste bezieht sich auf die Art der Institution der Dienstleistungserbringer. Im Zusammenhang mit *E-Government* liegt der Schwerpunkt bei Verwaltungseinheiten auf nationaler, regionaler oder kommunaler Ebene. Viele der von diesen Verwaltungen erbrachten Dienstleistungen sind gesetzlich geregelt; ihre Entwicklung und Gestaltung wird durch die Vergabeverordnung, die Mitbestimmung der Arbeitnehmervertreter und Zugänglichkeitsrichtlinien (*accessibility*) u. a. m. geregelt. Der Begriff der öffentlichen Services gilt insbesondere im *Open-Government-Kontext* jedoch auch für Dienstleistungen von öffentlichem Interesse, die in Kooperation mit oder von Sozialeinrichtungen oder anderen Organisationen der Zivilgesellschaft erbracht werden. Beispiele für solche Dienstleistungen sind Vorschulen, Begegnungsstätten, Beratungsdienste, die teilweise unter staatlicher Lizenz stehen und auf staatlicher Finanzierung beruhen. In den meisten Fällen haben solche Dienstleister mehr Autonomie über die von ihnen bereitgestellten Informationsdienste und können daher offener für deren Co-Creation sein.

## 2.2 Relevante Co-Creatoren und ihre Rollen

Bisher sind die Entwickler\*innen von öffentlichen digitalen Dienstleistungen eigene oder beauftragte IT-Fachleute der Verwaltungen. Die *Open-Data*-Bewegung pro-

giert, dass diese entweder mit *Civic Hackern* bzw. *Civic Tech*-Aktivisten kooperieren oder diesen die Entwicklung von sogenannten *Civic Apps* überlassen, die sie anschließend in ihre Portale integrieren. Dies ist in Einzelfällen gelungen, wenn die Verwaltung einen regelmäßigen und intensiven Austausch mit der *Community* führt, wie es z. B. in Wien der Fall ist. Der Regelfall dürfte dies jedoch nicht werden (siehe auch Lee et al. 2015). Die beabsichtigte Einbindung eines co-creierten Dienstes in ein umfassenderes *E-Government*-Portal erfordert vielfältige technische Abstimmungen. Deshalb ist es sinnvoll, wenn im Co-Creation-Prozess Entwickler\*innen mitwirken, die diese Infrastrukturen kennen. Gleichzeitig stellt ein Co-Creation-Prozess mit Teilnehmenden, die vor allem ihr inhaltliches Wissen und ihre Bedürfnisse einbringen, hohe Anforderungen an die Entwickler\*innen: Im Entwicklungsprozess müssen sie sich auf die wandelnden Anforderungen und Ideen im Aushandlungsprozess der Teilnehmenden einlassen. Dies kann den zeitlichen und finanziellen Rahmen eines solchen Prozesses auch überschreiten und muss moderiert werden.

Daher braucht ein Co-Creation-Prozess Moderator\*innen. Sie unterstützen die Co-Creation-Aktivitäten durch z. B. *Workshops*, Fokusgruppen, Interviews und beeinflussen bewusst oder unbewusst den Verlauf und das Ergebnis. Wenn Interessenkonflikte zwischen Behörden und bestimmten Teilnehmergruppen zu erwarten sind, ist es sinnvoll eine neutrale Stelle mit dieser Aufgabe zu betrauen. Bei großem Konfliktpotenzial, auch zwischen verschiedenen *Stakeholdern*, kann es sogar sinnvoll sein, die Auswahl auf einer Stakeholderkonferenz im Einvernehmen zu treffen.

Außerhalb des Kernbereichs hoheitlicher und streng geregelter Verwaltungsdienste kann es sinnvoll sein, unterschiedliche Dienstleistungsanbieter als Kooperationspartner einzubeziehen. Da sich die meisten digitalen Dienste auf bestehende *Face-to-Face*-Angebote beziehen, können deren Erbringer ihre Erfahrungen und eigenen Unterstützungsbedarf einbringen und später die Verbreitung dieser Informationen und den Zugang der verschiedenen Zielgruppen zu diesem Informationsangebot unterstützen. Ein zu entwickelnder Dienst kann somit auch die Dienstleistungsanbieter selbst als Zielgruppe und zukünftige Nutzer haben.

Daneben gibt es noch andere Organisationen und Einzelpersonen, die für die Bereitstellung fehlender Informationen, finanzieller Ressourcen oder die Unterstützung der Nutzung und Verbreitung des Dienstes eingebunden werden und zu gewinnen sind. Vor allem zur Bekanntmachung und Unterstützung bei der Nutzung in der Zielgruppe ist eine solche Kooperation mit Multiplikatoren zu empfehlen. Die Einbettung einer *App* in einen Service muss nicht nur auf der Angebotsseite erfolgen, sondern auch auf der Nutzerseite. Dies gilt vor allem, wenn es sich um Dienste für Nutzer\*innen mit einem gewissen Unterstützungsbedarf handelt, z. B. für bildungsferne Jugendliche, Arbeitssuchende, Migrant\*innen, Menschen mit Behinderungen und ältere Menschen, also für alle, für die es heute auf der lokalen Ebene kommunale und/oder ehrenamtliche Betreuung und Unterstützung gibt. Für diese sind der Bedarf und das Potenzial co-creierter Dienste besonders groß. Ihre Wirkung können die

entwickelten Services aber nur entfalten, wenn sie auch in diese Betreuungsarbeit integriert werden.

Schließlich hängt der Erfolg von partizipativen Projekten von der Einbeziehung geeigneter und repräsentativer Nutzer\*innen ab. Die Rolle der Bürger\*innen als zukünftige Nutzer\*innen eines digitalen öffentlichen Dienstes kann sich von anderen Formen der Bürgerbeteiligung, aber auch von anderen Formen der partizipativen Softwaregestaltung unterscheiden, da sich ihre Beteiligung über die Planung, Gestaltung und Erbringung des Services erstreckt (Gomillion 2013):

- (1) Bei Co-Creation bringen Nutzer\*innen nicht nur ihre Bedürfnisse und Anforderungen ein und geben *Feedback*, sondern werden auch in die Programmier- und Designaktivitäten einbezogen.
- (2) Nutzer\*innen definieren oder beeinflussen die Architektur des Systems, nicht nur einzelne Funktionen und Schnittstellen.
- (3) Die Nutzer\*innen übernehmen die Verantwortung für die entwickelten Dienste und Systeme und können diese (oder bestimmte Aspekte davon) aufrechterhalten.

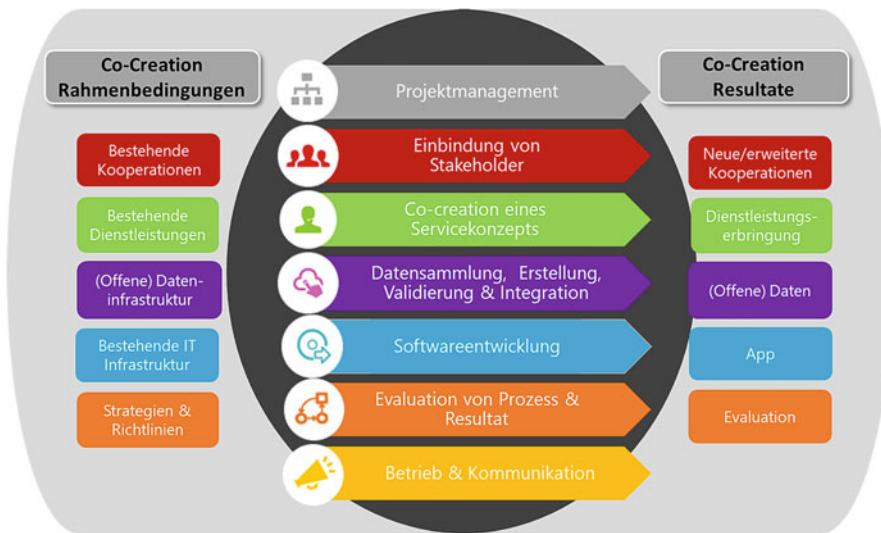
Dabei können die Teilnehmer\*innen verschiedene Rollen in einem Co-Creation-Prozess übernehmen. Diese können entlang der Phasen Planung, Umsetzung, Betrieb definiert werden: Bürger\*innen als Initiator, als Mitgestalter oder als Umsetzer (z. B. Voorberg et al. 2015), oder in Bezug auf spezifische Aufgaben wie Erkundung, Ideenfindung, Gestaltung, Gestaltung, Verbreitung: Bei der Planung eines Co-Creation-Prozesses können Bürger\*innen als Initiatoren oder Erkunder einbezogen werden, während sie in der nachfolgenden Phase als Ideengeber und Mitgestalter beteiligt sind. Schließlich können Bürger\*innen als Implementierer oder Multiplikatoren von Diensten einbezogen werden (z. B. Nambisan und Nambisan 2013). Vor allem bei der Entwicklung von Services auf Basis von offenen Daten können sie auch als Datenkuratoren arbeiten und Daten erheben und/oder validieren.

Bei *E-Government*-Diensten, die letztlich von einer Behörde angeboten und verantwortet werden sollen, liegt es nahe, dass diese auch den Co-Creation-Prozess initiiert, steuert und am Ende das Ergebnis übernimmt. Es ist aber auch möglich, dass eine zivilgesellschaftliche Organisation oder eine wissenschaftliche Einrichtung einen solchen Prozess startet, in möglichst früher Abstimmung mit der zuständigen Behörde den Prozess koordiniert und am Ende übergibt.

## 2.3 Teilprozesse, Phasen und Aktivitäten

Darüber, wie ein Co-Creation-Prozess in Phasen unterteilt wird, gibt es unterschiedliche Vorschläge. Im oben bereits erwähnten Projekt *Mobile Age* wurde ein Vorgehensmodell entwickelt, das zunächst vier inhaltliche Teilprozesse unterscheidet, die miteinander verwoben sind und sich über die gesamte Projektdauer erstrecken:

- (1) Einbindung von *Stakeholdern*;
- (2) Co-Creation eines Servicekonzepts;



**Abb. 1** Kernprozesse von Co-Creation in Verbindung mit den Rahmenbedingungen und Resultaten (eigene Darstellung)

(3) Sammlung, Validierung und Integration von (offenen) Verwaltungsdaten und (4) partizipative Softwareentwicklung. Diese inhaltlichen Prozesse sind gerahmt von Prozessen des Projektmanagements, der Evaluation und der Kommunikation. Abb. 1 veranschaulicht die sieben Teilprozesse (in der Mitte des Bildes). Diese Prozesse erfolgen eingebettet in den Anwendungskontext und berücksichtigen etwa bestehende Kooperationen zwischen Akteuren, bestehende IT- und Dateninfrastrukturen und bestehende öffentliche Dienstleistungen und Services (linke Seite der Abbildung: Co-Creation-Rahmenbedingungen). Das Resultat eines Co-Creation-Prozesses ist dann schließlich ein digitaler öffentlicher Service, der sich als soziotechnische Innovation aus *Software* zumeist in Form einer *App*, (offenen) Daten und einem institutionellen Arrangement für den nachhaltigen Betrieb zusammensetzt (rechte Seite der Abbildung: Co-Creation Resultate).

Jeder der Teilprozesse kann in verschiedene Phasen untergliedert werden. Wie bei der Unterscheidung der Rollen der Bürger\*innen ausgeführt wurde, beginnt ein Co-Creation-Prozess mit der Klärung eines Bedarfs oder Problems und der anschließenden gemeinsamen Suche nach Lösungsmöglichkeiten. Die Phasen oder Schritte der Teilprozessen folgen in den meisten Projekten im Wesentlichen der Idee des „Design Thinking“, welches Design-Projekte in vier Schritte unterteilt:

Problem verstehen: Ausgehend von einem Problemfokus und einer Zielgruppe für den zu entwickelnden Service geht es zunächst darum, das Problem gemeinsam mit den betroffenen Bürger\*innen und anderen relevanten Akteuren zu verstehen. Hierbei werden Möglichkeitsräume geöffnet und ein möglichst breites Verständnis des Problems geschaffen.

Problem definieren: In einem nächsten Schritt geht es darum, das Problem klar zu formulieren und zu definieren. Ein Teil der Co-Creation-Arbeit befasst sich mit der Analyse und den Limitationen existierender Services. Mögliche Funktionalitäten (auch mit Blick auf existierende Services) werden erarbeitet. Gleichzeitig werden mögliche relevante Daten auf ihre Qualität und Konsistenz überprüft.

Am Ende dieses ersten Zyklus steht eine gemeinsame Problemdefinition aller Beteiligten, eine konkrete Definition der Zielgruppe sowie eine „Value Proposition“, die definiert welchen Mehrwert der zu entwickelnde Service gegenüber existierenden Services und mit Blick auf die Problemdefinition haben soll.

Ideen entwickeln: Ausgehend vom gemeinsamen Verständnis für ein Problem bzw. einen Problembereich werden weitere Akteure in den Prozess einbezogen und gemeinsam Ideen für ein grobes Servicekonzept entwickelt. Dies beinhaltet auch die Erstellung und Integration von (offenen) Daten sowie erstes *Prototyping*. Auch in dieser Phase geht es zunächst um die Öffnung der möglichen Umsetzungsoptionen.

Serviceprototyp umsetzen: In einem letzten Schritt wird ein detailliertes Servicekonzept erarbeitet und der Prototyp durch Nutzertests final umgesetzt. Das Servicekonzept beinhaltet auch Strategien für die Einbettung des Service in bestehende Infrastrukturen.

## 2.4 Methoden

Zielführend sind Methoden, die Einblicke in die konkrete Lebenswirklichkeit der Zielgruppe im Zusammenhang mit einem Problemfokus ermöglichen. Dies können zum Beispiel Methoden der Selbstaufschreibung und Reflektion, wie etwa „Cultural Probes“ umfassen. Die Methode stammt ursprünglich aus der Designforschung und ermöglicht Teilnehmer\*innen, ihren Alltag zu dokumentieren und reflektieren (etwa durch Tagebücher, Postkarten, Karten oder Kameras). Designer erlangen so Einblicke in die Lebenswelt(en) ihrer Teilnehmer\*innen und nutzen diese als Inspiration (Jarke und Gerhard 2018). Andere Methoden, die in Co-Creation Projekten zum Einsatz kommen, stammen aus dem Bereich des Co-Design und partizipativen Designs und umfassen *Workshops*, Fokusgruppen, *Prototyping* oder *Data Walks* (Jarke 2013).

---

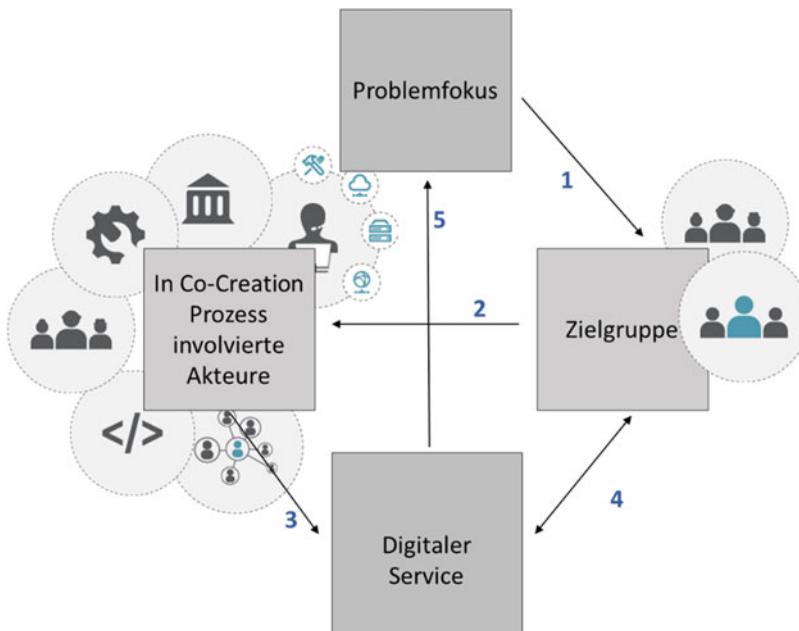
## 3 Anwendungen und Umsetzungsstand

In einem umfassenden Literaturüberblick über die Co-Creation von Dienstleistungen des öffentlichen Sektors haben Voorberg et al. (2015) englischsprachige Zeitschriftenbeiträge und Berichte detailliert analysiert, in denen die Begriffe „co-creation“ oder „co-production“ vorkommen. Diese decken alle öffentlichen Sektoren ab, jedoch mit einer Dominanz im Gesundheitswesen (30 Fälle) und im Bildungswesen (15 Fälle). In 52 % der Beiträge wird überhaupt kein Ziel genannt. 29 % der Fälle wollten mehr Effektivität oder Effizienz, 8 % mehr Kundenzufriedenheit und nur 7 % mehr Bürgerbeteiligung. Die Autoren gehen davon aus, dass in den Fällen, in

denen keine Ziele erwähnt wurden, die Co-Creation selbst explizit das Ziel und die Rechtfertigung war, unabhängig von einem Ergebnis (ebd., S. 1341). Im Abschluss ihres Beitrags schließen Voorberg et al. (2015), dass es nicht klar ist, ob Co-Creation tatsächlich zu den angestrebten Ergebnissen beiträgt. Sie hinterfragen weiterhin, „ob es einen Zusammenhang zwischen mehreren Graden der Bürgerbeteiligung (Co-Implementierung, Co-Design und Co-Initiator) und den Ergebnissen sozialer Innovationen gibt“ (ebd., S. 1348). Das Ergebnis ist, dass in den meisten Studien Co-Creation an sich als Wert verstanden wird.

Noch liegen keine hinreichenden Erfahrungen vor, um die Frage beantworten zu können, ob und unter welchen Bedingungen Co-Creation zu besseren und stärker genutzten digitalen öffentlichen Dienstleistungen führt. Sicher ist nur, dass der Aufwand deutlich höher ist als eine Entwicklung ohne oder mit nur geringer Nutzerbeteiligung und dass die einzelnen Elemente in jedem Fall in Abhängigkeit vom Gegenstand und der Zielgruppe sorgfältig ausgewählt, angepasst und kombiniert werden müssen. Inzwischen gibt es zwar einige Leitfäden, die jedoch ein zentrales Problem nicht lösen können, das man als das doppelte Stellvertreterproblem bezeichnen kann und das anhand von Abb. 2 verdeutlicht werden soll.

Ein Co-Creation-Prozess beginnt mit der Definition eines Problems, das durch die Bereitstellung eines digitalen Dienstes gelöst werden soll. Dieser soll eine bestimmte Zielgruppe ansprechen (Pfeil 1 in Abb. 2). Die erste Herausforderung besteht darin, eine geeignete Gruppe von Mitgestalter\*innen zu engagieren und andere Interessen-



**Abb. 2** Herausforderungen von Co-Creation-Prozessen (eigene Darstellung)

vertreter\*innen, die diese Zielgruppe vertreten, sowie diejenigen, die den Dienst anbieten und aufrechterhalten werden, einzubeziehen (Pfeil 2). Anschließend muss ein Co-Creation-Prozess inhaltlich, zeitlich und im Hinblick auf die eingesetzten Methoden so geplant werden, dass ein digitaler Service geschaffen wird, der das Ausgangsproblem löst (Pfeil 3). Dabei wird zunächst eine *App* entwickelt, die dann in einen dauerhaft angebotenen Service einer Verwaltung oder eines anderen Trägers eingebettet werden muss. Hier enden die meisten dokumentierten Co-Creation-Prozesse. Außerdem stellt sich die Herausforderung, dass die Zielgruppe von der Existenz dieses Angebots erfährt, motiviert wird und praktisch in der Lage ist, den Dienst zu nutzen. Erst dann zeigt sich, ob und wie der Dienst zur Lösung des Problemfokus beiträgt (Pfeil 4). Ob und wie der Problemfokus erfüllt wird, muss bewertet und die beabsichtigten und unbeabsichtigten Auswirkungen analysiert werden (Pfeil 5).

Ob und wieweit dieses Ziel erreicht wird und sich der Aufwand für eine Verwaltung als Diensterbringer lohnt, hängt davon ab, ob es zu Beginn gelingt, die ‚richtigen‘ Personen für den Co-Creation-Prozess zu gewinnen und bis zum Ende des Prozesses zu halten. Denn diese agieren in diesem Modell als Stellvertreter\*innen in zweierlei Hinsicht. Zum einen müssen sie über das inhaltliche und technische Wissen verfügen, das erforderlich ist, um einen sach- und nutzergerechten Dienst zu entwickeln, also über näher zu bestimmende Kompetenzen verfügen. Zum anderen vertreten sie aber auch die Zielgruppe des Dienstes, die möglicherweise wenig Vorwissen und Technikkompetenz hat, letztlich aber mit ihrem Verhalten darüber entscheidet, ob der Dienst akzeptiert wird und sich der Entwicklungsaufwand gelohnt hat. Das Problem liegt also darin, dass die Co-Creatoren gleichzeitig Produzenten- und Nutzungswissen haben müssen, gleichzeitig Expert\*innen für den Gegenstandsbereich und die Zielgruppe sein müssen.

Grundsätzlich wird dies umso schwieriger, je umfassender und komplexer der Gegenstandsbereich und umso heterogener die Zielgruppe ist. Daher ist zu empfehlen, Co-Creation-Prozesse auf relativ gut definierte Gegenstandsbereiche und homogene Zielgruppen zu konzentrieren. Eine weitere praktische Frage ist, ob es angelsichts der vielfältigen Wissens- und Kompetenzfelder zweckmäßig ist, an der Grundidee einer permanenten Gruppe von Co-Creatoren festzuhalten oder etwa phasenweise neue Mitglieder zu kooperieren und andere ggf. auch zu entlassen. So kommt es am Anfang und am Ende sehr darauf an, die konkreten Alltagsprobleme und -situationen der Zielgruppe zu erkennen, auch ganz unabhängig von einem Technikeinsatz. Bei der Datensammlung und Softwaregestaltung sind technische Kompetenzen jedoch unverzichtbar. Noch gibt es keine hinreichenden Erfahrungen, um diese Frage abschließend zu beantworten. Vielleicht wird das mit Gewissheit nie möglich sein, weil digitale Informationsdienste und ihre Nutzungskontexte insgesamt zu unterschiedlich sind.

---

## 4 Zukunftsperspektiven:

Voorberg et al. (2015) sprechen bei Co-Creation von einem „magischen Begriff“, der als „Eckpfiler für soziale Innovation“ im öffentlichen Sektor verstanden wird (ebd., S. 1346, eigene Übersetzung). Demnach bietet Co-Creation eine Chance,

die Nutzerzentrierung und Nutzerfreundlichkeit bei digitalen, öffentlichen Services zu verbessern und ihre Akzeptanz und Nutzung zu erhöhen. Es gibt jedoch keine Garantie für den Erfolg. Es handelt sich um einen komplexen Multi-Aufgaben- und Multi-Stakeholder-Prozess, der anspruchsvoller ist als die traditionelle Nutzer- und Bürgerbeteiligung. Unsere eigene Forschung zu Erfolgsfaktoren der Bürgerbeteiligung hat drei Erfolgsfaktoren identifiziert: (1) klare Zielsetzung der Beteiligung, (2) ein Problem, das für beide Seiten, Verwaltung und Bürger\*innen, von großer Dringlichkeit ist und (3) ausreichende Ressourcen (Kubicek et al. 2011). Wir sind überzeugt, dass dies auch für Co-Creation-Prozesse gilt. Es ist nicht einfach, diese Anforderungen in Zeiten eines Missverhältnisses zwischen dem vielfältigen Bedarf an Dienstleistungen im öffentlichen Interesse und angespannten öffentlichen Haushalten zu erfüllen. Ein niedriges Budget für Co-Creation, das es nicht ermöglicht, die Ziele und gewünschten Ergebnisse zu erreichen, ist jedoch eine Verschwendug von Ressourcen. Aufgrund der Offenheit und Flexibilität, die jeder Co-Creation-Prozess benötigt, ist die Bereitstellung von Leitlinien und Empfehlungen für einen solchen Prozess eine widersprüchliche und damit herausfordernde Aufgabe. Es gibt eine Reihe von ersten Leitfäden zu Erfahrungen mit Co-Creation (siehe zum Beispiel [www.mobile-age.eu](http://www.mobile-age.eu)). Jeder Prozess ist eine Reise in ein teilweise unbekanntes Gebiet und ein Abenteuer. Wir alle können von Reiseberichten profitieren. Daher ist es wichtig, dass zukünftige Co-Creation-Prozesse dokumentiert, bewertet und die gewonnenen Erkenntnisse veröffentlicht werden, um unser Wissen zu vertiefen.

---

## Literatur

- Aichholzer, Georg, und Stefan Strauß. 2015. Collaborative forms of citizen (e-)Participation. In *Evaluating E-participation. Frameworks, practice, evidence*, Hrsg. Georg Aichholzer, Herbert Kubicek und Lourdes Torres, 109–122. Cham: Springer.
- Bratteteig, Tone, und Ina Wagner. 2016. Unpacking the notion of participation in participatory design. *Computer Supported Cooperative Work (CSCW)* 25(6): 425–475.
- European Commission. 2009. Smarter, Faster, Better eGovernment: 8th Benchmark Measurement. [Prepared by Capgemini, Rand Europe, IDC, Sogeti and DTI]. [http://www.mof.gov.cy/mof/DITS/dits.nsf/All/C1B4301D69B229D7C225781700420412/\\$file/egov\\_benchmark\\_20098th.pdf](http://www.mof.gov.cy/mof/DITS/dits.nsf/All/C1B4301D69B229D7C225781700420412/$file/egov_benchmark_20098th.pdf). Zugegriffen am 09.10.2019.
- Gomillion, David. 2013. *The co-creation of information systems*. Tallahassee: Florida State University. <http://diginole.lib.fsu.edu/islandora/object/fsu%3A183733>. Zugegriffen am 09.10.2019.
- Jarke, Juliane, und Ulrike Gerhard. 2018. Using probes for sharing (tacit) knowing in participatory design. Facilitating perspective making and perspective taking. *i-com Journal of Interactive Media* 17(2): 137–152. <https://doi.org/10.1515/icom-2018-0014>.
- Jarke, Juliane. 2019. Open government for all? Co-creating digital public services for older adults through data walks. *Online Information Review* 43(6): 1003–1020. <https://doi.org/10.1108/OIR-02-2018-0059>.
- Kubicek, Herbert, Barbara Lippa, und Alexander Koop. 2011. *Erfolgreich beteiligt? Nutzen und Erfolgsfaktoren internetgestützter Bürgerbeteiligung. Eine empirische Analyse von 12 Fallbeispielen*. Bielefeld: Bertelsmann Stiftung. [https://www.bertelsmann-stiftung.de/fileadmin/files/BS/Studien/Publikationen/imported/leseprobe/LP\\_978-3-86793-304-9\\_1.pdf](https://www.bertelsmann-stiftung.de/fileadmin/files/BS/Studien/Publikationen/imported/leseprobe/LP_978-3-86793-304-9_1.pdf). Zugegriffen am 09.10.2019.

- Lee, Melissa, Esteve Almirall, und Jonathan Wareham. 2015. Open data and civic apps: First-generation failures, second-generation improvements. *Communications of the ACM* 59(1): 82–89. <https://doi.org/10.1145/2756542>.
- Nambisan, Satish, und Priya Nambisan. 2013. *Engaging citizens in co-creation in public services lessons learned and best practices*. Washington, DC: IBM Center for The Business of Government.
- Open Government Partnership. 2018. Open government partnership participation and co-creation toolkit. [http://live-ogp.pantheonsite.io/sites/default/files/OGP\\_Participation-CoCreation-Tool\\_kit\\_20180509.pdf](http://live-ogp.pantheonsite.io/sites/default/files/OGP_Participation-CoCreation-Tool_kit_20180509.pdf). Zugegriffen am 09.10.2019.
- Voorberg, William H., Victor J. J. M. Bekkers, und Lars G. Tummers. 2015. A systematic review of co-creation and co-production. Embarking on the social innovation journey. *Public Management Review* 17(9): 1333–1357. <https://doi.org/10.1080/14719037.2014.930505>.
- Wewer, Götztrik. 2013. Eine Blaupause für Deutschland? Barack Obama und die kollaborative Verwaltung. *der moderne staat-dms* 6(2): 411–424.



---

# Mobilisierung von Recht durch Legal Technologies

Britta Rehder und Katharina van Elten

## Inhalt

1 Klärung des Begriffs .....	362
2 Theoretische Grundlagen .....	363
3 Praktische Anwendungsfelder .....	365
4 Umsetzungsstand und Auswirkungen .....	368
5 Perspektiven für Staat und Verwaltung .....	368
Literatur .....	370

---

## Zusammenfassung

Die Automatisierung von Rechtsdienstleistungen durch *Legal Technologies* erleichtert die digitale Rechtsmobilisierung. Rechtsdienstleister, die im Zuge der erweiterten technischen Möglichkeiten Massenklagen initiieren, werden zu neuen Akteuren der Interessenvermittlung. Der Rechtsstaat ist zunehmend mit strategischer Prozessführung konfrontiert. Regulierungsversuche stellen darauf ab, aus Effizienzgründen Quasi-Sammelklagen zu ermöglichen. Gleichzeitig wird versucht, den Einfluss kommerzieller Rechtsdienstleister zu begrenzen und stattdessen die Klagebefugnisse von Verbänden zu stärken.

---

## Schlüsselwörter

Digitale Rechtsmobilisierung · Legal Technologies · Rechtsdienstleistung · Justizialisierung · Rechtsberatung · Rechtsgeneratoren

---

B. Rehder (✉) · K. van Elten

Fakultät für Sozialwissenschaften, Ruhr-Universität Bochum, Bochum, Deutschland  
E-Mail: [britta.rehder@rub.de](mailto:britta.rehder@rub.de); [Katharina.Vanelten@rub.de](mailto:katharina.vanelten@rub.de)

## 1 Klärung des Begriffs

Rechtsmobilisierung wird allgemein verstanden als ein Prozess, in dem „a desire or a want is translated into a demand as an assertion of rights“ (Zemans, zitiert nach: McCann 2008, S 523). Die *digitale Rechtsmobilisierung* nutzt zur Einleitung rechtlicher Verfahren so genannte *Legal Technologies*. Sie umfassen *Software*-Angebote oder *Online*-Dienste, die juristische Arbeitsprozesse technisch unterstützen oder ersetzen und dabei Rechtsdienstleistungen automatisieren. In diesem Zusammenhang kommt auch Künstliche Intelligenz zum Einsatz.

*Legal Technologies* sind in Bezug auf die Rechtsmobilisierung in folgenden Varianten und Einsatzbereichen relevant:

- *Online*-Plattformen, wie z. B. Anwaltssuchmaschinen, Anwaltsportale oder Marktplätze ermöglichen die aktive Suche nach Klagenden, z. B. durch personalisierte Werbung, sowie die Zusammenführung von Rechtsuchenden und Anwaltskanzleien. Diese neuen Vermarktungsformen wurden gefördert nach der Verabschiedung des Rechtsdienstleistungsgesetzes im Jahr 2008, das den Markt für *Rechtsberatung* liberalisierte. Das sogenannte „Anwaltsmonopol“ wurde im Bereich der außergerichtlichen Rechtsdienstleistungen deutlich ge lockert. Im Zusammenspiel mit der fast vollständigen Abschaffung der Singularzulassung, d. h. der Zulassung eines Anwalts an ausschließlich einem bestimmten Gericht, wurde der Wettbewerb zwischen den Anwaltskanzleien sowie mit der nicht-anwaltlichen Rechtsberatung intensiviert. Mit dem Wegfall der örtlichen Beschränkung von Rechtsdienstleistern wurden *Online*-Plattformen zu wichtigen Instrumenten der Markterschließung.
- Automatisch generierte Anträge oder Widersprüche in standardisierten oder niedrigschwelligen Gerichts- und Verwaltungsverfahren werden häufig von organisierten Interessengruppen oder im Rahmen professionell geführter Kampagnen unterbreitet. Auch Verfassungsbeschwerden werden über derartige Mechanismen gesammelt. Die Digitalisierung erfüllt hier lediglich eine Hilfsfunktion, weil im Regelfall die generierten Schriftsätze ausgedruckt und mit manueller Unterschrift an einen Adressaten versendet werden müssen. In dem Maße, in dem sich im Zuge der weiteren Digitalisierung von Verwaltung und Justiz die rechtsverbindliche Signatur durchsetzt, wird dies zukünftig verzichtbar sein. Dessen ungeachtet kann die durch das Netz fast grenzenlose Verbreitung dieser Musterbriefe auch heute schon eine beträchtliche Wirkung im Rechtssystem entfalten. So mobilisierte ein Netzwerk aus den Organisationen „Mehr Demokratie“, „Campact“ und „foodwatch“ mit ihrer Kampagne gegen das Freihandelsabkommen CETA im Jahr 2016 mit ca. 125.000 Verfassungsbeschwerden die größte sogenannte Bürgerklage in der Geschichte der Bundesrepublik.
- *Rechtsgeneratoren* übernehmen, anders als die beiden bisher genannten *Legal Technologies*, juristische Kernaufgaben, indem sie eine automatisierte Beurteilung zu einem einfachen rechtlichen Sachverhalt erstellen. Letzterer wird dabei über einen Fragenkatalog abgefragt und mit einer – meist zuvor programmierten und darum auch standardisierten – rechtlichen Beurteilung verknüpft. Gebühren-

und Fristenrechner zählten zu den ersten Rechtsgeneratoren. Prominent werden sie seit einigen Jahren v. a. im Bereich des Verbraucherschutzes, wenn Entschädigungsansprüche bei Zug- und Flugverspätungen oder -ausfällen ausgerechnet werden (z. B. *Flightright*). *Legal Robots* gelten als besonders weit entwickelte Rechtsgeneratoren, weil sie durch den Einsatz von Künstlicher Intelligenz als lernende Systeme auch komplexere Rechtsprobleme beurteilen können sollen. Ihre Entwicklung und Anwendung steckt jedoch noch in den Kinderschuhen. Und ihr Entwicklungspotenzial wird kontrovers beurteilt.

Mit dem Einzug der Digitalisierung in das Rechtssystem ist ein neuer Akteurstyp in Erscheinung getreten, so genannte *Legal-Tech-Rechtsdienstleister*, in denen Betriebswirte und vor allem IT-Spezialisten ebenso zentral sind wie Juristen, weil die *Software* das Herzstück der Unternehmung bildet. Als eigenständige Anwaltskanzleien oder in Kooperation mit traditionellen Kanzleien bieten sie die skizzierten automatisierten Rechtsdienstleistungen an. Die *Legal Technologies* ermöglichen es, mehrere Tausend Widerspruchs- oder Gerichtsverfahren parallel zu verarbeiten und zu koordinieren. Die digitalen Rechtsdienstleister werden damit zu wichtigen Akteuren der (rechts-)politischen Mobilisierung und der *Justizialisierung* von Konflikten. Mit den neuen technischen Möglichkeiten, die die Bündelung von Klagen praktikabel machen, werden Massenklagen potenziell zu koordinierten und strategisch genutzten Quasi-Sammelklagen. Dies führt ein neues Element in das deutsche Verfahrensrecht ein, das im Wesentlichen auf dem Prinzip der Individualklage basiert und nur in eng definierten Ausnahmefällen kollektive Klagerechte zubilligt.

---

## 2 Theoretische Grundlagen

Da das Phänomen der digitalen Rechtsmobilisierung bisher kaum sozialwissenschaftlich untersucht worden ist, liegen keine themenspezifischen Theorien vor. Für die Politikwissenschaft ist das Thema jedoch relevant in Bezug auf Fragen der Mobilisierung von Recht und der Verrechtlichung von Politik. Rechtsmobilisierung kann als eine Variante der politischen Partizipation verstanden werden, wenn sie deren grundlegende Funktionen erfüllt (instrumentelle Durchsetzung von Zielen, Stärkung der Identifikation, Erziehung zum Staatsbürger, expressive Funktion der Darstellung eigener Positionen). In instrumenteller Hinsicht wäre dies der Versuch, durch Gerichtsentscheidungen materielle oder altruistische Ziele durchzusetzen und Einfluss auf politische Entscheidungen zu nehmen oder diese herbeizuführen. Die Identifikationsfunktion wird erfüllt, wenn z. B. durch Massenklagen Prozesse der Gruppen- und Identitätsbildung stattfinden. Im Zuge der Wahrung von Rechten und des Kampfes um die Anerkennung von Rechtsansprüchen wird die Erziehung und Bildung zum Staatsbürger gefördert, sie setzt diese aufgrund der Expertenzentriertheit rechtlicher Verfahren jedoch gleichzeitig auch schon voraus. Und auch die expressive Funktion der politischen Partizipation kann durch die Rechtsmobilisierung erfüllt werden, wenn diese durch mediale Aufmerksamkeit oder Öffentlichkeitskampagnen Unterstützung erfährt. Für die Analyse politischer Prozesse ist die

Rechtsmobilisierung dann besonders interessant, wenn sie als kollektives Handeln und damit als Form der Interessenvermittlung in Erscheinung tritt, wobei ein Spezifikum der Rechtsmobilisierung darin besteht, dass auch durch individuelles Handeln nachhaltige politische Effekte erzielt werden können. Individuelle Rechtsmobilisierung kann also ein funktionales Äquivalent zur kollektiven politischen Mobilisierung sein. Die Idee des Minderheitenschutzes macht den Rechtsweg immer auch zu einer attraktiven zweitbesten Strategie zur Interessendurchsetzung, wenn der direkte Zugang zur Legislative oder Exekutive blockiert ist.

Im allgemeisten Sinne beeinflusst die Digitalisierung Prozesse der Mobilisierung dahingehend, dass sie den Zugang zum Rechtssystem erleichtert. Das Internet bzw. die sozialen Medien sowie *die Legal Technologies* mit ihren Informations-, Kommunikations- und Vernetzungsoptionen ermöglichen die kostengünstige, ortsunabhängige individuelle oder kollektive und ggfs. auch transnationale Rechtsmobilisierung. Für die potenziellen Mandanten reduzieren sich Transaktionskosten und Entscheidungsunsicherheit, weil wichtige Barrieren der politischen und rechtlichen Mobilisierung gesenkt werden. Dies ermöglicht Massenklagen, die bisher eher aus dem US-amerikanischen Rechtssystem bekannt sind, in bisher ungekannter Zahl und Verbreitung.

Die Wahrscheinlichkeit von (Massen-)Klagen ist in der rechtssoziologischen Forschung untersucht worden. Sie hat gezeigt, dass die Bereitschaft, Konflikte als Rechtskonflikte zu deuten, mit der sozialen und regionalen Distanz der Beteiligten steigt. Auseinandersetzungen in gelegentlichen oder anonymen Sozialbeziehungen werden häufiger verrechtlicht als laufende und persönliche Sozialbeziehungen. Bei Verkehrsdelikten sind justizelle Auseinandersetzungen also eher zu erwarten als im Arbeitsrecht, in großen Betrieben klagen Beschäftigte eher als in kleinen Betrieben. Im Zuge der Digitalisierung steigt vor allem die Zahl der gelegentlichen und anonymen Beziehungen. Die Wahrscheinlichkeit des rechtlichen *Framings* eines Konflikts wächst dadurch. Gleichzeitig können Menschen unter den Bedingungen von Anonymität und sozialer Distanz eher für eine Interessendurchsetzungsstrategie über den Rechtsweg als für kollektives politisches Handeln (z. B. im Rahmen einer sozialen Bewegung oder Bürgerinitiative) gewonnen werden, denn einige der zentralen Handlungsvoraussetzungen entfallen. Die Rechtsmobilisierung braucht Ressourcen, aber keine Organisation der Betroffenen. Sie braucht auch keine kollektive Identität, weil keine direkten politischen Aktionen stattfinden. Die digitale Rechtsmobilisierung ermöglicht die anonyme und niedrigschwellige Interessenverfolgung über große soziale und regionale Distanzen hinweg.

Zudem wird in der Literatur davon ausgegangen, dass Menschen eine Kosten-Nutzen-Relation anstellen, bei denen die (häufig monetären) Kosten und der (häufig finanzielle) Gewinn abgewogen werden. Eine Rechtsschutzversicherung erhöht die Bereitschaft zur Klage. Der potenzielle Gewinn wird den Betroffenen jedoch im Regelfall erst im Zuge einer Rechtsberatung verdeutlicht, die sie aktiv einholen müssen. *Legal-Tech*-Kanzleien senken die Komplexität und Entscheidungsunsicherheit massiv durch verschiedene Faktoren. Durch offensive (und häufig auch personalisierte) Werbung, z. B. in den sozialen Medien, wird das Verhältnis von Nachfrage und Angebot umgekehrt. Der Ratsuchende sucht keine Rechtsberatung auf,

sondern die Rechtsberatung kommt zu ihm und bietet ihm ein rechtliches *Framing* an, während er sich der Natur seines Konflikts womöglich noch gar nicht bewusst ist. Wenn ratsuchende Menschen im Internet kostenfrei durch Rechtsgeneratoren ihre vermeintlichen Ansprüche auf Schadensersatz oder Abfindung ausrechnen können, noch bevor sie mit einem Anwalt oder einer anderen Rechtsberatung gesprochen haben, rücken der vermeintlich sichere Erfolg und der finanzielle Nutzen in den Vordergrund und die Erwartungshaltung wird entsprechend vorstrukturiert. Dadurch wird auch die *Gatekeeper*-Funktion der Rechtsberatung neu akzentuiert. Aus ihren kommerziellen Interessen heraus tendieren *Legal-Tech*-Kanzleien vermutlich dazu, Konflikte eher in konfrontative Widerspruchs- und Gerichtsverfahren statt in Verhandlungslösungen münden zu lassen. Allerdings liegen bisher kaum empirische Befunde zum Selbstverständnis von *Legal-Tech*-Rechtsdienstleistern als Konfliktakteure vor.

Ihre Schlüsselstellung für die (rechts-)politische Mobilisierung und die Justizialisierung der Konflikte reiht sie ein in die Riege der Akteure, die Interessenvermittlung über den Markt organisieren (Speth und Zimmer 2015). Im Zentrum stehen dabei Nichtregierungsorganisationen oder professionelle Agenturen, die keine politischen Mitgliederorganisationen im engeren Sinne mehr darstellen, sondern kommerziell oder auf der Basis von Spendengeldern ohne demokratische Mitbestimmungsstrukturen agieren. (Digitale) Anwaltskanzleien als interessenpolitische Akteure können in diesem Konzept gerahmt werden. Motiviert durch ihre kommerziellen Interessen, realisieren sie gleichzeitig die Interessen von Personengruppen, die ohne dieses „Geschäftsmodell“ kaum durchsetzungs- und konfliktfähig wären. Dabei übernehmen sie wichtige Funktionen in Bezug auf die Mobilisierung, die Koalitionsbildung sowie auf das *Framing* des Konflikts.

---

### 3 Praktische Anwendungsfelder

Digitale Rechtsmobilisierung ist vor allem ein Instrument schwacher Interessen und insofern in den verschiedensten Politikfeldern zu beobachten. Dies gilt aber auch schon für die klassischen „analogen“ Formen der Rechtsmobilisierung. Spezifischer können die Anwendungsfelder umrissen werden, wenn kommerzielle *Legal-Tech*-Kanzleien involviert sind. Diese bieten ein „Supermarktmodell“ der Rechtsdienstleistung an und verfolgen eine Strategie der „economies of scale“. Mit Bezug zu sehr selektiven Rechtsfragen werden einfache und standardisierte Rechtsdienstleistungen angeboten, die aber ein Massenpublikum adressieren. Im Sozialrecht sind dies z. B. Hartz-IV-Bescheide, Sozialhilfe- oder BaFin-Bescheide. Auch hier stehen schwache Interessen im Zentrum, die über einen vermeintlich schlechten Zugang zum Rechtssystem verfügen oder deren Streitwert so gering ist, dass sie ihr Recht ohne die niedrigschwelligen Angebote der *Legal-Tech*-Anbieter nicht mobilisieren würden. Anders als z. B. bei NGOs oder Bewegungsnetzwerken geht es immer um die Verfolgung materieller Interessen. Klassische Adressaten sind Verbraucher, Patienten, aber auch Sozialbürger und Arbeitnehmer. Während die *Legal-Tech*-Anbieter im Verbraucherschutz und im Gesundheitssektor den Umstand nutzen,

dass einflussreiche Mitgliederorganisationen fehlen, signalisiert ihre Entstehung im Arbeits- und Sozialrecht die abnehmende Wirkmächtigkeit von Sozialverbänden und Gewerkschaften.

Der Prototyp einer digitalen Rechtsmobilisierungskampagne ist die Massenklage gegen den Volkswagen-Konzern im Zuge des Skandals über die Manipulation von Abgaswerten in Diesel-Fahrzeugen. Die „Dieselgate“-Affäre dürfte eine der größten transeuropäischen Bürgerbewegungen der letzten Jahrzehnte hervorgerufen haben, die ohne jede direkte Aktion und Protestformen auskommt, sondern die sich ausschließlich über den Rechtsweg formiert. In mehreren Verbünden aus Anwaltskanzleien und Verbraucherschutzorganisationen wurden Zighausende Schadensersatzklagen von betroffenen Dieselfahrzeug-Besitzern gebündelt. Die transnationale Bewegung erstreckt sich auf viele europäische Länder. Neben Deutschland sind dies Österreich, die Schweiz, Italien, Belgien, Spanien, Litauen, Slowenien, die Slowakei und Portugal. Einer der zentralen Akteure ist die *Legal-Tech-Agentur „MyRight“*, die das Handeln transnational koordiniert.

Die Entstehung der Bewegung kann auf zwei Ursachen zurückgeführt werden. Erstens legte sich die deutsche Bundesregierung in diesem Konflikt sehr frühzeitig darauf fest, vorrangig die Interessen der deutschen Automobilkonzerne und weniger die Verbraucherinteressen zu schützen. Volkswagen sollte zwar verpflichtet werden, die betroffenen Fahrzeuge nachzurüsten und Fehler zu beheben. Eine Entschädigung sollte den Fahrzeugbesitzern jedoch nicht zugesprochen werden. Dieses Vorgehen fand auch die Unterstützung der IG Metall, die ein Interesse daran formulierte, die Arbeitsplätze der Beschäftigten abzusichern. Die Öffentlichkeit und die Betroffenen reagierten empört, der Automobilkorporatismus – das Herzstück der koordinierten Ökonomie in Deutschland – verlor innerhalb kurzer Zeit seine Legitimität. Die zweite Ursache lag in der Vorbildfunktion des US-amerikanischen Rechtssystems, das Volkswagen sowohl in straf- als auch in schuldrechtlicher Hinsicht sehr viel stärker zur Rechenschaft zog. Über den Weg der Sammelklage wurde der Konzern in einen Vergleich gezwungen, der in einen Entschädigungsfonds von 10 Milliarden Dollar mündete. Die Gegner des deutschen Diesel-Korporatismus nahmen die US-amerikanische Sammelklage als Vorbild, um in und für Europa nach funktionalen Äquivalenten zu suchen. Dieser Fall ist ein klassisches Beispiel für eine Interessenpolitik über das Rechtssystem, die für gesellschaftliche Gruppen als zweitbeste Strategie gewählt wird, wenn der Zugang zu politischen Entscheidungskanälen blockiert ist. Diese Strategie wird umso attraktiver, je mehr sie in anderen Ländern erfolgreich ist.

In Europa beschäftigen sich vermutlich mehrere Hundert Anwaltskanzleien mit den Folgen des Diesel-Skandals und bieten Rechtsvertretung an. Dass aus diesem fragmentierten Handeln eine politische Bewegung werden konnte, ist ein Ergebnis der *Legal Technologies* und ihrer Protagonisten. Aufgrund des Fragmentierungsgrades des Verfahrensrechts in Europa existieren verschiedene parallele Aktionsnetzwerke, die entlang jeweils eigener rechtlicher Wege operieren. Aus deutscher Perspektive ist dabei der *Legal-Tech-Rechtsdienstleister „MyRight“* besonders interessant. Er nimmt aber auch innerhalb der gesamten Bewegung eine Schlüsselstellung ein, weil er explizit transnational agiert. *MyRight* ist ein deutsches Unternehmen mit Sitz in Berlin, gegründet von drei jungen Männern (Wirtschaftsingenieur, Rechtsanwalt, IT-Spezialist). Zwei von ihnen haben sich zuvor bereits mit der Durchsetzung von Fluggastrechten auf der

EU-Ebene profiliert (*FlightRight*), *MyRight* spezialisiert sich nun auf den Abgas-Skandal. Die Rolle von *MyRight* als auch politischer Akteur wird besonders deutlich. Erstens: das Unternehmen bündelt Klageaktivitäten, und zwar auf transnationaler Basis. *MyRight* betreibt offensiv und digital Werbung, um potentielle Mandanten mit dem expliziten Ziel mehrerer „Sammelklagen“, die jeweils Zehntausende Einzelklagen umfassen. Mit einem Rechtsgenerator, der auf verschiedene Fallkonstellationen eingeht, können sich Betroffene auf der *Homepage* über ihre Ansprüche informieren und werden sogleich zur Rechtsvertretung weitergeleitet. Zweitens: *MyRight* formiert in diesem Zusammenhang Koalitionen. Am Anfang des Prozesses standen dabei Kooperationen mit verschiedenen europäischen Verbraucherschutzorganisationen im Zentrum. Jüngst wurden aber auch Kooperationsvereinbarungen mit Verbänden der Logistikbranche geschlossen, deren Mitgliedsunternehmen *MyRight* die Interessenvertretung für ihren gesamten Fuhrpark übertragen haben. Dadurch wurde der Konflikt auch zu einem Konflikt zwischen verschiedenen Wirtschaftsinteressen transformiert. Drittens: *MyRight* definiert ein *Framing*, das explizit auch ein politisches *Framing* ist, indem auf der *Homepage* gleichzeitig die Bundesregierung kritisiert wird. Man operiert hier an der Schnittstelle zwischen professioneller Anwaltskanzlei mit Wirtschaftsinteressen und politischer Nicht-Regierungsorganisation – ähnlich wie dies die so genannten „Public-Interest-Law-Firms“ in den USA tun. Und viertens bietet *MyRight* kreative rechtliche Verfahrenslösungen an, um koordinierte strategische Prozessführung zu betreiben. Die Akteure bezeichnen ihren Klagetypus als Sammelklage, die in dieser Form bisher weder in Deutschland noch auf der EU-Ebene existiert. Diese begriffliche Deklaration ist aber Teil der Offensivstrategie, US-amerikanische Praktiken zu transferieren und die Politik sowie Volkswagen durch strategische Prozessführung unter Druck zu setzen. Eine bis dato wenig bekannte Regelung der Zivilprozessordnung wird zur Anspruchsbindung genutzt. Die Betroffenen treten ihre jeweiligen Ansprüche an die Kanzlei ab, die auf eigenes Risiko klagt, im Erfolgsfall aber jeweils 35 Prozent des Gewinns einbehält. Für die Kläger ist die Kosten-Nutzen-Bilanz ideal. Sie tragen weder Kosten noch Risiko, da sie sich per Mausklick am Klagegeschehen beteiligen und mit ihren Ansprüchen auch alle Risiken an die Kanzlei abtreten.

*Legal-Tech*-Kanzleien präsentieren sich als kleine *Start-Up*-Unternehmen. Im Fall von *MyRight* wird aber deutlich, dass man angewiesen ist auf eine größere Struktur, denn die offensive digitale Rechtsmobilisierung ist in erheblichem Maße auf externe Ressourcen angewiesen. Bedeutend sind hier finanzielle Ressourcen für die strategische Prozessführung und vor allem für das finanzielle Risiko, das von der Kanzlei getragen wird. Im Hintergrund steht eine Kooperation mit der sehr renommierten US-amerikanischen Anwaltskanzlei Hausfeld, die bekannt ist für offensive Prozessführung und in den USA auch an der Aushandlung des Volkswagen-Vergleichs beteiligt war. Finanziert wird die Kampagne vom anglo-amerikanischen Finanzdienstleister Burford Capital, der auf Prozessfinanzierung spezialisiert ist. Die *Legal-Tech-Start-Up*-Szene, die mit ihren Entwicklungen die technischen Voraussetzungen zur digitalen Rechtsmobilisierung schafft, bietet also ein Einfallstor für große US-amerikanische Anwaltskanzleien, die das System der an Marktgrundsätzen orientierten und risikobereiten Rechtsdurchsetzung beherrschen und finanzieren können. Die Digitalisierung im Rechtssystem zieht auch dessen potenziell weitere Amerikanisierung nach sich.

## 4 Umsetzungsstand und Auswirkungen

Digitale Rechtsmobilisierung und insbesondere *Legal-Tech*-Rechtsdienstleister sind eine neue Erscheinung. Der Deutsche Anwaltstag vermutet, dass ca. 60 *Legal-Tech-Start-Ups* in Deutschland (und ca. 1500 weltweit) tätig sind, mit stark wachsender Tendenz (Stand 4/2017). Während einige Rechtsgebiete, v. a. die Abwicklung von Fluggastrechten in der EU, heute schon weitgehend in digitaler Hand liegen, sind *Legal Technologies* in den meisten anderen Rechtsgebieten eher noch ein Ausnahmephänomen. Welche Anbieter sich mittelfristig etablieren können, ist bisher kaum absehbar und auch nicht erforscht. Allerdings wird schon jetzt deutlich, dass digitale Kanzleien durch *First-Mover-Advantages* erhebliche Marktkonzentrationen anstreben können. So betreut z. B. die Kanzlei „RightMart“ nach eigenen Angaben 40.000 Hartz-IV-Mandate und ist damit im kleinteilig organisierten Markt der sozialrechtlichen Rechtsberatung ein bedeutender *Player* geworden.

Die weitere Etablierung der digitalen Rechtsmobilisierung über *Legal-Tech*-Anbieter hängt von mindestens vier Faktoren ab. Der wichtigste Faktor der fortschreitenden Automatisierung von Rechtsdienstleistungen ist die technische Entwicklung. In welchem Umfang auch komplexere Rechtsvorgänge durch Künstliche Intelligenz digitalisiert werden können, (die vom Mandanten auch akzeptiert werden!), liegt heute noch im Bereich der Spekulation. Der zweite kritische Faktor liegt in der weiteren Entwicklung der finanziellen Geschäftsmodelle. Im Verbraucherschutz, teilweise auch im Arbeitsrecht, profitieren *Legal-Tech*-Rechtsdienstleister von der Kooperation mit anglo-amerikanischen Anwaltskanzleien und Prozessfinanzierern. Im Sozialrecht wird vor allem die staatliche Prozesskostenhilfe abgeschöpft. Wie stark der Markt für digitale Rechtsdienstleistungen auf dieser Basis wachsen kann und ob alternative Finanzierungsquellen erschlossen werden können, ist ungewiss. Der hohe Finanzbedarf macht es wahrscheinlich, dass digitale Rechtsmobilisierung nur in spezifischen Segmenten ertragreich sein kann. Ein dritter Faktor liegt in möglichen Diffusionsprozessen. In dem Maße, in dem auch konventionelle Anwaltskanzleien digitale Instrumente adaptieren, verlieren die *Legal-Tech-StartUps* ihren Exotenstatus und werden womöglich die Differenzen zwischen analoger und digitaler Rechtsmobilisierung nivelliert. Und die derzeit wohl bedeutendste potenzielle Grenze der digitalen Rechtsmobilisierung liegt in der staatlichen Regulierung, die schon im jetzigen sehr frühen Entwicklungsstadium auf eine Begrenzung der kommerziellen Spielart digitaler Rechtsmobilisierung abzielt (s. unter Abschn. 5). Das Negativszenario des politischen Handelns liegt im Heranwachsen einer „Klageindustrie“ US-amerikanischer Spielart.

---

## 5 Perspektiven für Staat und Verwaltung

Für den Staat und die Verwaltung impliziert die digitale Mobilisierung erstens eine abnehmende Fähigkeit, Interessenvermittlungsprozesse einflusslogisch zu kontrollieren. Insofern signalisiert und verstärkt die digitale Rechtsmobilisierung die ohnehin stattfindende schleichende Erosion korporatistischer Beziehungen zwischen Interessengruppen und dem Staat. Zudem ist die Justiz verstärkt mit der Möglichkeit

strategisch geführter Massenklagen konfrontiert. Die politischen Bewertungen der digitalen Rechtsmobilisierung variieren erheblich. Auf der einen Seite wird eine Stärkung schwacher Interessen konstatiert, wenn große Konzerne durch Massenklagen wirksam unter Druck gesetzt werden können, wenn die Politik dies nicht kann oder will. Gleichzeitig wird aber das Vordringen der US-amerikanischen „Klageindustrie“ in das deutsche bzw. europäische Rechtssystem befürchtet. Diese Sorge kommt auch zum Ausdruck in den verschiedenen Regulierungsvorschlägen, die gegenwärtig auf der nationalen Ebene sowie in den EU-Institutionen diskutiert werden.

Die EU-Kommission befürwortet seit längerem eine Stärkung kollektiver Klage-rechte im Verbraucherschutz nach US-amerikanischem Vorbild. Die deutsche Politik ist – unabhängig von den jeweiligen parteipolitischen Regierungskoalitionen – deutlich skeptischer. Dass auch sie dennoch seit einigen Jahren über eine Stärkung kollektiver Klagerechte diskutiert, ergibt sich aus dem Phänomen. In dem Maße, in dem Massenklagen auftreten, wird es notwendig, Instrumente zu entwickeln, um sie gebündelt zu bearbeiten, da sonst ein Kollaps der Justiz droht. Dessen ungeachtet spiegeln sich die unterschiedlichen Präferenzen zwischen nationalen und europäischen Akteuren in den Vorschlägen wider. Das jüngst verabschiedete deutsche Musterfeststellungsklagegesetzes sieht ein zweistufiges Verfahren vor. Demnach soll auf der ersten Stufe kollektiv geklagt werden können, wenn die Feststellung der Schuld im Zentrum steht. Den daraus resultierenden individuellen Schadensersatz soll dann aber wieder jeder Betroffene individuell einklagen müssen. Die Rechts-mobilisierung wird dadurch in erheblichem Maße ausgebremst. Der Richtlinien-Vorschlag der EU-Kommission geht demgegenüber deutlich weiter. So wie in den USA soll aus der kollektiven Klage ein unmittelbarer Schadensersatzanspruch hervorgehen.

Beide Vorschläge stimmen indessen darin überein, die Macht der digitalen Anwaltskanzleien begrenzen zu wollen. Hier formiert sich auch eine Koalition mit den Rechtsanwaltskammern, die die Konkurrenz der digitalen Rechtsdienstleister vehement bekämpfen – vorrangig ebenfalls über den Rechtsweg. Stattdessen sollen Verbände oder andere so genannte „qualifizierte“ Organisationen und Institutionen klagebefugt sein, die kein unmittelbar ökonomisches Eigeninteresse daran haben. Damit wird ein in Europa schon länger beobachtbarer Weg weiter beschritten, der das Instrument der altruistischen Verbandsklage ausbaut, um die anwaltszentrierte Sammelklage zu verhindern. Dass dies die vordringende Macht US-amerikanischer Anwaltskanzleien und ihrer digitalen Ableger in Europa tatsächlich nachhaltig begrenzen wird, ist eher nicht zu erwarten. Erstens ist der Verbraucherschutz in Europa ein interessanter und potenziell wachsender Markt, den interessierte Anwaltskanzleien sich nicht nehmen lassen werden, zumal zu erwarten ist, dass eine europäische Sammelklage im Verbraucherschutz auf andere Politikfelder ausstrahlen wird, vor allem in den Gesundheitssektor und die Agrar- und Lebensmittelwirtschaft. Zweitens dockt die Vorstellung eines Verbandsklagerechts an korporatistische Ordnungsmodelle an, in denen wenige Interessenorganisationen gesellschaftliche Interessen bündeln und kanalisieren. Dieses Modell spielt in weiten Teilen Europas keine Rolle. Im Spektrum des Verbraucherschutzes wird sich immer eine

Organisation finden, die ein Interesse an strategischer Prozessführung hat. Und die weitere Entwicklung von *Legal Technologies* entzieht die Diffusion von Prozessen der digitalen Rechtsmobilisierung jeder Kontrolle. Und drittens werden auch viele der qualifizierten Institutionen ihr Klagerecht nur durch professionelle Anwaltskanzleien wirksam wahrnehmen können, zumal sowohl das deutsche Gesetz als auch der europäische Richtlinievorschlag einen *First-Mover-Advantage* vorsehen. Demnach definiert der Akteur, der die erste Klage einreicht, den „Master-Frame“ des Konfliktgeschehens. Dies wird ohne anwaltliche Unterstützung kaum möglich sein. Eher ist zu erwarten, dass nun auch andere Akteure in anderen Politikfeldern für eine Stärkung ihrer kollektiven Klagerechte kämpfen werden, so z. B. die Gewerkschaften, die der Stärkung von Verbraucherrechten etwas entgegensemzen wollen, um Arbeitnehmerrechte zu schützen, zumal sie auch in ihren Kernpolitikfeldern mit kommerziellen digitalen Rechtsdienstleistern konfrontiert sind.

---

## Literatur

- Blankenburg, Erhard. 1980. Mobilisierung von Recht. Über die Wahrscheinlichkeit des Gangs zum Gericht, die Chance des Erfolgs und die daraus folgenden Funktionen der Justiz. *Zeitschrift für Rechtssoziologie* 1(1): 33–64.
- Hartung, Markus, Micha-Manuel Bues, und Gernot Halbleib. 2018. *Legal Tech. Die Digitalisierung des Rechtsmarkts*. München: C.H. Beck/Vahlen.
- Kagan, Robert A. 2001. *Adversarial legalism. The American way of law*. Harvard: Harvard University Press.
- Kelemen, R. Daniel. 2011. *Eurolegalism. The transformation of law and regulation in the European Union*. Cambridge: Harvard University Press. (Hieran anschließend die beiden Titel von McCann und von Speth/Zimmer).
- McCann, Michael. 2008. Litigation and legal mobilization. In *The Oxford handbook of law and politics*, Hrsg. Keith E. Whittington, Daniel R. Kelemen und Gregory A. Caldeira, 522–540. Oxford: Oxford University Press.
- Speth, Rudolf, und Annette Zimmer, Hrsg. 2015. *Lobby Work. Interessenvertretung als Politikgestaltung*. Wiesbaden: Springer.
- Wagner, Jens. 2018. *Legal Tech und Legal Robots. Der Wandel im Rechtsmarkt durch neue Technologien und künstliche Intelligenz*. München: Springer/Springer Gabler.

---

## **Teil V**

### **Akteure und Institutionen**



---

# Digitale Agenda der Europäischen Kommission

Göttrik Wewer

## Inhalt

1 Klärung des Begriffs .....	374
2 Programmatische Grundlagen .....	374
3 Thematische Schwerpunkte .....	375
4 Umsetzungsstand und Auswirkungen .....	377
5 Perspektiven für Staat und Verwaltung .....	379
Literatur .....	380

---

## Zusammenfassung

Die Zukunft der Weltwirtschaft werde nicht mehr am Atlantik, sondern am Pazifik entschieden, heißt es. Die großen Spieler, die in der digitalen Ökonomie das Tempo bestimmen und die Standards setzen, kommen heute entweder aus den USA oder aus China. Die Digitale Agenda der Europäischen Kommission sollte einen Anstoss geben, Europa fit zu machen für das digitale Zeitalter. Die Strategie für einen einheitlichen digitalen Binnenmarkt zielte darauf ab, das Gewicht Europas im globalen Wettbewerb angemessen zur Geltung zu bringen und zugleich europäische Rechtsnormen auch gegenüber globalen Konzernen durchzusetzen. Auf beiden Feldern ist sie unterschiedlich weit gekommen.

---

## Schlüsselwörter

Staatenverbund · Einheitlicher Binnenmarkt · Globale Konkurrenz · Technologische Marktführerschaft · Digitale Souveränität

---

G. Wewer (✉)

Lorenz-von-Stein-Institut für Verwaltungswissenschaften an der Christian Albrechts-Universität zu Kiel, Kiel, Deutschland

E-Mail: [g.wewer@bvdp.de](mailto:g.wewer@bvdp.de)

## 1 Klärung des Begriffs

Die Europäische Union (EU) bzw. die Europäische Kommission hat das Aufkommen dessen, was Informationsgesellschaft, Kommunikationsgesellschaft, Wissensgesellschaft, Netzwerkgesellschaft (Danyel 2012), aber auch digitaler Kapitalismus oder Plattform-Ökonomie genannt wurde, von Anfang an beobachtet, begleitet und zu gestalten versucht. 2010 legte die Europäische Kommission – als einen von sieben Bausteinen der Strategie „Europa 2020“ –, erstmals eine „Digitale Agenda für Europa“ vor, mit der unter anderem Bildung, Forschung und Innovation gefördert werden sollten. Diesen auf zehn Jahre angelegten Aktionsplan ergänzte sie 2015, wie zuvor in ihrer *Single Market Strategy* angekündigt, mit einer speziellen „Strategie für den digitalen Binnenmarkt“, die ihrerseits sechzehn Initiativen umfasste. 2016 verabschiedete die Kommission außerdem eine „Europäische Agenda für die kollaborative Wirtschaft“, an der sich die Mitgliedstaaten bei der Regulierung der sogenannten *Sharing Economy* möglichst orientieren sollten (Wewer 2016).

Wenn die Europäische Kommission ausdrücklich eine Digitale Agenda formuliert, dann will sie nicht nur signalisieren, dass sie die Bedeutung dieses Megathemas verstanden hat, sondern auch die Mitglieder der Union mahnen, dass hier dringend etwas getan werden muss, wenn Europa gegenüber Amerika und Asien nicht weiter an Boden verlieren soll.

---

## 2 Programmatische Grundlagen

Europa ist weder ein Bundesstaat noch ein Staatenbund, sondern – in der Interpretation des Bundesverfassungsgerichts – ein Gebilde *sui generis*, ein Staatenverbund. Die gemeinsam handelnden EU-Mitgliedstaaten bilden völkerrechtlich keinen Staat, aber durch die weitreichende Übertragung von Souveränitätsrechten an die Europäische Union stellt sie doch mehr dar als einen Staatenbund. Eine digitale Agenda oder Strategie verfolgen können die Europäische Kommission, das Europäische Parlament, der Europäische Rat, in dem sich die Staats- und Regierungschefs der Mitgliedstaaten mindestens vierteljährlich treffen, oder die Räte der Europäischen Union, denen die jeweiligen Fachminister angehören (EU-Ministerräte), nur im Rahmen der Kompetenzen, die sie in diesem Verbund durch die Europäischen Verträge zugebilligt bekommen haben. Gesetzentwürfen der Kommission (Verordnungen, Richtlinien) müssen sowohl der zuständige Ministerrat als auch das Parlament zustimmen, damit sie in Kraft treten können. Mit dem Auftrag, einen einheitlichen Binnenmarkt zu schaffen und Europa binnen zehn Jahren zum „wettbewerbsfähigsten und dynamischsten wissensgestützten Wirtschaftsraum der Welt“ zu machen, wie es in der Lissabon-Strategie aus dem Jahre 2000 hieß, hat die Kommission allerdings genügend Rückendeckung für ihre digitale Agenda. „Europa 2020“, zehn Jahre nach Lissabon verabschiedet, ist die Fortschreibung dieses Programms.

Wo sie mit Widerständen bei Verordnungen oder Richtlinien rechnen muss oder nicht unmittelbar zuständig ist, aber ein Thema für so wichtig hält, dass es unbedingt angepackt werden muss, arbeitet die Kommission mit „weicheren“ Instrumenten.

Dazu gehören Förderprogramme (wie „Horizon 2020“, das europäische Rahmenprogramm für Forschung und Innovation), aber auch Interpretationen der Beschluss- oder Rechtslage, an denen sich die Mitgliedstaaten orientieren sollen (wie in den Leitlinien zur „kollaborativen Wirtschaft“). Die Kommission kann bei alledem zwar Anstöße geben und gewisse Akzente setzen; sie ist aber letztlich auf das Engagement der Mitgliedstaaten angewiesen, wenn Europa insgesamt voran kommen soll.

Die Digitale Agenda ist eine von sieben Initiativen im Rahmen von „Europa 2020“, einem auf zehn Jahre angelegten Wirtschaftsprogramm der Europäischen Union, mit dem die zweite Kommission unter José Manuel Barroso (2010 bis 2014) auf die Banken- und Finanzkrise reagierte. Sie sieht unter anderem den Ausbau des Breitbands und der Netze in Europa sowie Erleichterungen bei grenzüberschreitender Kommunikation und Dienstleistungen vor. Zwar würde 2010 rund die Hälfte der Europäer das Internet schon täglich nutzen, aber Millionen Menschen noch gar nicht. Man erwartete damals, dass die Anzahl der Arbeitsplätze, bei denen IKT-Kompetenzen zwingend erforderlich seien, bis 2020 um 16 Millionen steigen und grundlegende Kenntnisse schon 2015 bei 90 % aller Arbeitsplätze verlangt würden.

Die Kommission unter Jean-Claude Juncker, die ab 2014 amtierte, schrieb die Digitale Agenda mit ihrer Strategie für einen einheitlichen digitalen Binnenmarkt fort und konkretisierte die bisherigen Vorhaben. Als Präsident der Kommission nahm Juncker einen neuen Zuschnitt der Kommission vor, wonach die Vizepräsidenten sogenannte *Cluster*, also größere Bereiche, übergreifend leiten sollten. Dazu gehörte ein Vizepräsident für den Digitalen Binnenmarkt (Andrus Ansip, Estland). Wie Juncker in seiner Rede vor dem Europäischen Parlament am 22. Oktober 2014 sagte, wollte er „wieder Bewegung in die europäische Politik bringen“. Denn: „Jeder Tag, an dem Europa das große Potenzial seines riesigen digitalen Binnenmarkts nicht nutzt, ist ein verlorener Tag“. Es gelte, die große Lücke an Investitionen zu schließen, die seit dem Höchststand von 2007 von knapp 500 Mrd. € um zwanzig Prozent zurückgegangen seien. Die Strategie für einen einheitlichen digitalen Binnenmarkt, die seine Kommission im Jahr darauf vorlegte, sollte eine Antwort auf verpasste Chancen sein. Rechtliche Hemmnisse müssten beseitigt, die 28 nationalen Märkte zu einem einzigen zusammengeführt werden. Dadurch könnten 415 Mrd. € erwirtschaftet und hunderttausende neue Arbeitsplätze geschaffen werden.

---

### 3 Thematische Schwerpunkte

Da die Digitalisierung sämtlich Lebensbereiche verändert, ist auch die Liste der Themen, die in diesem Wandel zu gestalten sind, beinahe endlos. Die Digitale Agenda der Europäischen Kommission konzentriert sich darauf, durch rechtliche Vorgaben und technische Standards eine gemeinsame Infrastruktur und einen einheitlichen Binnenmarkt zu schaffen, in dem digitale Produkte und Dienste problemlos über nationale Grenzen hinweg angeboten werden können. Einheitliche Spielregeln für alle, das sogenannte *level playing field*, würden es nicht nur Unternehmen, die ihren Hauptsitz nicht in Europa haben, erschweren, die Mitgliedstaaten

bei Steuersätzen, Datenschutz oder anderen Themen gegeneinander auszuspielen, sondern bei rund 520 Millionen Einwohnern auch einen Marktplatz darstellen, der im globalen Wettbewerb Gewicht hat.

Die fortgeschriebene Digitale Agenda sah folgende Schwerpunkte vor:

- Schaffung eines digitalen Binnenmarkts,
- Verbesserung der Interoperabilität, Normen und Standards,
- Stärkung des Vertrauens und der *Online*-Sicherheit,
- Förderung eines schnellen und besonders schnellen Internetzugangs,
- Steigerung der Investitionen in Forschung und Innovation,
- Verbesserung der digitalen Kompetenzen, der Qualifikationen und der Integration in den Arbeitsmarkt.

Die Strategie für einen digitalen Binnenmarkt, die kein Aktionsprogramm für ein ganzes Jahrzehnt darstellt, sondern zügig umgesetzt werden sollte, ruht auf drei Säulen, die jeweils eine Vielzahl von Initiativen und Programmen enthalten:

- ein besserer Zugang für alle zu digitalen Waren und Dienstleistungen,
- optimale Rahmenbedingungen für digitale Netze und Dienstleistungen,
- die digitale Wirtschaft als europäischer Wachstumsmotor.

Mit der Agenda wie mit den ergänzenden Strategien geht es der Kommission im Kern um folgende Ziele:

- die Unterschiede zwischen den Mitgliedstaaten allmählich zu verringern, ohne die digitalen Vorreiter zu bremsen;
- elektronische Transaktionen über Grenzen hinweg zu erleichtern und auszubauen, um die nationalen Märkte zu einem gemeinsamen Markt zusammenzuführen;
- einen europäischen Digitalmarkt zu schaffen, der global Gewicht hat und wettbewerbsfähig ist,
- Innovationen anzustoßen, damit auch in Europa künftig digitale „Champions“ entstehen, die den Weltmarkt anführen.

Ihre eigene Arbeitsweise zu digitalisieren, hat für die Kommission nicht unbedingt Priorität. Allerdings hat sie schon früh begonnen, im *Internet* über ihre Aktivitäten zu informieren und *Online*-Konsultationen durchzuführen (deren Ergebnisse noch nicht systematisch aufgearbeitet sind). Mit dem „eGovernment-Aktionsplan 2016–2020“, der an frühere Pläne seit 2002 anknüpft, will sie die digitale Transformation des öffentlichen Sektors innerhalb der Union weiter vorantreiben, zu der auch die Brüsseler Behörden gehören. Alle öffentlichen Einrichtungen sollen bis 2020 grenzüberschreitende, personalisierte, nutzerfreundliche und durchgängig digitalisierte Dienstleistungen anbieten. Dabei sollen sich alle unter anderem an den Grundsätzen „digital by default“, „cross-border by default“ und „interoperability by default“ sowie dem *Once-only*-Prinzip orientieren, wonach Bürger\*innen und

Unternehmen gewisse Basisdaten nur einmal übermitteln müssen und nicht bei jedem Vorgang wieder. Der Plan ruht auf drei Säulen: einer Modernisierung der Verwaltungen durch elektronische Dienstleistungen, einer Vernetzung der Behörden über Grenzen hinweg und einer Vereinfachung der Interaktionen mit Bürger\*innen und Unternehmen. Die mehr als zwanzig Einzelmaßnahmen dieses Aktionsplans wurden später durch weitere Aktivitäten ergänzt wurden (Europäische Kommission 2017).

Die Kommission, die zu den offiziellen Partnern der *Open Government Partnership* gehört, aber kein Mitglied dieser Plattform werden kann, da es sich dort um ein Bündnis nationaler Regierungen handelt, hat auch über ein offeneres Regieren und Verwalten nachgedacht (Rohen 2014; vgl. auch Brook et al. 2016 und Bremers und Deleu 2016), ohne dass daraus bisher ein stringentes Konzept geworden wäre.

---

## 4 Umsetzungsstand und Auswirkungen

Der europäische Gesetzgeber hat in den letzten Jahren einiges getan, um einen einheitlichen Rechtsrahmen für die digitale Wirtschaft zu schaffen. Dazu gehört neben der Datenschutz-Grundverordnung, die 2018 in Kraft getreten ist, auch die Verordnung über elektronische Identifizierung und Vertrauensdienste im Binnenmarkt (eIDAS-VO), die seit 2016 gilt. Sie legt einheitliche Kriterien für elektronische Signaturen, Zeitstempel, Siegel, Zustelldienste und weitere Dienste fest, die wechselseitig anzuerkennen sind (Roßnagel 2016) und grenzüberschreitende elektronische Transaktionen erleichtern sollen.

Im Rahmen des Programms „Horizon 2020“ hat die Kommission nach eigenen Angaben in den ersten fünf Jahren mit 5,7 Mrd. € rund 1970 ICT-Projekte gefördert, an denen rund 6250 Partner beteiligt waren, um bei digitalen Themen Forschung, Entwicklung und Innovation voranzutreiben.

Bei der Halbzeitbewertung ihrer digitalen Binnenmarktstrategie betonte die Kommission am 10. Mai 2017, sie habe zu den darin vorgesehenen 16 zentralen Maßnahmen insgesamt 35 Vorschläge und Initiativen vorgelegt. Insgesamt seien gute Fortschritte zu verzeichnen, teilweise würden ihre Vorschläge aber noch vom Europäischen Parlament und vom Rat der Europäischen Union als den Mitgesetzgebern beraten. In drei Bereichen seien aus ihrer Sicht weitere Maßnahmen erforderlich: Datenwirtschaft, Cybersicherheit und *Online*-Plattformen. Der Wert der Datenwirtschaft könnte bis 2020 auf 739 Mrd. € steigen, was nach einem Szenario mit hohem Wachstum 4 % des EU-BIP ausmachen würde, sich aber nur realisieren ließe, wenn Daten kontinuierlich zugänglich seien und frei fließen könnten. Wenn es nicht gelänge, Cybersicherheit zu gewährleisten, könnte andererseits ein wirtschaftliches Potenzial von bis zu 640 Mrd. € verloren gehen (European Commission 2019). Bei den *Online*-Plattformen müssten zwei Themen genauer untersucht werden: ihre Handelspraktiken gegenüber Unternehmen, um zu einem fairen Umgang miteinander zu kommen, und die Entwicklung von geeigneten Verfahren für eine einfache Meldung und wirksame Entfernung illegaler Inhalte von solchen Plattformen.

Um die kritischen Infrastrukturen besser zu schützen und ein einheitliches Schutzniveau bei digitalen Produkten und Dienstleistungen festzulegen, legte die Kommission eine Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) vor, die 2016 in Kraft getreten und im Jahr darauf in deutsches Recht übernommen worden ist. Einer größeren Sicherheit soll auch der Ausbau der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) dienen, der Ende 2018 beschlossen worden ist.

Die Kommission erhebt regelmäßig, wie weit sie selbst und die Mitgliedstaaten auf dem Weg in ein digitales Europa gekommen sind. Das *Digital Agenda Scoreboard* ist ein jährlicher Fortschrittsbericht über die Umsetzung dieses Programms, der öffentlich zugänglich ist. Dieses Punktesystem enthält Daten aus dem *Digital Economy and Society Index* (DESI) (European Commission 2018) und dem *European Digital Progress Report* (EDPR). „Europe improves but still needs to close digital gap“, lautete die Pressemitteilung vom 3. März 2017 bei der Vorstellung des Index. Auf den meisten Gebieten gebe es noch erhebliche Disparitäten zwischen den Mitgliedern, die digital besonders weit entwickelt seien, und jenen, die noch am meisten aufzuholen hätten.

Der „Digital Economy and Society Index“ (DESI) verbindet verschiedene Indikatoren, die nicht nur die erreichten Fortschritte („digital performance“) der EU-Staaten abbilden sollen, sondern auch deren Entwicklung hinsichtlich ihrer wirtschaftlichen Wettbewerbsfähigkeit („digital competitiveness“). In den Index fließen fünf Faktoren ein: die Versorgung mit Breitband („Connectivity“), die digitalen Kenntnisse und Fähigkeiten der Bevölkerung („Human Capital“), die tatsächliche Nutzung des Internets durch die Bürger\*innen („Use of Internet Services“), die Verbreitung einschlägiger Werkzeuge in der Wirtschaft („Integration of Digital Technology“) und die Quantität und Qualität der öffentlichen Dienstleistungen, die *online* angeboten werden („Digital Public Services“). Neben dem Überblick über die Lage in der Union gibt es für jeden Mitgliedstaat ein eigenes Profil („Country Profiles“), dem er seine Stärken und Schwächen entnehmen kann.

Trotz aller Bestrebungen, die Entwicklung europaweit zu harmonisieren, zeigt der Index immer noch erhebliche Unterschiede zwischen den Mitgliedstaaten. Nach der Ausgabe aus dem Jahre 2018 hatten Dänemark, Schweden, Finnland und die Niederlande die am meisten fortgeschrittenen digitalen Ökonomien, gefolgt von Luxemburg, Irland, dem Vereinigten Königreich Belgien und Estland. Rumänien, Griechenland und Italien erreichten die niedrigsten Werte unter den 28 EU-Mitgliedern. Deutschland erreichte Platz 14, knapp über dem EU-Durchschnitt.

Die größten Fortschritte hatten 2017 Irland und Spanien gemacht, während es in Dänemark und Portugal die geringsten Fortschritte zu verzeichnen gab. Länder, die an der Spitze der Rangliste stehen, haben es naturgemäß schwerer, noch große Sprünge zu machen, als Länder, die noch einiges aufholen müssen. Trotz spürbarer Fortschritte erreichte Portugal nur Platz 16 unter den 28 Mitgliedern, lag also noch unter dem EU-Durchschnitt, während Dänemark trotz relativ geringer Fortschritte die Rangliste anführte. Fast alle Länder des früheren Ostblocks liegen unterhalb des EU-Durchschnitts oder sogar am Ende der Rangliste, nur Estland (Platz 9) und Litauen (Platz 13) haben es in die obere Hälfte geschafft. In der unteren Hälfte findet man neben Portugal aber auch Frankreich (Platz 18), Zypern (Platz 21) und Italien (Platz 25).

Bei der Dimension Konnektivität, mit der sowohl die Nachfrage als auch das Angebot an festem und mobilem Breitband erfasst werden soll, einschließlich der Preise, führten die Niederlande, Luxemburg, Dänemark und Schweden die Rangliste an, während Griechenland, Kroatien und Italien die Schlusslichter bildeten. Deutschland fiel im Index 2018 gegenüber dem Vorjahr sogar von Platz 11 auf Platz 13 zurück. Bei den öffentlichen Dienstleistungen, die elektronisch angeboten wurden (*eGovernment* und *eHealth*), stand Finnland an der Spitze, gefolgt von Estland, Dänemark und Spanien, während Griechenland, Ungarn und Rumänien die schlechtesten Werte bekamen. Deutschland landete bei den „Digital Public Services“ nur auf Platz 21 unter 28 EU-Mitgliedern. Fünfzehn Staaten lagen hier über dem EU-Durchschnitt, dreizehn darunter. „Den größten digitalen Nachholbedarf gibt es bei der Online-Interaktion zwischen Behörden und Bürgern“, heißt es im DESI-Länderbericht Deutschland 2018 (Europäische Kommission 2018, S. 2). „Nur 39 % der Bevölkerung nutzen elektronische Behördendienste. Damit liegt Deutschland unter den Mitgliedstaaten auf Platz 25“ (ebd.).

Die Kommission will nicht nur wissen, wie sich die Mitgliedstaaten entwickeln, sondern auch, wo Europa im Vergleich mit seinen Wettbewerbern steht. Im „International Digital Economy and Society Index“ (I-DESI) nutzt sie 24 Datensätze, um Trends zu erfassen und die digitale Performanz von 45 Staaten zu vergleichen, darunter siebzehn Staaten, die nicht Mitglieder der Union sind (Australien, Brasilien, Canada, Chile, China, Island, Israel, Japan, Mexico, Neuseeland, Norwegen, Russland, Serbien, Südkorea, die Schweiz, die Türkei und die Vereinigten Staaten). In der Studie von 2018, die sich auf Daten aus den Jahren 2013 bis 2016 stützte, werden die ausgewählten Länder jeweils mit dem EU-Durchschnitt verglichen und die vier besten und die vier schlechtesten Mitglieder in den fünf Dimensionen jeweils mit einer Kontrastgruppe von vier Staaten (China, Japan, Südkorea und die Vereinigten Staaten). Die Analyse zeige, dass die EU-Staaten insgesamt durchaus wettbewerbsfähig sind und dass die besten EU-Mitglieder sich auf dem gleichen oder sogar auf einem höheren Niveau befinden würden wie die Staaten, die im globalen Vergleich am besten abschnitten (S. 7). Bei der Versorgung mit Breitband schneide Europa ähnlich ab und bei der privaten Nutzung des Internets sei man insgesamt weiter als die Vergleichsgruppe. „EU28 Member States do not significantly out-perform their global counterparts in any of the sub-dimensions, but they are consistently just ahead of them“ (ebenda). Bei der Integration digitaler Technologien in die Wirtschaft und die Produktion habe man im EU-Durchschnitt erstmals seit 2013 ein ähnliches Niveau wie die Vergleichsstaaten erreicht. „Public Services is the one dimension where EU28 Member States have consistently performed below their 17 non-EU counterparts“ (ebd.).

---

## 5 Perspektiven für Staat und Verwaltung

Die Digitale Agenda und die Strategie für einen einheitlichen digitalen Binnenmarkt stellen Versuche der Europäischen Kommission dar, Europa im 21. Jahrhundert in der Weltwirtschaft neu zu positionieren. Nur wenn es gelänge, einen großen Markt-platz zwischen den USA (rund 320 Millionen Einwohner) und China (rund 1,4 Milliarden Einwohner) zu etablieren und globale Marktführer in der digitalen Öko-

nomie hervorzubringen, habe Europa eine Chance, nicht nur Wachstum zu generieren, wettbewerbsfähig zu bleiben und seinen Wohlstand zu erhalten, sondern auch eigene Standards weltweit durchzusetzen. Derzeit gehört nur ein einziges Unternehmen (SAP) zu den *Global Player* in der digitalen Ökonomie.

Wenn das gelingen soll, dann genügt es nicht, europäische Vorschriften in nationales Recht zu übernehmen, sondern dann müssen die Mitgliedstaaten darüber hinaus eigene Anstrengungen unternehmen. Dabei kommt es besonders auf die größeren und stärkeren Staaten an. Dass das größte Mitglied der Union im Vergleich mit anderen bei der *Digital Readiness* nur für einen Platz im Mittelfeld erreicht und bei den *Digital Public Services* nur für die hinteren Ränge, ist insofern bedauerlich. Inzwischen haben rund zwanzig EU-Mitglieder eine eigene Digitale Agenda entwickelt und ähnliche Strategien beschlossen.

Die zehn Jahre, für die die Digitale Agenda gelten sollte, laufen 2020 ab. Es bleibt abzuwarten, ob und wie sich die neue Kommission nach der Europawahl vom 23. bis 26. Mai 2019, der neunten Direktwahl des Europäischen Parlaments, digitalen Themen widmet. Dass sie dieses Megathema überhaupt nicht anspricht, ist nicht zu erwarten. Ein neuer Zehn-Jahres-Plan kann zwar als sinnvoll angesehen werden, weil spürbare Erfolge kaum in kurzer Zeit erzielt werden können, aber angesichts der Dynamik der digitalen Ökonomie können auch kurzfristigere Initiativen ratsam sein, um auf unerwartete Entwicklungen schneller zu reagieren. Ob sich die neue Kommission entweder auf den langfristigen oder auf einen kurzfristigen Ansatz festlegt oder für eine Kombination beider Ansätze entscheidet, muss sich zeigen. Die Grundfrage lautet unverändert, wie Europa im digitalen Zeitalter wettbewerbsfähig bleiben, Wachstum generieren und seinen Wohlstand erhalten kann. Wenn die Zukunft der Weltwirtschaft nicht mehr am Atlantik, also zwischen Amerika und Europa, entschieden wird, sondern am Pazifik, also zwischen Amerika und Asien, wo China, Singapur und andere ganz andere Wachstumsraten aufweisen, dann ist die Frage, wie eine schnellere digitale Transformation von Wirtschaft und Verwaltung gelingen kann, von zentraler Bedeutung für Europas Position im globalen Wettbewerb.

---

## Literatur

- Bremers, Joan, und Wouter Deleu. 2016. *Towards faster implementation and uptake of open government*. Brüssel: Europäische Kommission.
- Brook, Michelle, Mat Basford, Niamh Webster, Andy Williamson, und Anthony Zacharzewski. 2016. *Developing a model for open government in the EU*. Brüssel: Open Society European Policy Institute.
- Bundesregierung, Hrsg. 2017. *Legislaturbericht Digitale Agenda 2014–2017*. Berlin: Bundesministerium des Innern et al.
- Danyel, Jürgen. 2012. Zeitgeschichte der Informationsgesellschaft. *Zeithistorische Forschungen* 9 (2): 186–211.
- Europäische Kommission, Hrsg. 2014. *Digitale Agenda für Europa. Neustart für die europäische Wirtschaft*. Luxemburg: Amt für Veröffentlichungen der Europäischen Union.
- Europäische Kommission, Hrsg. 2017. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über die

- Halbzeitüberprüfung der Strategie für einen digitalen Binnenmarkt. *Ein vernetzter digitaler Binnenmarkt für alle.* 10.05.2017 COM (2017) 228 final. Brüssel: Europäische Kommission.
- Europäische Kommission, Hrsg. 2018. *Index für die digitale Wirtschaft und Gesellschaft 2018. Länderbericht Deutschland.* Brüssel: Europäische Kommission. [https://ec.europa.eu/digital-single-market/en\(scoreboard/germany](https://ec.europa.eu/digital-single-market/en(scoreboard/germany).
- European Commission, Hrsg. 2011. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *Open data. An engine for innovation, growth and transparent governance.* 12.12.2011 COM (2011) 882 final. Brüssel: Europäische Kommission.
- European Commission, Hrsg. 2016. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *EU eGovernment Action Plan 2016–2020. Accelerating the digital transformation of government.* 19.04.2016 COM (2016) 179 final. Brüssel: Europäische Kommission.
- European Commission, Hrsg. 2018. *International Digital Economy and Society Index 2018.* Final report. Luxemburg: Europäische Kommission.
- European Commission, Hrsg. 2019. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).* Brüssel: Europäische Kommission. <https://eur-lex.europa.eu/eli/reg/2019/881/oj>.
- Rohen, Mechthild. 2014. *Public sector modernization through open government.* Brüssel: Präsentation.
- Roßnagel, Alexander. 2016. *Das Recht der Vertrauensdienste. Die eIDAS-Verordnung in der deutschen Rechtsordnung.* Baden-Baden: Nomos.
- Wewer, Göttrik. 2016. Faire Chancen für die kollaborative Wirtschaft? Neue Agenda der EU-Kommission. *Zeitschrift für Rechtspolitik* 49(7): 193–196.



---

# Diskurse der Digitalisierung und organisationaler Wandel in Ministerien

Maximilian Hösl, Florian Irgmaier und Ronja Kniep

## Inhalt

1	Begriffsklärung .....	384
2	Theoretische Grundlagen .....	385
3	Digitalisierung, öffentliche Diskurse und Organisationswandel .....	386
4	Das Bundesministerium des Innern .....	390
5	Perspektiven für Staat und Verwaltung .....	392
	Literatur .....	394

---

## Zusammenfassung

Mit der Digitalisierung verändert sich die Organisationsstruktur der Ministerialverwaltung. Dabei kann unterschieden werden zwischen digitalen Zuständigkeiten, die sich auf die Einführung digitaler Technologien in der Verwaltung beziehen, und digitalpolitischen Zuständigkeiten, bei denen es um die politische Gestaltung der digitalen Transformation geht. Anhand von Organigramm-Historien lässt sich der Aufbau und Wandel operativer und strategischer Zuständigkeiten in den Bundesministerien zwischen 1995 und 2016 rekonstruieren und auf diskursive und verwaltungsspezifische Faktoren zurückführen.

---

## Schlüsselwörter

Organisationswandel · Cybersicherheit · Digitalpolitik · Netzpolitik · Diskursiver Institutionalismus

---

M. Hösl (✉) · R. Kniep  
Wissenschaftszentrum Berlin für Sozialforschung, Berlin, Deutschland  
E-Mail: [maximilian.hoesl@wzb.eu](mailto:maximilian.hoesl@wzb.eu); [ronja.kniep@wzb.eu](mailto:ronja.kniep@wzb.eu)

F. Irgmaier  
Weizenbaum-Institut für die vernetzte Gesellschaft/Wissenschaftszentrum Berlin für Sozialforschung, Berlin, Deutschland  
E-Mail: [florian.irgmaier@wzb.eu](mailto:florian.irgmaier@wzb.eu)

## 1 Begriffsklärung

Mit der Digitalisierung verändert sich nicht nur das Instrumentarium, das Staat und Verwaltung für die Bewältigung ihrer Aufgaben nutzen können. Auch Staat und Verwaltung selbst verändern sich, indem sie einerseits digitale Instrumente einsetzen und andererseits den gesellschaftlichen Prozess der Digitalisierung zu gestalten versuchen.

Von besonderer Tragweite ist diese Veränderung in der *Ministerialverwaltung* des Bundes. Sie ist der hierarchisch höchstgestellte Teil des staatlichen Verwaltungsapparates und erfüllt Funktionen der Information (Bereitstellung von Wissen), der Programmerarbeitung (z. B. Gesetzesformulierung), des Vollzugs (Ausführung von Regeln) und der Koordination (Abstimmung zwischen Ministerien bzw. zwischen Ministerium und nachgeordneten Behörden). Ihre kleinsten regulären Organisationseinheiten bilden thematisch spezialisierte Referate, die meist in Unterabteilungen zusammengefasst werden, welche wiederum zu Abteilungen gehören (vgl. Machura 2013). Neben diesen dauerhaften Einheiten existieren auch temporäre Stäbe, Projekt- oder Arbeitsgruppen, die zur Bearbeitung zeitlich begrenzter bzw. querschnittlicher Aufgaben etabliert und mittelfristig entweder aufgelöst oder in die Linienorganisation integriert werden.

Die Organisationsstruktur bestimmt maßgeblich die Art und Weise, in der Ministerien ihre Aufgaben wahrnehmen. Insofern sind die wiederkehrenden Debatten um ein Internet- bzw. Digitalministerium nicht trivial. Besonders in den Bundestagswahlkämpfen 2013 und 2017 spielte die Frage, wie stark *digitalpolitische* Zuständigkeiten innerhalb der Bundesregierung zentralisiert werden sollten, eine gewichtige Rolle. Während Befürworter\*innen eines eigenständigen Digitalministeriums die Notwendigkeit zentraler Koordination betonen, argumentieren Gegner\*innen, dass die Digitalisierung alle Lebensbereiche betreffe und sich deshalb jedes Ministerium mit diesem Thema beschäftigen müsse. Nach der Wahl 2017 mündete die Debatte in einen vorläufigen Kompromiss: die Einsetzung einer Staatsministerin für Digitalisierung im Bundeskanzleramt.

Mit „Digitalisierung“ ist der gesellschaftliche Transformationsprozess gemeint, der mit der Entwicklung, Verbreitung und praktischen Aneignung digitaler Technologien zur Informationsverarbeitung und Kommunikation einhergeht. Staat und Verwaltung haben mit dieser Transformation auf zwei Arten zu tun. Erstens lässt sich eine *operative Digitalisierung* des Staates beobachten, d. h. ein zunehmender Einsatz digitaler Technologien für die Erfüllung staatlicher Aufgaben – einschließlich der Bereitstellung von Dienstleistungen in elektronischer Form (*E-Government*) – und die Unterstützung der internen staatlichen Verwaltung. Die mit der operativen Digitalisierung befassten Einheiten werden im Folgenden als digitale Zuständigkeiten bezeichnet. Ministerien bauen solche digitalen Zuständigkeiten auf, um die Erfüllung ihrer Funktionen informationstechnisch zu unterstützen und Aufbau, Betrieb und Pflege der erforderlichen technischen Systeme zu gewährleisten. In der Regel handelt es sich um eigene Organisationseinheiten – so verfügt jedes Bundesministerium über mindestens ein Referat zur Betreuung der hausinternen Informationstechnik (IT).

Zweitens versucht der Staat, die digitale Transformation in eine gesellschaftlich wünschenswerte Richtung zu lenken (*strategische Digitalisierung*). Organisationseinheiten, die an dieser politischen Gestaltung mitwirken, werden im Folgenden *digitalpolitische Zuständigkeiten* genannt. Sie sind nicht primär mit der Bereitstellung der Mittel befasst, mit denen Verwaltung arbeitet, sondern mit einem eigenständigen Aufgabenbereich staatlicher Lenkung – vergleichbar mit traditionellen Politikfeldern wie Wirtschaft oder Gesundheit. Auch diese Aufgaben werden in Ministerien durch spezialisierte Organisationseinheiten mit eigener Expertise wahrgenommen. Beispiele sind die Abteilung *Digital- und Innovationspolitik* im Bundesministerium für Wirtschaft und Energie (BMWi), die Abteilung *Digitale Gesellschaft; Verwaltungsdigitalisierung und Informationstechnik* im Bundesministerium des Innern, für Bau und Heimat (BMI) oder die Abteilung *Digitale Gesellschaft* im Bundesministerium für Verkehr und digitale Infrastruktur (BMVI). Innerhalb dieser Abteilungen sind die Grundsatzreferate in besonderem Maße auf politisch-strategische Arbeit ausgelegt.

Freilich sind sowohl digitale als auch digitalpolitische Zuständigkeiten politisch in dem Sinne, dass beide an der Herstellung gesellschaftlicher Ordnung mitwirken. Digitalpolitische Zuständigkeiten sind jedoch in einem weiteren Sinne politisch: Sie werden aufgebaut, um an der Formulierung politischer Programme mitzuwirken, und konkurrieren mit anderen staatlichen wie nichtstaatlichen Akteuren um Deutungshoheit und Ressourcen für die Bearbeitung ihres Themenfeldes. Beide Varianten von Digitalisierung finden sich in der Ministerialverwaltung.

---

## 2 Theoretische Grundlagen

Der Aufbau digitaler und digitalpolitischer Zuständigkeiten in den Ministerien ist eine Form organisationalen Wandels. Zur Analyse und Erklärung dieses Wandels haben die Sozialwissenschaften verschiedene theoretische Ansätze entwickelt, die jeweils unterschiedliche Faktoren als ausschlaggebend erachten. Unter dem Schlagwort des *diskursiven Institutionalismus* heben jüngere Ansätze die Bedeutung spezifischer Weltsichten für organisationalen Wandel hervor (Schmidt 2010; Pohle et al. 2016). Institutionen, und daher auch Organisationen, gelten hier als verstetigte Diskurse. Das heißt, dass Diskurse, verstanden als Ensembles von Ideen, Konzepten, *Frames* und Definitionen (Hajer 1995), sich in Gestalt spezifischer Aufgabenbereiche und Problemlösungsansätze in Organisationen niederschlagen. Gerade im Kontext der Digitalisierung ist diese Perspektive instruktiv, da sie über technikdeterministische Erklärungen hinausgeht. Die strategische Digitalisierung der Ministerien ist nicht das Produkt unmittelbarer Anpassung an technische Gegebenheiten, sondern ein Ergebnis der Aushandlungsprozesse über die Deutung der Digitalisierung: Stehen z. B. sicherheits-, wirtschafts- oder kommunikationspolitische Fragen im Vordergrund? Daher unterscheiden sich die Zugriffe auf das Thema sowohl im Zeitverlauf als auch im Vergleich zwischen Ministerien.

Der digitale und digitalpolitische Wandel der Ministerien lässt sich anhand von Organigramm-Historien rekonstruieren. Organigramme bilden die formalen Struk-

turen der Ministerien ab und signalisieren intern wie extern, wer für welche Aufgaben zuständig ist. Eine chronologische Aneinanderreihung einzelner Organigramme desselben Ministeriums erlaubt Rückschlüsse auf historische Entwicklungen. Auf diese Weise kann der digitale und digitalpolitische Wandel der Ministerialverwaltung quantitativ und qualitativ nachvollzogen werden (Pohle et al. 2016).

Der quantitative Wandel betrifft Veränderungen in der Anzahl von Organisationseinheiten, die für ein Thema zuständig sind. Diese Anzahl entspricht der relativen Bedeutung des Themas innerhalb der Ministerien, da in Organisationen stets um die Verteilung knapper Mittel gerungen wird und Einheiten, die als obsolet erachtet werden, früher oder später aufgelöst werden. Eine besondere Relevanzzuschreibung liegt vor, wenn nicht nur ein spezialisiertes Referat, sondern eine Abteilung oder sogar ein eigenes Ministerium geschaffen wird. Quantitative Veränderungen deuten auch an, wie sich die gesellschaftliche Bedeutung von Themen entwickelt, weil Ministerien auf Debatten in der Fachwelt und in der Öffentlichkeit reagieren.

Der qualitative Wandel der digitalen und insbesondere der digitalpolitischen Zuständigkeiten innerhalb der Ministerien lässt sich an den Namen der Organisationseinheiten ablesen. Namen erlauben nicht nur Rückschlüsse auf das Thema, das eine Einheit bearbeitet, sondern auch auf die dort vorherrschende Sichtweise auf dieses Thema. Organisationseinheiten wählen ihre Namen, in Abstimmung mit der Hausleitung, mit Bedacht aus, um inner- und außerhalb ihres Hauses Zuständigkeit und Sachkenntnis zu signalisieren. Sie greifen dabei gesellschaftlich dominante Diskurse auf, führen aber auch gezielt neue Begrifflichkeiten ein. Veränderungen der Namen von Referaten oder Abteilungen zeigen, wie sich die Sichtweisen auf die Digitalisierung im Zeitverlauf wandeln.

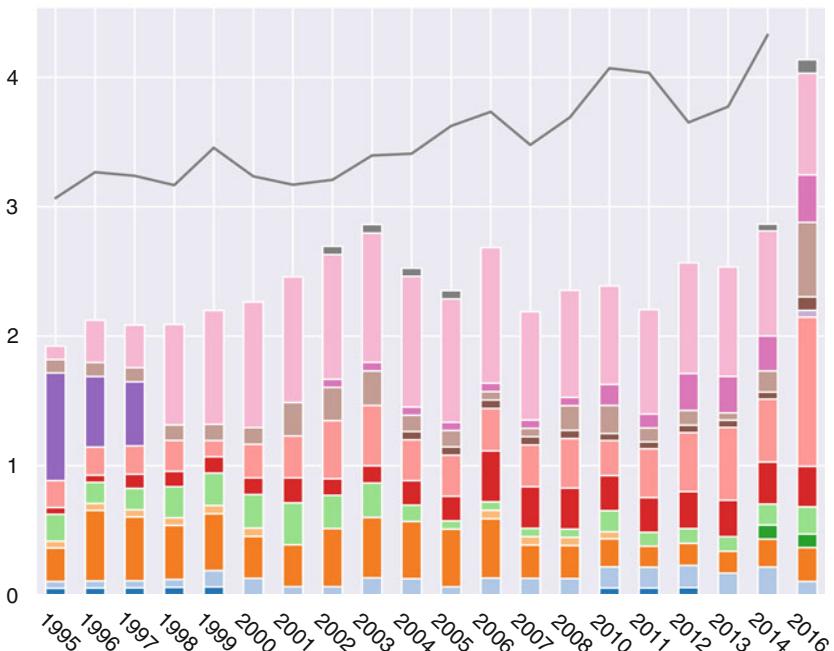
---

### 3 Digitalisierung, öffentliche Diskurse und Organisationswandel

Eine Analyse der Organigramme der Bundesministerien von 1995 bis 2016 zeigt den Auf- und Abbau von Organisationseinheiten und den Wandel der Bezeichnungen von Zuständigkeiten (Abb. 1 und 2). Im Abgleich mit der Entwicklung solcher Bezeichnungen in der Medienöffentlichkeit wird zudem die Beziehung zwischen öffentlichen Diskursen und Organisationsentwicklung deutlich. Drei Ministerien spielen dabei eine hervorgehobene Rolle: Das BMI, das BMWi und das Bundesministerium für Bildung und Forschung (BMBF). Die Entwicklung lässt sich in drei Phasen einteilen.

In der ersten Phase (1995–2003) bauten die Ministerien vor dem Hintergrund des Diskurses zur Informationsgesellschaft digitalpolitische Zuständigkeiten aus. Der Anteil einschlägiger Einheiten an der Gesamtzahl in den Ministerien stieg 2003 auf 2,9 %. Semantisch dominierten in dieser Phase Begriffe, die sich auf *Telekommunikation* (TK) und *Informations- und Kommunikationstechnologie* (IuK) beziehen. Letztere nahmen kontinuierlich zu. Die dominante Semantik korrespondiert mit einer Hochkonjunktur entsprechender Begriffe in der Medienöffentlichkeit, die Anfang der 2000er-Jahre wieder einbrach (DWDS 2018). Dies gilt auch für den

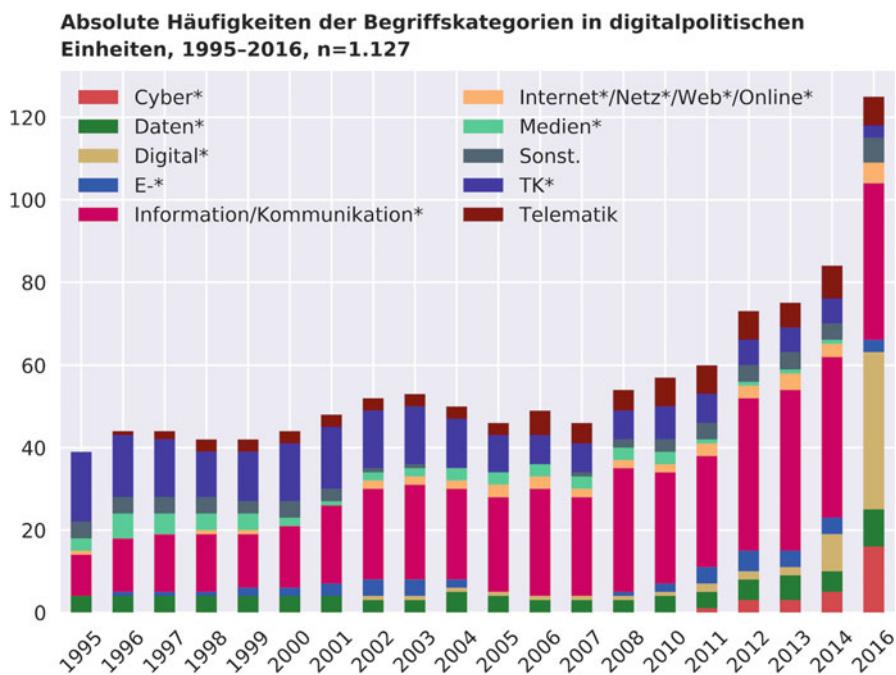
**Anteil digitalpolitischer (Säulen) und digitaler Zuständigkeiten  
an Ministerialbürokratie, in Prozent, 1995–2016, n=33.222**



**Abb. 1** Entwicklung digitalpolitischer Zuständigkeiten in den Ministerien. (Quelle: Eigene Erhebung auf Basis der Publikationen *Bund transparent* und *Staatshandbuch*; für 2009 und 2015 liegen keine Daten vor, für 2016 liegen nicht alle notwendigen Daten zu operativen Einheiten vor)

stärker politisch-programmatischen Begriff *Informationsgesellschaft*, den Ministerien in dieser Phase nutzten. Hürden der technologischen Entwicklung seien auszuräumen, um das ökonomische Potential der Informationsgesellschaft auszuschöpfen (vgl. Pohle et al. 2016). Diesen durch internationale Akteure getriebenen Diskurs gestalteten die Ministerien ab Mitte der 1990er-Jahre mit.

Vor allem das BMBF und das BMWi prägten diese Phase. Sie vereinten gemeinsam im Zeitraum 1995–2003 durchschnittlich 47,8 % der digitalpolitischen Einheiten auf sich. Das BMBF verfügte schon 1995 über eine Unterabteilung mit forschungspolitischen Zuständigkeiten für IT. Ab 1995 wurden diese auf Initiative des damaligen Ministers um Zuständigkeiten für *Multimedia* und *Informationsgesell-*



**Abb. 2** Begriffskonjunkturen in den Ministerien. (Quelle: Eigene Erhebung auf Basis der Publikationen *Bund transparent* und *Staatshandbuch*)

schaft ergänzt. Der Diskurs zur Informationsgesellschaft schlug sich auch in temporären Beratungsgremien der Bundesregierung nieder, an denen das BMBF, das BMI, das BMWi und das Bundesministerium für Post und Telekommunikation (BMPT) beteiligt waren. Nach dem Regierungswechsel 1998 übertrug die Bundesregierung die neuen Zuständigkeiten des BMBF an das BMWi, wo diese mit den ebenfalls seit 1995 angesiedelten Aufgaben für die *Informationsgesellschaft* in einer Unterabteilung zusammengeführt wurden. Auch Zuständigkeiten des BMPT wurden in das BMWi verschoben, als das BMPT 1997 im Zuge der Liberalisierung des Telekommunikationsmarktes aufgelöst wurde. Das BMI begann ab 2000, einschlägige Zuständigkeiten auszubauen, und verwies dabei ebenfalls auf die *Informationsgesellschaft*. Insgesamt überwog jedoch der *IT*-Begriff.

In der zweiten Phase (2004–2011) verankerten die Ministerien nur eingeschränkt politische Begriffe öffentlicher Diskurse in ihrer Organisation. Die Entwicklung digitalpolitischer Zuständigkeiten weist eine Delle auf. Der Anteil einschlägiger Einheiten in den Bundesministerien sank bis 2007 auf 2,2 %, stieg aber bis 2012 wieder auf 2,6 % an. *Telekommunikation* verlor an Popularität, während Begriffe mit *IuK*-Bezug weiterhin zunahmen. Die Medienöffentlichkeit nutzte beide Begriffe vergleichsweise wenig. Erst ab ca. 2008 stieg die öffentliche Aufmerksamkeit für digitale Themen mit dem zivilgesellschaftlich geprägten Begriff *Netzpolitik*, der mit Bürgerrechten, Transparenz und Bürgerbeteiligung assoziiert wurde, und dem

sicherheitspolitisch konnotierten Begriff *Cyber* erneut an (Hösl und Reiberg 2016; Hofmann und Kniep 2018). Obwohl die beiden Begriffe sich kaum bzw. nicht in Organisationseinheiten wiederfinden, entspricht die aggregierte Begriffskonjunktur in den Ministerien überwiegend dem Trend in der Medienöffentlichkeit.

Der Anteil des BMBF an den digitalpolitischen Einheiten nahm ab dieser Phase ab, während der des BMI stieg. Im Laufe dieses Zeitraums dominierten BMI und BMWi die digitalpolitischen Zuständigkeiten mit einem Anteil von 62,9 % der einschlägigen Einheiten im Jahre 2011. Auf der semantischen Ebene wurden weder *Cyber* noch *Netzpolitik* stärker in den Ministerien verankert. Einzig das BMI nutzte *Netzpolitik*, zeitlich etwas versetzt zur Konjunktur in der Medienöffentlichkeit, gab den Begriff jedoch 2014 wieder auf.

In der dritten Phase (2012–2016) bauten die Ministerien unter dem Eindruck von Cyber- und Digitalisierungsdiskursen ihre digitalpolitischen Zuständigkeiten aus. Deren Anteil in den Ministerien wuchs stark an – von 2,6 % auf 4,2 %. Entsprechend stieg auch die Signalisierung von Zuständigkeit durch einschlägige Begriffe, ein starker semantischer Wandel setzte ein. Zwar wurden zunächst Begriffe mit *IuK*-Bezug öfter genutzt, ab 2012 verwendeten die Ministerien aber vermehrt *Cyber* und *Digital* für ihre digitalpolitischen Zuständigkeiten – vor allem nach 2014. Dieser Trend deckt sich mit der stark ansteigenden Verwendung dieser Schlagwörter in der Öffentlichkeit, die dort entweder mit Sicherheitsaspekten (*Cyber*) oder mit Wirtschaft und Arbeit (*Digitalisierung*) assoziiert werden (Hofmann und Kniep 2018). *Cyber* wurde zeitversetzt zur öffentlichen Konjunktur in den Ressorts verankert (insb. BMI, BMVg, AA), *Digitalisierung* dagegen eher zeitgleich. Im Wahlkampf 2013 und in der folgenden Regierungsbildung war *Digitalisierung* ein bedeutendes Thema. Spätestens mit der *Digitalen Agenda 2014–2017* trugen alle Ministerien zu diesem Diskurs bei. Entsprechend hat sich ihre Semantik an den Begriff des *Digitalen* angepasst, vor allem in den federführenden Ministerien der Agenda: BMI, BMWi und BMVI. Sie vereinten 2016 64 % aller digitalpolitischen Einheiten in den Bundesministerien auf sich.

Der Anteil des BMI an den digitalpolitischen Zuständigkeiten nahm in der dritten Phase weiter zu. 2015 wurden dort neue Stäbe für *Cybersicherheit* eingerichtet. 2016 hatte es mit 29,3 % den größten Anteil an den digitalpolitischen Zuständigkeiten aller Ressorts. Das BMWi baute in dieser Phase seine bestehende Abteilung mit *IuK*-Bezug zur Abteilung *Digital- und Innovationspolitik* um. Die Anzahl digitalpolitischer Einheiten blieb stabil, ihr Anteil an der Gesamtzahl nahm jedoch ab (20 % 2016), da letztere insgesamt anstieg. Mit der Regierungsbildung 2013 wurde die Einrichtung einer Abteilung *Digitale Gesellschaft* im BMVI beschlossen und zwei Jahre später realisiert. Das Ministerium hatte 2016 einen Anteil von 14,7 % an den digitalpolitischen Zuständigkeiten aller Ressorts.

Insgesamt sind fünf Entwicklungen festzuhalten: (1) Die Zahl der digitalen Zuständigkeiten übersteigt die der digitalpolitischen, der Anteil letzterer wuchs jedoch von 1,9 % (1995) auf 4,2 % (2016). (2) Die Zuständigkeiten sind von Beginn an über mehrere Ministerien verteilt, insbesondere nach 2014. Jedoch dominieren bestimmte Ministerien einzelne Phasen: Während die wirtschaftspolitische Perspektive auf die digitale Transformation (BMWi) bis heute zentral ist, wurde die for-

schungspolitische Sichtweise (BMBF) geschwächt und die innenpolitische (BMI) gestärkt. (3) Zuständigkeit wurde anfangs eher durch Begriffe signalisiert, die sich auf *Telekommunikation* oder *IuK* bezogen. Die dritte Phase markiert einen semantischen Wandel hin zu *Cyber* und *Digitalisierung*. (4) Die identifizierten Phasen entsprechen weitgehend den öffentlichen Diskursen und ihrer Konjunktur. Sie markieren Zeiträume, in denen über die digitale Transformation verstärkt in Begriffen mit politischem Anspruch diskutiert wurde: *Informationsgesellschaft* (1990er), *Netzpolitik* (2006–2013), *Cyber* (ab 2006) und *Digitalisierung* (ab 2013) (Hofmann und Kniep 2018). (5) Die Ministerien verankerten einschlägige Begriffe in den 1990er-Jahren vor ihrer jeweiligen medialen Hochkonjunktur, nach 2012 aber verzögert dazu. So waren sie auf nationaler Ebene zunächst „Diskurstreiber“, vollzogen aber zuletzt eher eine nachholende Institutionalisierung öffentlicher Diskurse.

---

## 4 Das Bundesministerium des Innern

Um das Verhältnis von Digitalisierungsdiskursen und dem Wandel der Ministerialverwaltung auszuleuchten, wird die quantitative Perspektive durch einen qualitativen Blick auf das BMI ergänzt. Dieser Fall lohnt sich aus zwei Gründen. Erstens zeigt die quantitative Analyse, dass das BMI vergleichsweise früh vergleichsweise viele digital(politisch)e Zuständigkeiten aufgebaut hat. Zweitens spielt das BMI eine zentrale Rolle bei der operativen Digitalisierung der gesamten Bundesverwaltung. Es ist nicht nur für die eigene digitale Handlungsfähigkeit und Sicherheit zuständig, sondern auch für die IT-Strategie der gesamten Regierung. Diese zentrale Rolle ist keine Selbstverständlichkeit. In anderen Ländern, etwa Dänemark oder Australien, kommen vergleichbare Aufgaben dem Finanzministerium zu.

Doch was prägte die Entstehung und den Wandel digitaler und digitalpolitischer Zuständigkeiten im BMI? Zusammenfassend lässt sich sagen, dass internationale und öffentlichkeitswirksame Diskurse die Wahrnehmung von Risiken und damit den Aufbau organisationaler Strukturen genauso beeinflussen wie veränderte Praktiken im Bereich IT-Sicherheit und digitale Überwachung. Aber auch Konkurrenz und Konflikte zwischen Abteilungen, Ministerien oder Bund und Ländern sowie (partei-)politische Prioritäten von Minister\*innen sind ausschlaggebend für organisationale Veränderungen. Für alle diese Handlungslogiken lassen sich in der Organigramm-Historie des BMI Beispiele finden.

Den Beginn eigenständiger digitalpolitischer Zuständigkeiten markierten IT-Sicherheitsdiskurse, die seit 1999 aus der Fachöffentlichkeit in Politik und Öffentlichkeit getragen wurden. Um das sogenannte Jahr-2000-Problem, die Umstellung aller Computer von 99 auf 00, entstanden teils apokalyptische Katastrophenszenarien zu IT-Ausfällen, auf die sich das BMI durch einen Krisenstab und eine vorbereitete Notstandsverordnung einzustellen versuchte. Die Wahrnehmung einer Bedrohung setzte voraus, dass die operative Digitalisierung einen bestimmten Verbreitungsgrad erreicht hatte und damit Abhängigkeiten für die staatliche Handlungsfähigkeit erzeugte, etwa im Polizeibereich. Vor allem aber ist das Jahr-2000-Problem ein prägnantes Beispiel für die materiellen Effekte von Diskursen. Zwar blieben die

befürchteten Systemausfälle aus, aber das entstandene Bewusstsein für solche Risiken war mit ausschlaggebend für die Gründung eines eigenen *IT-Stabes* im BMI 2002. Unterstützt wurde die Gründung durch Versuche der Regierung, andere Staaten im Bereich *E-Government* einzuholen.

Bestehende Zuständigkeiten wurden dabei aus anderen Abteilungen (*Öffentliche Sicherheit, Verwaltungsmobilisierung*) herausgelöst und zu „reinen“ IT-Themen gebündelt. Solche Neuerungen bergen Konfliktpotential mit etablierten Strukturen. Der IT-Stab, der 2005 zu einer Abteilung wurde, trat in einen für digitale Netze spezifischen Konflikt mit der Abteilung *Öffentliche Sicherheit*. Mit der Abgrenzung reiner IT-Themen in der *IT-Abteilung* von den digitalen Zuständigkeiten für Sicherheitsbehörden hat sich eine zentrale Konfliktlinie zwischen Digitalpolitik und Sicherheitspolitik institutionalisiert: zwischen dem Schutz digitaler Netze und der Befähigung staatlicher Akteure, auf Daten in diesen Netzen zuzugreifen.

Bekannt ist dieser Konflikt spätestens seit den „Krypto-Debatten“ – den politischen Diskussionen über das Verbot von Kryptographie und über staatliche Hinter türen in kryptographischen Technologien, die bereits in den 1990ern geführt wurden. Dieser Konflikt ist also nicht BMI-spezifisch oder spezifisch für den deutschen Fall, ist aber in anderen Ländern anders institutionalisiert. Die aufbauorganisatorische Spiegelung des Krypto-Konflikts zwischen zwei Abteilungen im selben Haus prägte die Weiterentwicklung der Organisationsstrukturen. Mit der *Digitalen Agenda* wurden dann die Zuständigkeiten beider Abteilungen ausgebaut. Den Hintergrund bildeten Debatten zu den Überwachungsfähigkeiten des US-Geheimdienstes *National Security Agency* (NSA), aber auch Terrorismus-Debatten, in denen sowohl ein erhöhter Schutz von Netzen als auch erhöhte Überwachungskapazitäten begründbar wurden. Veränderungen der Organisationsstrukturen in den zwei Abteilungen *IT* und *Öffentliche Sicherheit* können auch als Aushandlung oder Kräfteverschiebung im Konflikt zwischen dem Schutz von IT und dem Schutz der Eingriffsfähigkeit in IT interpretiert werden.

In Organigramm-Historien lässt sich neben dem Wandel von Organisationsstrukturen auch der semantische Wandel beobachten, d. h. der Wandel von Begriffen und Deutungen der digitalen Transformation. Der Begriff *Digitalisierung*, der heute gängig erscheint und auch benutzt wird, um Anschlussfähigkeit herzustellen, wird erst seit den 2010er-Jahren vermehrt von Unternehmen, Öffentlichkeit, Verwaltung und Politik verwendet. Bedeutend sind solche semantischen Veränderungen, weil mit der Wahl von Begriffen je unterschiedliche Phänomene, Themen und Akteure hervorgehoben oder marginalisiert werden.

Im BMI zeigt sich ein Wandel von den Begriffen *Informationsgesellschaft* und *IT* zu *Digital* und *Cyber*. *Cyber* hatte in seiner Geschichte schon diverse Bedeutungen: vom altgriechischen *kybernetes*, dem Steuermann, und der lateinischen *gubernatio* (Regierung) über die Kybernetik als Wissenschaft von Kommunikation und Steuerung, hin zur Raummetapher für das Internet (*Cyberspace*) und zum Science-Fiction-Genre (*Cyberpunk*). Seit Ende der 2000er-Jahre ist *Cyber* in Deutschland vor allem sicherheitspolitisch aufgeladen. Das zeigt sich auch an den Namen von Organisationseinheiten im BMI, besonders ab 2014. In der Wahrnehmung der Akteure erzeugt *Cyber* mehr politische Aufmerksamkeit und Anschlussfähigkeit

als *IT*. Die semantische Verschiebung von *IT* zu *Cyber* spiegelt z. T. auch den Wandel von operativen zu strategischen, digitalpolitischen Kompetenzen wider.

Erhellend ist auch, welche Begriffe sich nicht durchsetzen konnten. Dazu gehört *Netzpolitik*. Der Begriff hatte ab ca. 2008 Konjunktur und wurde besonders von Opposition, Zivilgesellschaft und Medien geprägt, schließlich aber auch von Teilen der Regierung und Verwaltung übernommen – jedoch nicht längerfristig. Das Aufgreifen des Begriffs im BMI durch eine abteilungsübergreifende Projektgruppe *Netzpolitik* im Jahr 2009 erfolgte aus dem politischen Impuls des Ministers Thomas de Maizière: Es galt zu zeigen, dass auch das BMI den Schutz von Freiheit und Grundrechten von Bürger\*innen im Internet ernst nehme, nicht nur sicherheitspolitische Kontrollansprüche. Damit sollte vermieden werden, digitalpolitisch in die Fußstapfen von Wolfgang Schäuble zu treten, der in der netzpolitischen Bewegung mit dem Image einer „Stasi 2.0“ versehen wurde. Im Gegensatz zum IT-Stab konnte sich die Projektgruppe *Netzpolitik* nicht dauerhaft in der Struktur des Hauses verankern; sie wurde 2011 aufgelöst. Seit 2014 ist der Begriff aus den Organigrammen des BMI verschwunden.

Im BMI entwickelte sich also ein operativer Stab (2002) relativ schnell zu einer auch digitalpolitischen Organisationseinheit, die schließlich zur zweitgrößten Abteilung anwuchs (2005). Statt die Themen in einer Abteilung zu bündeln, hätte man ihre Bearbeitung auch auf verschiedene Einheiten verteilen können. Abteilungen gelten als relativ abgeschottete „Türme“ mit je eigenen *Communities*, zu denen Vertreter\*innen von Verbänden, NGOs oder Wissenschaft gehören. Mit einer Abteilung entsteht ein Anspruch, den jeweiligen Bereich selbst zu verantworten, sowie ein Denken in den eigenen Zuständigkeiten. Mit der Abteilung *IT* entwickelte sich, neben dem sicherheitspolitischen Denken, auch eine bestimmte digitalpolitische Denkweise im BMI.

Insgesamt lässt sich eine Zunahme digitalpolitischer Zuständigkeiten im BMI beobachten. Die frühe Integration operativer Digitalisierung in bestimmte Handlungsfelder des Hauses schaffte die Grundlage für strategische Zuständigkeiten. Die Leitung der IT-Abteilung trug gewissermaßen „zwei Hüte“: einen für die strategische und einen für die operative Digitalisierung. Operative Zuständigkeiten sind gewöhnlich nachgeordneten Behörden zugeordnet. Wird ihr Anteil gegenüber den strategischen Zuständigkeiten zu groß, findet in der Regel eine Auslagerung in diese Behörden statt, damit genügend Raum für Strategieentwicklung bleibt, die Ministerien als ihre Kernaufgabe ansehen.

---

## 5 Perspektiven für Staat und Verwaltung

Die Entwicklung digitalpolitischer Zuständigkeiten in den Bundesministerien wurde von einem Zusammenspiel von etablierten Organisationsprinzipien und verschiedenen Digitalisierungsdiskursen geprägt. Sofern diese Mechanismen auch in Zukunft wirken, sind Aussagen über wahrscheinliche künftige Entwicklungen möglich.

Denkbar sind sowohl eine stärkere Zentralisierung als auch eine stärkere Dezentralisierung. Beispiele einer stärkeren Zentralisierung digitalpolitischer Zuständig-

keiten, d. h. ihrer Bündelung in spezialisierten Organisationen, finden sich in den Bundesländern (z. B. NRW), in anderen Staaten (*Department for Digital, Media, Culture & Sports*, UK) und auf EU-Ebene mit der Generaldirektion CONNECT, einer Art Digitalministerium. Sie zeigen, dass der Grad der Fragmentierung von Zuständigkeiten weder selbstverständlich noch dem Charakter digitaler Technologien selbst geschuldet ist. Dass die Einrichtung spezialisierter Ministerien durch die Zusammenführung zuvor verteilter Organisationseinheiten auch auf Bundesebene möglich ist, belegt u. a. das 1986 gegründete Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit (Derlien 1996). Mehrere Faktoren fördern eine digitalpolitische Zentralisierung auf Bundesebene, darunter die hohe Bedeutung der Digitalisierung in öffentlichen Diskursen sowie der in Medien- und Fachöffentlichkeit wahrgenommene Koordinations- und Strategiebedarf. Auch parteipolitische Erwägungen können die Gründung eines eigenständigen Digitalministeriums unterstützen – etwa wenn in einer Regierungskoalition Ministerposten proportional verteilt werden sollen oder sich bestimmte Regierungsmitglieder mit einem öffentlichkeitswirksamen Zukunftsthema als „Digitalminister\*in“ profilieren wollen.

Allerdings wirken andere Faktoren einer Zentralisierung digitalpolitischer Kompetenzen entgegen und lassen erwarten, dass die dezentrale Organisation beibehalten wird. So hemmt das Argument, Digitalpolitik sei ein Querschnittsthema und jedes Ministerium müsse über digitalpolitische Zuständigkeiten verfügen, eine stärkere Zentralisierung. Der Schaffung eines eigenständigen Ministeriums steht zudem entgegen, dass hierfür bereits etablierte digitalpolitische Zuständigkeiten aus Ministerien herausgelöst werden müssten, was aufgrund der Konkurrenz der Ministerien um Ressourcen und Zuständigkeiten schwer durchzusetzen ist. Ferner hemmen zu erwartende Kostenargumente und Präferenzen für eine handlungsfähige Kabinettsgröße sowie für ressortinterne Koordination und Konfliktregulierung die Zentralisierung in Form eines eigenen Ministeriums (Derlien 1996).

In diesem Spannungsfeld erscheint sowohl eine umfassende Zentralisierung als auch eine weitergehende Fragmentierung digitalpolitischer Zuständigkeiten unwahrscheinlich. Mittelwege, d. h. Koordinierungsinstanzen „unterhalb“ eines eigenständigen Ministeriums, werden dagegen wahrscheinlicher. Dazu gehört in der 19. Legislaturperiode die Position der Staatsministerin für Digitalisierung. Ebenfalls denkbar ist eine Zuständigkeitsbündelung in den nachgeordneten Bereichen der Ministerien, etwa in Gestalt der im Koalitionsvertrag von Union und SPD vorgesehenen „Digitalagentur“.

Mit einem baldigen Ende der Debatten um die „richtige“ Organisationsweise ist aufgrund der dauerhaften Relevanz, die der Digitalisierung von (Fach-)Öffentlichkeit, Staat und Verwaltung zugeschrieben wird, nicht zu rechnen. Profitieren kann die Diskussion durch – für die Digitalpolitik bislang fehlende – sozialwissenschaftliche Studien, die den Zusammenhang von Zuständigkeitsverteilung einerseits und *Policy*-Ergebnissen, Strategie- und Implementationsfähigkeit andererseits in den Blick nehmen. Solche Untersuchungen könnten, etwa durch internationale Vergleiche, Aufschluss darüber geben, welche Organisationsweise welche Digitalpolitik wahrscheinlich macht und weshalb.

## Literatur

- Derlien, Hans-Ulrich. 1996. Zur Logik und Politik des Ressortzuschnitts. *Verwaltungsarchiv* 87: 548–580.
- DWDS. 2018. Wortverlaufskurve für /Telekommunikation/i, /Telematik/i, /Informationstechnlog/i, /Informationsgesellschaft/i, /Netzpoliti/i, /Cyber/i, /Digitalisierung/i, erstellt durch das Digitale Wörterbuch der deutschen Sprache. <https://www.dwds.de/r/plot?view=2&corpus=zeitungen>. Zugegriffen am 21.11.2019.
- Hajer, Maarten A. 1995. *The politics of environmental discourse. Ecological modernization and the policy process*. Oxford: Oxford University Press.
- Hofmann, Jeanette, und Ronja Kniep. 2018. *Die Pop-Karriere der deutschen Netzpolitik. Eine Erfolgsgeschichte?* <https://www.youtube.com/watch?v=Id3t6U7qq08>. Zugegriffen am 18.11. 2019.
- Hösl, Maximilian, und Ronja Kniep. 2019. Auf den Spuren eines Politikfeldes. Die Institutionalisierung von Internetpolitik in der Ministerialverwaltung. *Berliner Journal für Soziologie*. (im Erscheinen).
- Hösl, Maximilian, und Abel Reiberg. 2016. Netzpolitik in statu nascendi. Eine Annäherung an Wegmarken der Politikfeldgenese. In *Text Mining in den Sozialwissenschaften. Grundlagen und Anwendungen zwischen qualitativer und quantitativer Diskursanalyse*, Hrsg. Matthias Lemke und Gregor Wiedemann, 315–342. Wiesbaden: Springer.
- Machura, Stefan. 2013. Ministerialbürokratie. In *Handwörterbuch des politischen Systems der Bundesrepublik Deutschland*, Hrsg. Uwe Andersen und Wichard Woyke, 453–456. Wiesbaden: Springer.
- Pohle, Julia, Maximilian Hösl, und Ronja Kniep. 2016. Analysing internet policy as a field of struggle. *Internet Policy Review* 5(3). <https://doi.org/10.14763/2016.3.412>.
- Schmidt, Vivien A. 2010. Taking ideas and discourse seriously. Explaining change through discursive institutionalism as the fourth ‚new institutionalism‘. *European Political Science Review* 2(1): 1–25.



# Digitalisierung der Ministerialverwaltung

Nadin Fromm und Stefanie Vedder

## Inhalt

1 Klärung der Begriffe .....	396
2 Theoretische Grundlagen .....	397
3 Institutionelle Rahmenbedingungen .....	399
4 Praktische Anwendungsfelder .....	400
5 Perspektiven für Staat und Verwaltung .....	402
Literatur .....	404

## Zusammenfassung

Die Digitalisierung erfasst auch die politisch planende und steuernde Ministerialverwaltung, die durch ausgeprägte traditionelle Strukturprinzipien gekennzeichnet ist. Aus einer Innenperspektive bieten digitale Anwendungen neue Möglichkeiten für Arbeitsstrukturen und Entscheidungsprozesse. Ausgewählte digitale Applikationen, die in den Ministerien des Bundes zum Einsatz kommen, können eventuell neue Handlungskorridore innerhalb sowie zwischen Ministerien und anderen Akteuren schaffen, Hierarchien abflachen und intra-/interministerielle Kommunikation verstärken.

## Schlüsselwörter

Weberianisches Bürokratiemodell · Strukturprinzipien · Negativkoordination · Verwaltungskultur · E-Government

---

N. Fromm (✉) · S. Vedder

Lehrstuhl für Public Management, Universität Kassel, Kassel, Deutschland  
E-Mail: [nfromm@uni-kassel.de](mailto:nfromm@uni-kassel.de); [Stefanie.Vedder@uni-kassel.de](mailto:Stefanie.Vedder@uni-kassel.de)

## 1 Klärung der Begriffe

Die Ministerien sind auf Bundesebene und in den sechzehn deutschen Bundesländern die obersten Verwaltungsbehörden, von denen aus die nachgeordneten Behörden im Geschäftsbereich der jeweiligen Fachressorts gesteuert werden. Als oberste Verwaltungsbehörden unterscheiden sich die Ministerien von den nachgeordneten Behörden darin, dass sie im funktionenverschränkenden System der Bundesrepublik Deutschland ein breites Aufgabenspektrum im Kreislauf politischer Entscheidungsfindung übernehmen. So beruhen die zur parlamentarischen Lesung und Abstimmung vorbereiteten Regierungsprogramme und Gesetzesentwürfe in der Regel auf Vorarbeiten der Ministerialverwaltung. Nach der Verabschiedung eines Entwurfes obliegt ihr durch den Erlass von Rechtsverordnungen die Operationalisierung der Maßnahmen, was der Ministerialverwaltung Ermessens- und Gestaltungsräume eröffnet. Die Ministerien sind der Direktive der/s jeweiligen Minister\*in als Leitung des Hauses unterstellt. Konkret legt die Gemeinsame Geschäftsordnung den rechtlichen Rahmen der Arbeit innerhalb der Ministerien bei der Vorbereitung von Gesetzentwürfen fest, regelt die Aufgabenverteilung zwischen den Ressorts und unterstützt so die Arbeit der Regierung.

Als zentraler Teil der staatlichen Exekutive hat die Ministerialverwaltung die Aufgabe, gesellschaftliche Entwicklungen zu erkennen und im Rahmen ihres gesetzlich vorgesehenen Aufgabenbereichs sowie auf Basis von Koalitionsvereinbarungen und Parlamentsbeschlüssen planend und steuernd zu handeln. Dazu bleibt sie über den Stand gesellschaftlicher Entwicklungen informiert, zieht Bilanz und verwendet ihre Erkenntnisse als Grundlage für Empfehlungen und Entwürfe. Die Anforderungen an die Ministerialverwaltung steigen dabei mit der Geschwindigkeit, Reichweite und Komplexität gesellschaftlicher Veränderungen und politischer Entscheidungen.

Abgesehen vom Kanzleramt und den Staats- und Senatskanzleien der Länder, in denen die Politik der Regierung und die föderale Zusammenarbeit koordiniert wird, gibt es im Bund derzeit 14 Ministerien (Stand Juli 2019) und in den Ländern jeweils zwischen sieben (Saarland) und zwölf Ressorts (Bayern). Die Ministerien bestehen aus Abteilungen und diese wiederum aus Referaten, die durch Stabstellen oder Arbeitsgruppen ergänzt werden.

Unter Digitalisierung der Ministerialverwaltung lässt sich Verschiedenes verstehen: Die technische Infrastruktur, die notwendig ist, um elektronisch zu arbeiten (Regierungsnetz, Intranet, Internet usw.), die technischen Geräte, die im täglichen Arbeitsablauf genutzt werden (Laptops, Tablets, Smartphones usw.), der elektronische *Workflow* (E-Mail, E-Akte, Dokumenten-Management-Systeme usw.), neue Formen digitaler Kommunikation (Soziale Medien usw.) und elektronische Dienstleistungen (*E-Government*), die sich gegenseitig ergänzen und Auswirkungen auf die Arbeit der Ministerialverwaltung zur Folge haben. Digitalisierung kann dementsprechend als der Prozess eines Wandels verstanden werden, „der durch Einführung digitaler Technologien, darauf aufbauender Anwendungssysteme und vor allem ihrer Vernetzung angestoßen wird“ (Hirsch-Kreinsen 2018, S. 16).

Hinsichtlich der Digitalisierung der Ministerialverwaltung ist die Frage zentral, ob die neuen Formen der elektronischen Vorgangsbearbeitung die Art und Weise

verändern, wie Ministerien grundsätzlich arbeiten. Digitalisierung hat das Potenzial, die (inter-)ministeriellen Strukturen zu modifizieren. So ist eine vereinfachte Koordination zwischen Ressorts, d. h. eine horizontale Steuerung statt starrer Silostrukturen, und ein Aufbrechen einer stark ausgeprägten vertikalen Arbeitsteilung und kleinteiliger Spezialisierung hin zu flacheren Hierarchien denkbar. Darüber hinaus kann Digitalisierung auch gefestigte Entscheidungsprozesse hin zu einem agileren, also stärker antizipierenden und initiativen Arbeiten verändern.

---

## 2 Theoretische Grundlagen

Die deutsche Ministerialverwaltung gilt als der Idealtypus des legalistisch geprägten *Weberianischen Bürokratiemodells* (Weber 2013) und ist bei der Erfüllung ihrer Aufgaben in der Form von Gesetzesvorbereitung, -ausführung und -evaluation durch die Strukturmerkmale der klaren Zuständigkeiten und der Arbeitsteilung, durch die Dokumentationspflicht sowie durch eine stark hierarchische Struktur und durch spezialisiertes Personal charakterisiert: Weisungen der Leitungsebene bestimmen die Rahmenbedingungen für die Tätigkeit der Arbeitsebene, die im Gegenzug Berichtspflichten gegenüber der Leitungsebene unterliegt. Die Kommunikation zwischen Ebenen, Arbeitseinheiten und Personen erfolgt traditionell auf stark formalisierten, klar geregelten und aktenmäßig nachprüfbares (Dienst-)Wegen. Dies gilt analog auch für die Kommunikation und Koordination zwischen mehreren Abteilungen oder Referaten (intraorganisatorisch) und unterschiedlichen Ressorts (interorganisatorisch), die an der Ausarbeitung komplexer Gesetzesvorhaben beteiligt sind. Eine Entscheidung, die auf die Mitwirkung vieler Akteure angewiesen ist, gestaltet sich oftmals langwierig. Sie ist darauf angewiesen, dass relevante Informationen für alle Beteiligten zu jedem Zeitpunkt vollumfänglich verfügbar sind, was nicht immer leicht umsetzbar ist. Eine übergreifende Kommunikation findet im Rahmen der Vorbereitung eines Gesetzesentwurfs zumeist erst in einem sehr späten Stadium und dann in Form einer *Negativkoordination* statt, also als Minimalkonsens der involvierten Abteilungen und Referate.

Die deutsche Ministerialverwaltung wird häufig dahingehend kritisiert, sie bearbeite drängende politische Fragen verzögert. Bei einer Konfrontation mit externen Veränderungen agiere sie kurzsichtig und wenig nachhaltig. Ihr Handeln gilt als inkrementalistisch, also als langwierig und kleinschrittig, und als reaktiv, wonach sie im Sinne einer vorausschauenden Politik kaum initiativ oder innovativ tätig würde. Insgesamt gilt die Ministerialverwaltung als eher reformresistent. Gerade Reformen, die auf die Modifikation tradierter Strukturen abzielen, um etwa die Koordinationsleistung der Ministerialverwaltung zu verbessern, stoßen intern häufig auf Hindernisse oder sogar eine aktive Ablehnung. Die deutsche Ministerialverwaltung zeichnet sich also durch eine hohe strukturelle und prozessuale Kontinuität aus und bleibt in ihrer Kultur verhaftet.

Unter der „Kultur“ einer Organisation werden allgemein sowohl die aktiven Handlungsmuster der Kulturträger – also der Mitglieder der Organisation – als auch die dahinterliegenden Einstellungen und Werte verstanden. Die Kultur einer Orga-

nisation drückt damit ihre „Systemrationalität“ (König 2014) aus, die auch ihre Entscheidungen beeinflusst. Sie resultiert aus einer eingespielten Praxis, die von den Kulturträger\*innen in ihrer täglichen Arbeit als selbstverständlich hingenommen wird. Durch ihr Handeln bedingen die Kulturträger\*innen also die Strukturen und Arbeitsprozesse einer Organisation. Sie können diese sowohl perpetuieren und verfestigen als auch – insbesondere in leitenden Positionen – auf eine individuelle Initiative hin aktiv verändern.

Auch wenn sich die Anzahl der Ministerien und ihr Themenzuschnitt je nach Legislaturperiode verändern können, weist die Arbeitsweise der Ministerien eine hohe Kontinuität auf. Die „ministeriale“ *Verwaltungskultur* lässt sich bis ins 19. Jahrhundert zurückverfolgen. Sie zeichnet sich traditionell durch eine gewisse Autonomie gegenüber der jeweiligen Minister\*in und auch gegenüber dem Parlament aus, da „Politikereliten und Politikmoden viel rascherem Wechsel unterworfen sind“ (Patzelt 2008, S. 116). So hat sich im Zeitverlauf eine spezifische Mischung aus formalen Richtlinien und informellen Spielregeln herausgebildet, die eine Stabilität von Arbeitsroutinen gewährleisten. Das betrifft sowohl das Personal, das sich größtenteils aus Laufbahnbeamten zusammensetzt, als auch die Arbeitsweise, die auf besonderen Grundsätzen beruht. Die daraus resultierende Systemrationalität wirkt sich auch auf das Rollenverständnis und das Entscheidungsverhalten der Kulturträger aus (Hill 2014, S. 125).

Da sich das Umfeld, in dem Ministerialverwaltungen arbeiten, ständig verändert, stehen sie immer vor der Herausforderung, auf politische und gesellschaftliche Veränderungen zu reagieren (Hill 2014, S. 125). Digitalisierung beeinflusst diesen Anpassungsdruck in zweierlei Hinsicht: Erstens verlangt die „digitale Revolution“ durch ihren dynamischen Charakter und den Stellenwert, den sie in der öffentlichen Debatte hat, eine politische Reaktion, die von den Ministerien vorbereitet und begleitet werden muss. Dabei ist es auch ihre Aufgabe, potenzielle negative Folgen der Digitalisierung aller Lebensbereiche (z. B. einen *digital divide*) zu erkennen und ihrer Funktion entsprechend neue Impulse für politische Reaktionen zu erarbeiten. Die Erfüllung dieser Kernaufgabe setzt das Verständnis für digitale Anwendungen und deren praktische Integration in die eigene Arbeit voraus. Zweitens verändern sich im digitalen Zeitalter auch die von Politik und Öffentlichkeit artikulierten Erwartungen darüber, wie eine Verwaltung grundsätzlich arbeiten sollte.

Eine konsequente Digitalisierung ihrer Arbeitsweise bietet der Ministerialverwaltung die Chance, stärker responsiv mit Umweltveränderungen und den daraus resultierenden Herausforderungen umzugehen: Der Einsatz digitaler Anwendungen in den Arbeitsabläufen der Ministerialverwaltung verspricht, dass die Eingaben der Politik, die als Erwartung an die Ministerialverwaltung herangetragen werden, ganzheitlich effektiver und effizienter verarbeitet werden. Ein dazu notwendiger Wandel von Strukturen und Prozessen setzt letztendlich einen Wandel der Kultur der Ministerialverwaltung voraus und kann in einem Widerspruch zu den hergebrachten Strukturprinzipien stehen. Vor dem Hintergrund ihrer gefestigten Traditionen und ihrer Tendenz zur Reformresistenz ist noch ungeklärt, wie empfänglich die Ministerialverwaltung für nachhaltige strukturelle Veränderungen im Kontext der Implementation von digitalen Anwendungen ist. Im Anschluss daran ergibt sich auch die Frage, ob diese Veränderungen für sämtliche

Arbeitsplätze oder alle Verwaltungsprozesse gleichermaßen gelten oder ob es im Falle der Ministerialverwaltung Bereiche und Aufgabenfelder gibt, die sich „nicht digitalisieren lassen“. Kann langfristig sogar von einer Automatisierung von Vorgängen innerhalb des Ministeriums (*data driven administration*) ausgegangen werden oder beschränkt sich der Einsatz digitaler Werkzeuge auf eine Unterstützung (*data-supported administration*) bestehender Arbeitsprozesse?

---

### 3 Institutionelle Rahmenbedingungen

Die Digitalisierung der Ministerialverwaltung wird durch institutionelle Rahmenbedingungen bestimmt. Auf Bundesebene hat es in den letzten Jahren tiefgreifende strukturelle Veränderungen gegeben – ein Prozess, der gegenwärtig keinesfalls abgeschlossen ist. Zahlreiche neue Akteure sind in dem Feld aktiv (u. a. Beauftragter der Bundesregierung für Informationstechnik, IT-Rat, Konferenz der IT-Beauftragten der Ressorts, IT-Planungsrat, Nationaler Normenkontrollrat), die im Folgenden kurz vorgestellt werden.

Das zentrale Digitalisierungsgremium auf Bundesebene ist der IT-Rat, welcher sich gegenwärtig aus dem Beauftragten der Bundesregierung für Informationstechnik, den beamteten Staatssekretär\*innen der Bundesministerien, der Staatsministerin für Digitalisierung sowie den zuständigen Abteilungsleiter\*innen des Bundeskanzleramts, der Beauftragten der Bundesregierung für Kultur und Medien und dem Presse- und Informationsamt der Bundesregierung zusammensetzt. Das Gremium steuert auf politisch-strategischer Ebene die Informationstechnik der obersten Bundesverwaltung und berät sich hinsichtlich ressortübergreifender strategischer Fragen. Mit den operativen Fragen und der Umsetzung der Beschlüsse des IT-Rates ist die Konferenz der IT-Beauftragten der Ressorts betraut.

Seit 2016 hat das Informationstechnikzentrum Bund (ITZ Bund) als IT-Dienstleister die Aufgabe, die Ministerien ressortübergreifend und nach einheitlichen Standards in der Umsetzung ihrer IT-Strategien zu beraten. Das ITZ liegt im Geschäftsbereich des Bundesministeriums der Finanzen (BMF). Sein Aufgabenbereich umfasst Beratung und Service (IT-Konsolidierung) bezüglich der Informationstechnik in der Bundesverwaltung, die bis dahin nicht gebündelt, sondern auf unterschiedliche Dienstleister verteilt war. Neben dem ITZ erfüllt auch die BWI GmbH die Funktion eines Dienstleisters der Informationstechnik insbesondere für die Bundeswehr.

Der IT-Planungsrat wurde in Folge des IT-Staatsvertrags, welcher der Umsetzung des Art. 91c Grundgesetz dient, als föderales Koordinierungsgremium installiert und setzt sich aus Vertretern des Bundes und der Länder zusammen. Das Gremium benennt Handlungsfelder für die Verwaltung u. a. im Bereich IT-Koordinierung (Interoperabilität) und IT (Sicherheits-)Standards. 2010 wurde die Nationale *E-Government*-Strategie beschlossen, die auch als strategischer Leitfaden für die öffentliche Verwaltung auf Bundes- und Landesebene dient und die Aufgaben für die Umsetzung von *E-Government* in der Ministerialverwaltung benennt. Die Papiere sind eine Reaktion auf die zunehmend lauter werdende Kritik, dass sich die Digitalisierung in der öffentlichen Verwaltung verzögert. Hat der IT-Planungsrat

in der Vergangenheit bewusst auf die Vorgabe konkreter Maßnahmen verzichtet, scheint er sich gegenwärtig zum zentralen Akteur bei der Koordination von Bund und Ländern bezüglich einer digitalen Verwaltungsmodernisierung zu entwickeln. Dem vorausgegangen war die Forderung, das Gremium solle zugunsten einer zentralen „Koordinierungsstelle“ im Bundeskanzleramt abgeschafft werden, um tatsächliche rechtsverbindliche Maßnahmen einleiten und Standards bezüglich des Einsatzes von digitalen Anwendungen entwickeln zu können. Infolgedessen hat der IT-Planungsrat eine Reihe von Maßnahmen beschlossen (u. a. Nationales Waffenregister, Digitalisierung des Asylverfahrens, Digitalisierungslabor), welche auch die föderale Zusammenarbeit betreffen. Er ist dabei bestrebt, konkrete technische Lösungsvorschläge für eine digitale Verwaltung zu erarbeiten.

Der Nationale Normenkontrollrat (NKR), der keinen direkten Einfluss auf die Strukturen und Arbeitsweise der Ministerialverwaltung hat, übernimmt die Funktion eines Monitorings hinsichtlich des bürokratischen Aufwandes bei der Erstellung von Gesetzgebungsprojekten. Dabei fokussiert sich die Arbeit des NKR zunehmend auch auf den Einsatz aufgewendeter Mittel im Verhältnis zum Nutzen digitaler Anwendungen in der Verwaltung. Bisher spielt die Folgenabschätzung, z. B. hinsichtlich Strukturveränderungen und Wandel von Arbeitsabläufen oder aber hinsichtlich potenzieller sozio-ökonomischer Auswirkungen eine untergeordnete Rolle. Perspektivisch dürften der NKR und andere Akteure auch mögliche Schwachstellen beim Einsatz der digitalen Anwendungen in der Ministerialverwaltung in den Blick nehmen und Impulse für die Zukunft geben (Fromm et al. 2015).

---

## 4 Praktische Anwendungsfelder

Ausgewählte Formen digitaler Anwendungen sind bei der Arbeit der Ministerialverwaltung inzwischen selbstverständlich. So wird beispielsweise der Einsatz von *Tablets*, *Smartphones*, die Kommunikation über *E-Mails* oder die Nutzung geteilter Terminkalender als Grundformen digitaler Anwendungen nicht mehr hinterfragt; sie sind ein akzeptierter Bestandteil der Organisationskultur.

Angesichts ihres jeweiligen spezialisierten Handlungsgebiets werden die Ministerien vor die Herausforderungen gestellt, ihre Nutzung digitaler Anwendungen z. B. in Form einer eigenen digitalen Entwicklungsstrategie auf ihren Aufgabenbereich zuzuschneiden. Dies hat insgesamt zu einer Heterogenität der zum Einsatz kommenden Anwendungen geführt, wobei eine ressortübergreifende Kompatibilität der Anwendungen nicht vorausgesetzt werden konnte. Um flexibel auf technische Neuentwicklungen zu reagieren und gleichzeitig ein Überangebot an unterschiedlichen IT-Lösungen zu vermeiden, wurde im Jahr 2015 eine IT-Konsolidierung des Bundes beschlossen, welche drei Handlungsfelder zusammenfasst: (1) Betriebskonsolidierung (Einführung eines Bundesrechnungszentrums), (2) Dienstekonsolidierung (Doppel- oder Mehrfachentwicklung von IT zukünftig vermeiden) und (3) Beschaffungsbündelung (Vereinheitlichung der Beschaffung von IT) (Bundesministerium des Innern 2015, S. 7). Eine Vielzahl neuer Lösungen befindet sich derzeit (Stand Juli 2019) in der Test- bzw. Pilotphase oder wird bereits implementiert. Im

Folgenden wird eine Auswahl digitaler Anwendungen vorgestellt, die sich auf die tradierten Strukturmerkmale der Ministerialverwaltung (des Bundes) auswirken können.

Fragen der Sicherheit sind auch bei der Digitalisierung der Ministerialverwaltung zentral. Deshalb wurde auf Bundesebene eine einheitliche Infrastruktur mit dem Titel „Netze des Bundes“ geschaffen, welche die ebenenübergreifende Kommunikation und den Datenaustausch zwischen Bundes-, Länder- und kommunalen IT-Netzen sicher und in ihrer Pflege weniger aufwendig gestalten soll.

Die elektronische Akte (E-Akte) ist ein Beispiel für Digitalisierung in der Ministerialverwaltung, welches insbesondere das Strukturmerkmal der Dokumentationspflicht betrifft. Das *E-Government-Gesetz* des Bundes (EGovG) sieht bis 2020 die Einführung der elektronischen Aktenführung (E-Akte sowie E-Laufmappe), die Übertragung (und das Vernichten) des Papieroriginals durch ersetzendes *Scannen* sowie die Migration bestehender Dokumentationsmanagement-Systeme vor. Die Digitalisierung von Papierdokumenten kann durch die erleichterte Erhebung und Speicherung von Metadaten und durch Kreuzverweise die Zuordnung und Verbindung von Akten erleichtern. Diese Verpflichtung wird jedoch abgeschwächt, indem Behörden, „bei denen das Führen elektronischer Akten bei langfristiger Betrachtung unwirtschaftlich ist“, ausgenommen werden (§ 6 S. 2 EGovG). Gegenwärtig befindet sich die technische Umsetzung der E-Akte beim Bundesministerium für Justiz sowie beim Bundesministerium der Finanzen in der Pilotphase. Mit dem Digitalen Zwischenarchiv des Bundes (DZAB) gewährleistet das Bundesarchiv eine dauerhafte Möglichkeit des Speicherns der elektronischen Dokumente. Man verspricht einen sicheren und dauerhaften Zugang. Diese gemeinsame Lösung kann die hausinterne IT personell, organisatorisch wie technisch entlasten. Dabei ist es technisch grundsätzlich möglich, die E-Akte mit einem „dokumentenbasierten Workflow“ zu verbinden, der die Weiterleitung bzw. den Austausch von Informationen ressortübergreifend beinhaltet.

Auch über die E-Akte hinaus können digitale Anwendungen bis zu einer Automatisierung von Verwaltungsvorgängen führen. So unterstützt z. B. die im BMF angesiedelte elektronische Haushaltsdatenbank HaFi (HPL) die Erstellung von Bundestags- und Bundesratsvorlagen und die Abbildung der Ergebnisse der einzelnen Verhandlungsrunden über den Finanzplan des Bundes. Gleichzeitig erleichtert die komplementäre Datenbank HaFi (RPL) einheitenübergreifende Kommunikation, indem sie Finanzbedarfe zusammenfasst.

Zugunsten einer verstärkten Zusammenarbeit und Entscheidungsfindung befindet sich derzeit das Projekt „Social Intranet des Bundes“ (SIB) in einer abschließenden Phase der Planung und soll Ende des Jahres 2019 eingeführt werden. Es dient dem ressort- und behördenübergreifenden Austausch von Informationen, Wissen und Dokumenten. Ziel ist es auch, dass sich die Initiatoren bestimmter Maßnahmen mit Hilfe des SIB identifizieren und zuordnen lassen. Zusätzlich wird derzeit an der technischen Umsetzung einer „Bundescloud“ gearbeitet, um den intra- wie interministeriellen Datenaustausch zu ermöglichen.

Ein weiterer Baustein, die IT-Lösung für das elektronische Gesetzgebungsverfahren (E-Gesetzgebung), zielt in eine ähnliche Richtung: So soll es bald technisch möglich sein, einzelne Arbeitsschritte beim Erarbeiten eines Gesetzesentwurfs (elek-

tronische Zeitplanung, Organisation des Abstimmungsverfahren, inhaltliche Änderungen und Nachhaltigkeitsüberprüfung) elektronisch und interoperabel umzusetzen. Eine erste Projektphase ist abgeschlossen; derzeit wird auf Basis der ersten Praxiserfahrung die IT-Lösung überarbeitet.

---

## 5 Perspektiven für Staat und Verwaltung

Bei der Digitalisierung der Ministerialverwaltung handelt es sich um eine technikbasierte Modernisierung einer Organisation, die sich durch tradierte Strukturprinzipien und durch eine feste Organisationskultur kennzeichnet. Auf dieser Grundlage werden datengestützte Anwendungen implementiert, die bisher analoge Prozesse ergänzen, teilweise ersetzen oder sogar automatisieren. Anpassungen haben sich besonders bei der intra- und interministeriellen Vernetzung und Kommunikation in der vorgelagerten Phase politischer Entscheidungsfindung vollzogen.

So fassen Datenbanken den jeweiligen Planungsstand von Verhandlungen zusammen, was für ressort- wie behördenübergreifende Planungs- und Steuerungsprozesse genutzt wird. Diese beeinflussen interministerielle Kommunikationswege langfristig und schaffen die Voraussetzungen für dezentrale Kollaboration. Unter diesen Umständen kann die Aufteilung von Zuständigkeiten weniger entlang von Ressort- und Abteilungsgrenzen (Stichwort „Silostrukturen“), sondern eher entlang thematischer Überschneidungen zwischen mehreren Ressorts verlaufen. Dies spiegelt interministeriell die Koordinations- und Abstimmungsprozesse innerhalb der einzelnen Ministerien wider, in denen Prozesse auch oder gerade in Form von informellen Beratungen und Netzwerken der Fachreferate ablaufen. Zusammen mit der Abschaffung analoger Akten kann damit die Ministerialverwaltung insgesamt effizienter agieren und der Kritik entgegentreten, sie bearbeite politische Probleme nur verzögert und reagiere zu langsam auf die Erwartungen, die an sie herangetragen werden.

Bisher liegen jedoch noch keine empirischen Evaluationen hinsichtlich der langfristigen Wirkungen der Implementation digitaler Anwendungen vor. Es muss bedacht werden, dass gerade die tradierten Strukturen der Ministerialverwaltung einer Nachhaltigkeit der umfassenden intendierten Wirkungen von Digitalisierung entgegenstehen können. So kann zwar die Einführung der E-Akte zu einem kostensparenden Datenmanagement führen, die Nutzung von E-Akten ist jedoch nicht überall möglich und oftmals sind die Bearbeitung auf (ausgedruckter) Formularbasis und eine Unterschrift notwendig, um Verantwortlichkeiten nachzuvollziehen. Momentan zeigt sich, dass sich durch uneinheitliche Umsetzung rechtlicher und politischer Vorgaben und durch eine „doppelte Buchführung“ ein Daten- und Archivierungsmanagement eher noch verkompliziert, was eine kritische Diskussion bezüglich der Wirtschaftlichkeit des Vorgehens hervorruft.

Für andere Verwaltungskontexte ist bereits festgestellt worden, dass eine Beschleunigung und Personalisierung von Kommunikationswegen dazu führen können, dass intern Hierarchien abflachen und Kommunikation Hierarchieebenen überspringt. Bezuglich der traditionellen Hierarchien in Ministerien sollte daher vermutet

werden, dass sich das interne Kommunikationsverhalten zwischen Arbeitseinheiten mit der Etablierung digitaler Anwendungen zugunsten einer verstärkten horizontalen Koordination verändert. Die Kommunikation innerhalb der Ministerien ist traditionell jedoch stark vertikal orientiert und in Weisungen sowie Berichtspflichten unterteilt, was einer Veränderung entgegensteht.

Obwohl der Anspruch einer Vernetzung zwischen Behörden und an eine vereinfachte Kollaboration auf die Vermeidung einer Negativkoordination gerichtet ist, kann der Einsatz digitaler Anwendungen doch auch den gegenteiligen Effekt haben: So kann ein verstärkter Vermittlungs- und Steuerungsbedarf entstehen, wenn Teilelemente von Aufgaben zwischen Ministerien situationsspezifisch ausgehandelt werden müssen, was eine Negativkoordination verstärken würde. Die zunehmende Digitalisierung der Ministerialverwaltung wirft zudem Fragen nach Sicherheit und Datenschutz auf. Dagmar Lück-Schneider und Tino Schuppan betonen, dass „ohne einen Kulturwandel in der öffentlichen Verwaltung [...] die Gefahr [besteht], dass IT-Modernisierungen möglichst vermieden werden“ (Lück-Schneider und Schuppan 2017, S. 237). Diese Skepsis zielt auf die Veränderungsbereitschaft der Mitarbeiter\*innen der Ministerialverwaltung und eine gefestigte Ministerialkultur, die sich nicht kurzfristig verändern lässt, sondern einen Generationenwechsel in den Ministerien voraussetzt.

Die traditionsbedingten Strukturprinzipien und Arbeitsweisen scheinen dabei bisher weitgehend unangetastet zu bleiben. Im Sinne eines „Werkzeugkastens“ werden vielmehr einzelne digitale Anwendungen politik-, weisungs- und themenbezogen komplementär genutzt, anstatt ein ganzheitliches System zu etablieren, das tradierte Strukturen infrage stellen könnte. Hinzu kommt, dass die Heterogenität der Akteure, welche die Digitalisierung der Ministerialverwaltung direkt oder indirekt vorantreiben, tendenziell dazu führt, dass sich Verantwortlichkeiten zwar verteilen und damit Arbeitsteilung begünstigen, gleichzeitig aber einen erhöhten Abstimmungsbedarf mit sich bringt. Hier zeigt sich ein Bedarf an zentraler Steuerung.

Damit tritt eine Situation ein, wie sie sich vergleichbar in den letzten Jahren im Zusammenhang mit anderen Reformbemühungen, u. a. dem New Public Management gezeigt hat: Veränderungen vollziehen sich in unterschiedlichen Geschwindigkeiten je nach Haus, Aufgabenbereich und Reichweite. Die jetzige Phase der Umsetzung lässt sich als Phase des Umbruchs mit Experimentalcharakter bezeichnen, da sich die neuen „Werkzeuge“ teilweise erst noch bewähren müssen und ein nachhaltiger Nutzen noch nicht immer nachgewiesen werden konnte. Ein expliziter Beleg für den Experimentalcharakter digitaler Anwendungen sind die sog. Digitallabore bei der Umsetzung des Onlinezugangsgesetzes, in denen Fachleute, IT-Spezialist\*innen und Nutzer\*innen gemeinsam daran arbeiten, bestimmte Prozesse möglichst einfach elektronisch abzubilden, bevor sie in den Portalverbund aufgenommen werden. Zurzeit arbeiten Bund und Länder in 19 Digitallaboren daran, Leistungen wie z. B. die Beantragung von BAföG zu vereinfachen. Insgesamt bleibt damit die Frage, wie tiefgreifend und nachhaltig sich der Wandel vollzieht, bisher offen. Die Fallbeispiele zeigen jedoch deutlich, dass die Digitalisierung als technikbasierte Modernisierung in der Ministerialverwaltung angekommen ist und sie bei der Bewältigung ihrer Aufgaben von datengestützten Lösungen grundsätzlich profitieren kann.

## Literatur

- Bundesministerium des Innern. 2015. *Grobkonzept zur IT-Konsolidierung Bund*. [https://www.cio.bund.de/SharedDocs/Publikationen/DE/Innovative-Vorhaben/it\\_konsolidierung\\_bund\\_grobkonzept.pdf?\\_\\_blob=publicationFile](https://www.cio.bund.de/SharedDocs/Publikationen/DE/Innovative-Vorhaben/it_konsolidierung_bund_grobkonzept.pdf?__blob=publicationFile). Zugriffen im Juli 2019.
- Fromm, Jens, Christian Welzel, Lutz Nentwig, und Mike Weber. 2015. *E-Government in Deutschland. Vom Abstieg zum Aufstieg: Gutachten für den Nationalen Normenkontrollrat*. Berlin: Kompetenzzentrum Öffentliche IT/Fraunhofer FOKUS.
- Hill, Hermann. 2014. Wandel von Verwaltungskultur und Kompetenzen im digitalen Zeitalter. In *Transparenz, Partizipation, Kollaboration*, Hrsg. Hermann Hill, Mario Martini und Edgar Wagner, 123–148. Baden-Baden: Nomos.
- Hirsch-Kreinsen, Hartmut. 2018. Einleitung. Digitalisierung industrieller Arbeit. In *Digitalisierung industrieller Arbeit. Die Vision Industrie 4.0 und ihre sozialen Herausforderungen*, Hrsg. Hartmut Hirsch-Kreinsen, Peter Ittermann und Jonathan Niehaus, 13–33. Baden-Baden: Nomos.
- König, Klaus. 2014. Verwaltungskultur typologisch betrachtet. In *Grundmuster der Verwaltungskultur*, Hrsg. Klaus König, Sabine Kropp, Sabine Kuhlmann, Christoph Reichard, Karl-Peter Sommermann und Jan Ziekow, 11–28. Baden-Baden: Nomos.
- Lück-Schneider, Dagmar, und Tino Schuppan. 2017. Gestaltungskompetenzen für die Öffentliche Verwaltung im digitalen Zeitalter. *Verwaltung & Management* 23(5): 236–244.
- Patzelt, Werner J. 2008. Verwaltungskultur in der Ministerialbürokratie. Ein empirisches Essay. In *Führen Regierungen tatsächlich? Zur Praxis governementalen Handelns. Schriften der Sektion Regierungssystem und Regieren in der Bundesrepublik Deutschland der Deutschen Vereinigung für Politische Wissenschaft*, Hrsg. Everhard Holtmann und Werner J. Patzelt, 115–129. Wiesbaden: VS Verlag für Sozialwissenschaften.
- Weber, Max. 2013. *Wirtschaft und Gesellschaft: Grundriss der verstehenden Soziologie*, 5., revid. Aufl. Studienausg. Tübingen: Mohr Siebeck.



# IT-Planungsrat

Hans-Henning Lühr

## Inhalt

1	Grundlagen .....	406
2	Entwicklung .....	407
3	Kompetenzen und institutionelle Einbettung .....	409
4	Ergebnisse und Wirkungen – eine erste Bilanz .....	410
5	Perspektiven für Staat und Verwaltung .....	415
	Literatur .....	416

## Zusammenfassung

In föderalen Systemen wie der Bundesrepublik Deutschland muss der Ausbau des digitalen Verwaltens zwischen Bund, Ländern und Gemeinden koordiniert werden, wenn deren Behörden technisch miteinander kommunizieren wollen und ein gewisser Gleichschritt in der Entwicklung erreicht werden soll. Diese Aufgabe ist dem IT-Planungsrat von Bund und Ländern auf der Grundlage des neuen Artikel 91c des Grundgesetzes vor knapp zehn Jahren per Staatsvertrag übertragen worden. Seine Bilanz ist gemischt: Der Rat hat seither vieles auf den Weg gebracht, aber im Vergleich mit anderen Staaten liegt Deutschland beim *E-Government* noch immer bestenfalls im Mittelfeld. Die gesetzliche Vorgabe, bis 2022 alle öffentlichen Dienstleistungen auch online anzubieten, und der im Aufbau befindliche Portalverbund, über den diese Leistungen einfach zugänglich werden sollen, können hier womöglich spürbare Fortschritte bringen.

## Schlüsselwörter

*E-Government* · Kooperativer Föderalismus · IT-Standards · Portalverbund · Online-Zugangsgesetz (OZG)

H.-H. Lühr (✉)

Freie Hansestadt Bremen, Finanzressort, Bremen, Deutschland

E-Mail: [Henning.Luehr@finanzen.bremen.de](mailto:Henning.Luehr@finanzen.bremen.de)

## Abkürzungen

BMI	Bundesministerium für Inneres, für Bau und Heimat
CdBKA	Chef des Bundeskanzleramtes
CdS'e	Chef der Staats- und Senatskanzleien
FITKO	Föderale IT-Kooperation
FöKo I	Föderalismuskommission I
FöKo II	Föderalismuskommission II
Koop ADV	Kooperationsausschuss ADV (Bund-Länder-Abstimmungsgremium)
KOSIT	Koordinierungsstelle IT-Standards
OZG	Online-Zugangs-Beschleunigungsgesetz

## 1 Grundlagen

In zentralistischen Regierungssystemen können IT-Architekturen, -Standards und -Werkzeuge in allen Behörden einheitlich durchgesetzt werden; in föderalen Systemen muss das Vorgehen koordiniert werden, wenn ein gewisser Gleichklang erreicht werden soll und die Verwaltungen in Bund, Ländern und Gemeinden technisch miteinander kommunizieren sollen. Beim Zustrom an Flüchtlingen 2015 und 2016 ist exemplarisch sichtbar geworden, was es heißt, wenn die technischen Systeme von Behörden nicht kompatibel sind. Ein föderaler Flickenteppich an IT-Lösungen stößt im digitalen Zeitalter nicht nur auf Unverständnis bei Bürger\*innen und Unternehmen, er erschwert auch eine gute Platzierung in den Ranglisten, in denen der Entwicklungsstand von *Electronic Government* in verschiedenen Staaten verglichen wird. Wie die Bundesrepublik Deutschland bei solchen Vergleichen abschneidet, wirkt sich nicht nur auf die Bewertung des Wirtschaftsstandortes aus, sondern ist durchaus ein aussagekräftiger Indikator der Mängel der Online-Dienstleistungen für Wirtschaft und Bürger\*innen.

Während die IT-Koordinierung im deutschen Föderalismus lange Zeit auf informellem Wege erfolgte, haben Bund und Länder am 20. November 2009 einen Staatsvertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG geschlossen, mit dem eine klare Kooperations-, Gremien- und Verantwortungsstruktur errichtet wurde. Der IT-Planungsrat bekam umfangreiche Aufgaben zugewiesen; zudem berichtet er an die Konferenz des Chefs des Bundeskanzleramtes mit den Chefs der Staats- und Senatskanzleien.

Dem IT-Planungsrat von Bund und Ländern gehören der Beauftragte der Bundesregierung für Informationstechnik an, bisweilen auch Chief Information Officer (CIO) des Bundes genannt, sowie die entsprechenden Beauftragten der einzelnen Länder, die alle über die „erforderliche Entscheidungskompetenz“ (§ 1, 1 Geschäftsordnung des IT-Planungsrats) verfügen sollen. Außer diesen 17 ordentlichen Mitgliedern können an den Sitzungen mit beratender Stimme teilnehmen (§ 6,3 Ge-

schäftsordnung des IT-Planungsrats): (1) Vertreter der drei kommunalen Spitzenverbände, (2) der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (§ 1,2 IT-Staatsvertrag), (3) ein Vertreter aus dem Kreis der Landesdatenschutzbeauftragten, sofern Tagesordnungspunkte besprochen werden, die Datenschutzfragen auf Länderebene betreffen, (4) Vertreter des Arbeitsgremiums, das für die Verbindung der informationstechnischen Netze des Bundes und der Länder verantwortlich ist (§ 5, 2 und § 6, 2 IT-NetzG) und (5) weitere Personen auf Einladung des Vorsitzenden, insbesondere Ansprechpartner aus Fachministerkonferenzen. Der Vorsitz des Gremiums wechselt jährlich zwischen dem Bund und einem Land (in alphabetischer Reihenfolge). Nachdem Bremen 2019 den Vorsitz übernommen hatte, ist der Bund im Jahre 2020 wieder an der Reihe. Die Beauftragten für Informationstechnik im Bund und in den Ländern haben meist den Rang eines Staatssekretärs, manchmal auch den eines Ministerialdirektors. Wo formal Minister eines Fachressorts der „Chief Information Officer“ ihres Landes sind, lassen sie sich im IT-Planungsrat in der Regel durch Staatssekretäre\*innen vertreten. Inzwischen gibt es in Bayern und Hessen eigene Digitalisierungsministerien.

Die Geschäftsstelle des IT-Planungsrates ist im Bundesministerium des Innern angesiedelt, wird aber von Bund und Ländern gemeinsam finanziert und personell besetzt. Künftig wird der IT-Planungsrat von der FITKO (Föderale IT-Kooperation) sowohl als Geschäftsstelle als auch in der inhaltlichen Arbeit unterstützt werden. Die FITKO ist als Anstalt des öffentlichen Rechts mit Sitz in Frankfurt durch Staatsvertrag eingerichtet worden. Der IT-Planungsrat hat 2017 einen FITKO Aufbaustab als „kleine, agile Organisation“ eingerichtet, der mit der Errichtung der AÖR beauftragt ist. Ab 2020 wird die FITKO dann mit insgesamt 40 Mitarbeiterinnen und Mitarbeiter ihre Arbeit aufnehmen. Zu den Aufgaben der FITKO gehören u. a. Erarbeitung und Umsetzung der föderalen IT-Strategie, die Konzeption und Weiterentwicklung der föderalen IT-Architektur, die Bewirtschaftung des geplanten Digitalisierungsbudgets, die Koordination und der Dialog mit allen relevanten Stakeholdern sowie administrative Aufgaben.

---

## 2 Entwicklung

Als die automatisierte Datenverarbeitung (ADV), später EDV, IT oder IKT genannt, in die Behörden einzog, ergab sich auch die Notwendigkeit, die Entwicklung zu koordinieren, wenn man in Bund, Ländern und Gemeinden technisch miteinander kommunizieren und kooperieren wollte. Im Februar 1970 gründete sich z. B. der „Kooperationsausschuss von Bund und Ländern für automatisierte Datenverarbeitung“ (KoopA ADV), eines von zahlreichen informellen Gremien, die dafür sorgten, dass der Föderalismus auch auf diesem Gebiet funktionierte. So lange das als ein Thema für Spezialisten galt, konnten die Fachleute dort unter sich bleiben und für einen gewissen Gleichklang der Entwicklung sorgen. Der Ausschuss hatte allerdings nur eine geringe politische „Durchschlagskraft“, sondern musste für seine Anliegen jeweils in den Ressorts, in den Kabinetten und in den Konferenzen der Minister werben, und er verfügte auch nicht über eigene Ressourcen.

Anfang der 2000er-Jahre wurde das Thema auf die politische Ebene gehoben. Die Koordinierung der Aktivitäten übernahm ab 2002 eine Arbeitsgruppe von Staatssekretären aus Bund und Ländern, was die Frage aufwarf, wer innerhalb der Landesregierung eigentlich für *Electronic Government* zuständig sei – meistens das Innernressort, manchmal aber auch das Finanzressort. Die Kommunen sind nach Auffassung aller Länder ungeachtet der kommunalen Selbstverwaltung Bestandteil des jeweiligen Landes; daher nahmen Vertreter der kommunalen Spitzenverbände an den Sitzungen als ständige Gäste mit Vortragsrecht teil.

Der Arbeitskreis der Staatssekretäre\*innen stieß immer wieder auf erhebliche Grenzen. Er blieb ein informelles Gremium ohne rechtliche Grundlage und ohne eigene Ressourcen. Er konnte keine verbindlichen Vorgaben machen, sondern musste sich darauf verlassen, dass seine im Konsens entwickelten Beschlüsse freiwillig befolgt wurden. Projekte kamen nicht voran, weil die Länder sich nicht in der Lage sahen, eine Umsetzung einzuleiten und eine anteilige Mitfinanzierung zu übernehmen.

Dass ein föderaler Flickenteppich ohne Steuerungsinstanz ein elektronisches Regieren und Verwalten behindert und verzögert, galt allgemein als ausgemacht. Die im Jahre 2006 eingesetzte „Kommission zur Modernisierung der Bund-Länder-Finanzbeziehungen“, die die Föderalismusreform II vorbereiten sollte, nahm sich deshalb auch des Themas „Einführung von IT-Standards und -Systemen“ an. Zum Gesamtpaket der Reformen gehörte neben der „Schuldenbremse“ ein neu in das Grundgesetz eingefügter Art. 91c, wonach Bund und Länder in IT-Fragen bei Planung, Errichtung und Betrieb zusammenwirken und sich für den Datenaustausch und bei der IT-Sicherheit auf gemeinsame Standards verständigen sollen (Gesetz zur Änderung des Grundgesetzes vom 29. Juli 2009; BGBl. I S. 2248). Die Digitalisierung von Staat und Verwaltung sollte nicht mehr jedem selbst überlassen bleiben, sondern als Gemeinschaftsaufgabe angesehen werden. Der Artikel im Wortlaut:

- (1) „Bund und Länder können bei der Planung, der Errichtung und dem Betrieb der für ihre Aufgabenerfüllung benötigten informationstechnischen Systeme zusammenwirken.“
- (2) Bund und Länder können auf Grund von Vereinbarungen die für die Kommunikation zwischen ihren informationstechnischen Systemen notwendigen Standards und Sicherheitsanforderungen festlegen. Vereinbarungen über die Grundlagen der Zusammenarbeit nach Satz 1 können für einzelne nach Inhalt und Ausmaß bestimmte Aufgaben vorsehen, dass nähere Regelungen bei Zustimmung einer in der Vereinbarung zu bestimmenden qualifizierten Mehrheit für Bund und Länder in Kraft treten. Sie bedürfen der Zustimmung des Bundestages und der Volksvertretungen der beteiligten Länder; das Recht zur Kündigung dieser Vereinbarung kann nicht ausgeschlossen werden. Die Vereinbarungen regeln auch die Kostentragung.“
- (3) Die Länder können darüber hinaus den gemeinschaftlichen Betrieb informationstechnischer Systeme sowie die Errichtung von dazu bestimmten Einrichtungen vereinbaren.“

Auf dieser Grundlage schlossen der Bund und die Länder einen „IT-Staatsvertrag“ (Vertrag über die Errichtung des IT-Planungsrates und über die Grundlagen der

Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Art 91c GG), der am 1. April 2010 in Kraft getreten ist.

Art. 91c GG wurde im Rahmen der am 20. Juli 2017 in Kraft getretenen Grundgesetzänderung durch einen Abs. 5 ergänzt:

- (5) „Der übergreifende informationstechnische Zugang zu den Verwaltungsleistungen von Bund und Ländern wird durch Bundesgesetz mit Zustimmung des Bundesrates geregelt.“

Damit wurde die verfassungsrechtliche Grundlage für die ausschließliche Gesetzgebungskompetenz des Bundes zur Ausgestaltung des Zugangs zu den Verwaltungsdienstleistungen von Bund und Ländern (einschließlich Kommunen) geschaffen, auf der dann erst das Onlinezugangsverbesserungsgesetz verabschiedet werden konnte.

Der IT-Planungsrat ist also ein Bund-Länder-Gremium, das dafür sorgen soll, dass der Föderalismus als kooperativer Föderalismus funktioniert. Der IT-Planungsrat gehört – anders als sein Vorgänger – zu den föderalen Koordinierungsgremien, die auf gesetzlicher Grundlage operieren. 1969 wurde in das Grundgesetz der Abschnitt „Gemeinschaftsaufgaben“ als Reaktion auf die starre Aufgabenverteilung im deutschen Föderalismus eingefügt. Damit wurde ein System von Mitwirkungs-, Mitplanungs- und Mitfinanzierungsformen des Bundes unter Wahrung des bundesstaatlichen Prinzips geschaffen. Die aus einer gesamtstaatlichen Sicht heraus für erforderlich gehaltene Steuerung des Bundes, die in Kooperation mit den Ländern erfolgt, sollte so verfassungsrechtlich verankert werden. Diese Praxis wurde in der Föderalismusreform II durch den neuen Art. 91c des GG weiterentwickelt. Institutionell ist die Schaffung eines IT-Planungsrates damit eine neue Qualität bei den Gemeinschaftsaufgaben in Abschnitt VIII a des Grundgesetzes (Seckelmann 2009, S. 747). Durch die Erweiterung der Zuständigkeiten durch Abs. 5 in Art. 91c GG durch das Gesetz zur Änderung des GG vom 13.07.2017 (BGBl. I S. 2347) ist inzwischen eine nochmal erweiterte Qualität in der Aufgabenwahrnehmung eingetreten, da der IT-Planungsrat die Umsetzung des OZG und der Schaffung eines Portalverbundes als Steuerungsaufgabe übernommen hat.

---

### **3 Kompetenzen und institutionelle Einbettung**

Der IT-Planungsrat beschäftigt sich nicht mit allen digitalen Themen, sondern konzentriert sich darauf, technische Standards für die Digitalisierung der Verwaltungen im Bund, in den Ländern und in den Gemeinden zu entwickeln und das OZG umzusetzen. Auf der Basis dieser Standards Dienstleistungen elektronisch anzubieten, liegt allerdings weiterhin allein in der Entscheidungskompetenz des Bundes und der jeweiligen Länder. Die Funktion des IT-Planungsrats ist daher allein die verwaltungsebenenübergreifende Planung und Koordinierung.

Nach § 1 des Staatsvertrages soll der IT-Planungsrat folgende Aufgaben erledigen:

- die Zusammenarbeit von Bund und Ländern in Fragen der Informationstechnik koordinieren,

- fachunabhängige oder fachübergreifende Standards für Interoperabilität und IT-Sicherheit beschließen,
- die Projekte im Rahmen der Nationalen E-Government-Strategie steuern und
- das Verbindungsnetz der öffentlichen Verwaltungen planen und entwickeln.

Die Schrittfolge, die dabei angestrebt wird, schreibt er in seinem Aktionsplan jährlich fort.

Der IT-Planungsrat ist ausschließlich für die Digitalisierung der öffentlichen Verwaltungen zuständig, mit einem besonderen Augenmerk auf die Schnittstellen zwischen den IT-Systemen des Bundes und der Länder, Portalverbände und die Umsetzung des OZG. So wird die Digitalisierung des Gerichtswesens nicht von ihm, sondern von einem „eJustice-Rat“ der Justizministerkonferenz koordiniert. Diese hat sich für den elektronischen Rechtsverkehr in etlichen Gesetzen eigene Ziele und Fristen gesetzt. Dass auch die elektronische Kommunikation zwischen Behörden und Gerichten ohne Medienbrüche funktionieren sollte, ist damit nicht gesichert. Der IT-Planungsrat ist deshalb mit dem eJustice-Rat um eine enge Kooperation bemüht.

Die derzeitige Organisation des IT-Planungsrates ist in der folgenden Abbildung wiedergegeben (Abb. 1).

Nach Aufnahme der Arbeit durch die FITKO werden durch diese die Aufgaben der Geschäftsstelle übernommen. Um die politische Gestaltung der digitalen Transformation von Wirtschaft, Gesellschaft und Staat kümmern sich im Bund praktisch alle Ressorts, wenn auch unterschiedlich intensiv. Sie werden von einem Kabinett-ausschuss Digitalisierung, dem unter Leitung der Kanzlerin alle Minister angehören, gesteuert. Im Bundeskanzleramt ist die Beauftragte der Bundesregierung für Digitalisierung im Amt einer Staatsministerin mit einem Arbeitsstab angesiedelt. Die neue Abteilung 6 im Bundeskanzleramt „Politische Planung, Innovation und Digitalpolitik, Strategische IT-Steuerung“ ist allerdings dem Chef des Bundeskanzleramts unterstellt. Die Bundesregierung lässt sich zudem von einem „Digitalrat“ externer Experten beraten und hat eine „Datenethikkommission“ berufen, die Vorschläge erarbeiten soll, wie mit den moralischen Dilemmata umgegangen werden kann, die in der digitalen Ökonomie an vielen Stellen auftreten. In den Ländern sind die Zuständigkeiten für *E-Government* verschiedenen Ministerien (klassisch: Innen oder Finanzen), Staats- bzw. Senatskanzleien oder in Bayern und Hessen eigenen Digitalisierungsressorts zugeordnet. Die kommunalen Spitzenverbände fassen die Aktivitäten ihrer Mitgliedskommunen zusammen und bündeln die Interessenlagen. Der Deutsche Städtetag hat 2018 eigens einen „Arbeitskreis Digitalisierung“ zur Koordinierung eingerichtet.

---

## 4 Ergebnisse und Wirkungen – eine erste Bilanz

Seit seiner Gründung vor zehn Jahren hat der IT-Planungsrat diverse Beschlüsse gefasst und zahlreiche Projekte auf den Weg gebracht: Steuerungsprojekte von besonderer Bedeutung, die ihm vom Chef des Bundeskanzleramtes und den Chefs der Staats- und Senatskanzleien der Länder aufgegeben werden, fach- oder ebenen-

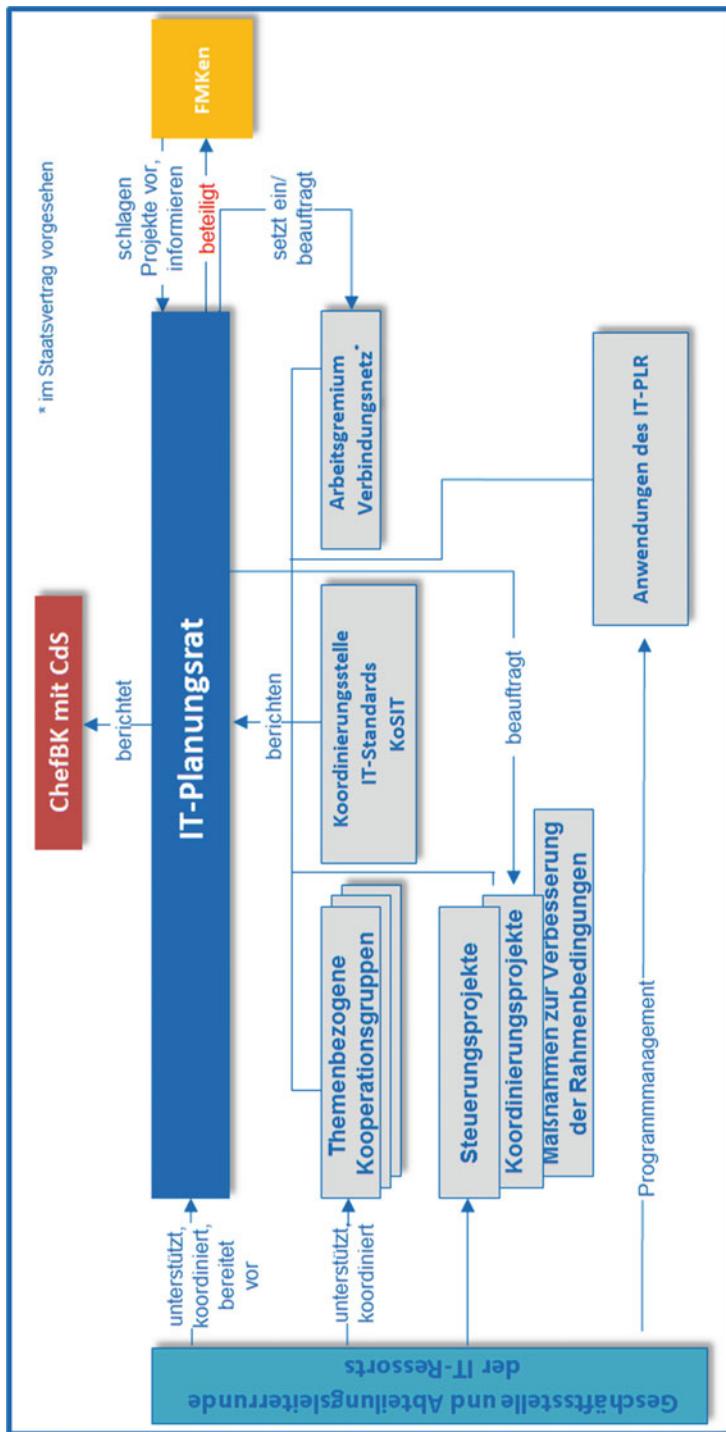


Abb. 1 IT-Planungsrat – Geschäftsstelle

übergreifenden Koordinierungsprojekte, die sich aus der eigenen Zuständigkeit ergeben, und einfache Maßnahmen und gemeinsame Aktivitäten, die nicht als Projekte betrieben werden müssen.

Zur Konkretisierung seines Auftrages hat der IT-Planungsrat 2010 eine Nationale E-Government-Strategie beschlossen, die schon in ihrem Titel deutlich machte, dass es sich bei den darin genannten Vorhaben nicht um Projekte des Bundes, sondern um eine gemeinsame Aufgabe von Bund, Ländern und Gemeinden handelte. Dieses „Leitbild für koordiniertes Handeln in Eigenverantwortung“, wie es in der Fortschreibung fünf Jahre später hieß (IT-Planungsrat 2015, S. 6), bildet die Basis für die konkreten Maßnahmen im jährlichen Aktionsplan und in der gemeinsamen Standardisierungsagenda.

Die Strategie des IT-Planungsrates ist eingebettet in den Nationalen Aktionsplan der Bundesregierung zur Umsetzung der Open-Data-Charta der G8 (2014) oder die Nationale Geoinformations-Strategie (NGIS) aus dem Jahre 2015, aber auch in die „Digitale Agenda 2014–2017“ der Bundesregierung bzw. ihre aktuelle „Umsetzungsstrategie zur Gestaltung des digitalen Wandels“ (Deutscher Bundestag 2018). Digitalisierungsstrategien sind inzwischen auch auf der Ebene der Länder entwickelt worden.

Die rechtlichen Grundlagen für die Digitalisierung der Verwaltungen sind mit dem E-Government-Gesetz des Bundes (als Artikel 1 des Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften vom 25. Juli 2013) gelegt worden. Danach setzt unter anderem der Rat der IT-Beauftragten der Bundesministerien (IT-Rat) innerhalb der Bundesregierung die Beschlüsse um, die der IT-Planungsrat für die IT-Zusammenarbeit von Bund und Ländern gefasst hat (§ 10 EGovG). Die meisten Bundesländer haben eigene E-Government-Gesetze erlassen, die auch die Entscheidungsinfrastruktur jeweils festlegen.

Nach dem Onlinezugangsgesetz (OZG) aus dem Jahre 2017 sind Bund, Länder und Gemeinden verpflichtet, alle Leistungen ihrer Verwaltungen bis 2022 (auch) digital anzubieten. Wenn es fristgerecht gelingen sollte, alle rund 575 staatlichen und kommunalen Leistungen, die (nach Geschäfts- oder Lebenslagen) 14 Themenfeldern zugeordnet worden sind, auch über das Netz anzubieten, würde das für das elektronische Regieren und Verwalten in Deutschland einen großen Sprung nach vorn bedeuten. Von den identifizierten Leistungen waren Ende 2018 erst 29 bundesweit verfügbar, wie beispielsweise die Einkommensteuer (ELSTER), die Ausbildungsförderung (BAföG) und der Rundfunkbeitrag. 119 weitere Leistungen konnten teilweise *online* beantragt werden, d. h. einzelne Schritte konnten elektronisch abgewickelt werden, aber nicht der ganze Prozess, oder die Lösung war zwar in einigen Ländern und Kommunen verfügbar, aber nicht flächendeckend. Den Fortschritt kann man im OZG-Umsetzungskatalog verfolgen, der 55 Pakete von Geschäfts- oder Lebenslagen enthält. Die digitale Version des OZG-Umsetzungskatalogs wird vorläufig passwortgeschützt bereitgestellt, wobei alle Beschäftigten der Verwaltung einen Zugang erhalten können. (zugang@ozg-umsetzung.de).

Der Bund und jeweils ein Land übernehmen gemeinsam die Federführung und die Verantwortung dafür, die einzelnen Leistungen ins Netz zu bringen. Die technischen Lösungen, die dabei entwickelt werden, sollen dann von allen anderen Bun-

desländern übernommen werden, die diese Leistung ebenfalls anbieten („einer für alle“). Um die Nutzung dieser Angebote möglichst einfach zu gestalten, wird die technische Umsetzung in „Digitallaboren“ mit Betroffenen getestet. Damit ist für die öffentliche Verwaltung ein bemerkenswert innovativer Weg der Erprobung neuer Verfahrensabläufe gewählt worden.

Damit sich Nutzer möglichst rasch zurechtfinden und möglichst nur einmal authentifizieren müssen, sollen die Portale von Bund, Ländern und Gemeinden technisch zu einem Verbund verknüpft werden, in dem sich jede Bürgerin, jeder Bürger und jede Firma für seine Transaktionen mit der Verwaltung ein Konto anlegen kann. Unabhängig vom Einstieg würde man dort alle staatlichen und kommunalen Leistungen finden und seine Behördengänge abwickeln können.

Der Bund will in die OZG-Umsetzung in den nächsten Jahren rund 500 Mio. € investieren. Die Länder und Gemeinden müssen die Kosten für ihre Schnittstellen zum Portalverbund selbst tragen. Nach dem Ausprobieren eines Piloten waren Ende 2018 Leistungen von fünf Partnern über den Verbund zugänglich, dem sukzessive alle weiteren Länderportale folgen sollen.

Welche Prioritäten der IT-Planungsrat setzt, kann man seinem Digitalisierungsprogramm von 2016 entnehmen. Nach dem Beispiel der Digitalisierung des Asylverfahrens sollen „konkrete Vorhaben mit klar umrissenen Anforderungen bei hinreichender Mittelausstattung“ dafür sorgen, dass bei besonders wichtigen Themen (z. B. Querschnittsaufgaben, Steuern und Unternehmensführung) durch gemeinsame Architekturprinzipien, Basiskomponenten, Arbeitsprozesse und Schnittstellen möglichst schnell spürbare Fortschritte erzielt werden können. Bisher sind die Gegenstände und die Konsensbildung bei Entscheidungen im IT-Planungsrat nicht Gegenstand wissenschaftlicher Forschung geworden.

Der thematische Rahmen der Entscheidungsfelder ergibt sich zum einen aus den rechtlichen Vorgaben (Art. 91c GG, Staatsvertrag zu Art. 91c GG, Staatsvertrag zur FITKO): IT-Standards, Netzinfrastrukturen und die Umsetzung des OZG. Dies lässt sich dann in einzelne Entscheidungsfelder differenzieren:

- Portalverbund
- Einheitliches Unternehmenskonto
- OZG-Umsetzung
- Registermodernisierung
- Digitale Qualifizierung
- Cybersicherheit
- Digitale Souveränität

Auffällig bei einer Analyse der Entscheidungsvorgänge ist, dass – abgesehen von der Steigerung der Dynamik in den letzten Jahren – eine Erweiterung von der anwendungsbezogenen Informatik zu gesellschaftspolitisch relevanten Themen abzeichnet: *Users first* als neue Orientierung für öffentliche Dienstleistungen, Barrierefreiheit, Arbeit 4.0, Qualifizierung und digitale Souveränität.

Die Entscheidungsfundung im IT-Planungsrat ist abgesehen von den in § 3 des IT-Staatsvertrages zu IT-Interoperabilitäts- und IT-Sicherheitsstands und über das

Verbindungsnetz nach § 4,3 IT-NetzG immer auf Einstimmigkeit orientiert (§ 9,2 der Geschäftsordnung). Abgesehen von Empfehlungen für die öffentliche Verwaltung, die der IT-Planungsrat mit einfacher Mehrheit beschließen kann, hat die Geschäftsordnung einen „Ausweg für Helden“ offen gehalten: Bindungswirkung haben auch Beschlüsse, sofern sie nur für die zustimmenden Mitglieder gelten und dies auch im Beschluss vorgesehen worden war. Diese Variante ist bisher nicht praktiziert worden. Zudem wäre diese Orientierung auf einen Wettbewerbsföderalismus der Sache, der Vereinheitlichung von Standards und Verfahren in der IT, nicht dienlich.

Es bleibt also nur die Staatskunst des Föderalismus, zwischen Bund und Ländern eine gemeinsame Linie zu erzeugen. Die klassischen Instrumente und Mittel sind dabei die gemeinschaftliche Finanzierung oder gezielte Einzelfinanzierung, Prototypen von Anwendungen mit landesspezifischer Ausgestaltungsmöglichkeit, konvergente Verfahren der schrittweisen Annäherung auf der Ebene bestehender Lösungen, gemeinschaftliche Erstellung von Lösungen und eine Lasten- und Vorteilsverteilung bei Anwendungen.

Zunehmend wird das Handeln des IT-Planungsrats kritisch in der Presse gewürdigt. Unternehmerverbände, Gewerkschaften und Interessengruppen (z. B. die Behindertenverbände) nehmen starken Einfluss. Eine besondere Rolle spielt als kritische gesellschaftliche Einrichtung der Deutsche Normenkontrollrat. Seine Berichte und Gutachten werden sehr stark wahrgenommen und haben eine unmittelbare Wirkung auf die Entscheidungsfindung.

Gespräche oder Anhörungen von Verbänden, Gewerkschaften sind ausdrücklich in dem Entscheidungsablauf einbezogen. Um diese unterschiedlichen Wirkungen im Einzelfall einbeziehen und realisieren zu können, hat sich die Entscheidungsfindung zu einem prozeduralen Entscheidungsverfahrens, das – um bisherige Chancen- und Risikozurechnungen auch bei künftigen Entscheidungen einbeziehen zu können – auf Erfahrung und ein qualitatives Wissens- und Entscheidungsmanagement aufbaut.

Trotz aller Anstrengungen und trotz unbestreitbarer Erfolge ist die Gesamtbilanz nach zehn Jahren IT-Planungsrat eher durchwachsen. Die Umsetzung des OZG ist zwar angelaufen und hat sich als System etabliert, insbesondere ist es gelungen, die Kommunen verschiedener Größenklassen einzubeziehen, gleichwohl ist es nicht realistisch, von einer Umsetzung des OZG bis 2022 auszugehen.

Insbesondere zur Nachnutzung der entwickelten Prototypen in den Digitalisierungslaboren bedarf es konzeptioneller Vorarbeiten und gezielter Umsetzungsstrategien. Der Nationale Normenkontrollrat hat in seinem Jahresbericht 2018 (Nationaler Normenkontrollrat 2018, S. 35 ff.) erneut auf die schlechte Platzierung Deutschlands in internationalen Vergleichsstudien hingewiesen. Im *Digital Economy and Society Index* (DESI) der Europäischen Kommission habe Deutschland bei den *Digital Public Services* zuletzt nur Platz 21 unter den 28 EU-Mitgliedern erreicht. Und eine alle zwei Jahre stattfindende Umfrage des Statistischen Bundesamtes zeige, dass die Verwaltung gerade in den Kategorien schlechter abschneide, in denen eine konsequente Digitalisierung besonders helfen würde. „Der große Durchbruch und ein flächendeckendes, nutzerfreundliches Onlineangebot aller wichtigen

Verwaltungsleistungen sind bisher jedoch nicht gelungen“ (Nationaler Normenkontrollrat 2018, S. 35).

---

## 5 Perspektiven für Staat und Verwaltung

Beim aktuellen Stand der Entwicklung bleiben folgende Fragen noch offen:

- Wird der Anspruch einer Steuerung des E-Government von Bund/Ländern/Kommunen einlösbar sein?
- Ist der IT-Planungsrat in der bundesstaatlichen Ordnung ein handlungswirksames Entscheidungsgremium? Was wären die alternativen Gestaltungsmöglichkeiten? (OZG-Umsetzung, Registermodernisierung, digitale Qualifizierung des öffentlichen Sektors, digitale Souveränität)
- Wird der IT-Planungsrat zunehmend zur institutionellen „Drehscheibe“ für die Forcierung der Digitalisierung in der öffentlichen Verwaltung?

Die Geschichte des elektronischen Regierens und Verwaltens in Deutschland ließe sich auch als eine Geschichte des Scheiterns schreiben. Stichworte dafür sind die elektronische Gesundheitskarte, die nach zehn Jahren trotz erheblicher Investitionen kaum mehr als den Mitgliedsausweis einer Krankenkasse darstellt, der elektronische Personalausweis, der nur von relativ wenigen Bürger\*innen tatsächlich für elektronische Dienstleistungen genutzt wird, oder die De-Mail, für die es nach der Begründung des Gesetzentwurfs fünf Jahre später sechzig Provider geben sollte.

Nur ELSTER, die elektronische Steuererklärung, stößt auf eine relativ große Resonanz. Das Land Bremen hat die Entwicklung forciert und eine neue organisatorische Ausgestaltung und Außenpräsentation mit dem *Online-Finanzamt* etabliert. Bei der Plattform „Bund online“ ist es nicht vollständig gelungen, die zehn von den Bürger\*innen genutzten Dienstleistungen der Verwaltung *online* zu bringen. Trotzdem sollte das in der letzten Wahlperiode für die hundert wichtigsten Dienstleistungen versucht werden – ein Ziel, das verfehlt wurde.

Im Portalverbund sollen ab 2022 nicht weniger als 575 Dienstleistungen elektronisch abgerufen werden können. Dieses Großprojekt erfordert daher auch eine Analyse und damit ein besseres Wissen darüber, warum deutlich bescheidenere Zielsetzungen früher nur teilweise erreicht worden sind.

Der IT-Planungsrat ist ein notwendiges Instrument zur Koordinierung der Digitalisierung der Verwaltungen von Bund, Ländern und Gemeinden, aber er kann nur dann zu einem entscheidenden Instrument für ein erfolgreiches *E-Government* in Deutschland werden, wenn er von einer Fehleranalyse ausgeht: Warum sind viele gute Ansätze immer wieder versandet, warum ist die erhoffte Resonanz bei den Bürger\*innen nicht gefunden worden? Darüber ist aber nicht viel bekannt. Die weitere Entwicklung des IT-Planungsrates wird daher mit einer laufenden Fehleranalyse einhergehen müssen, um die anspruchsvollen Zielsetzungen des OZG umsetzen zu können.

## Literatur

- Deutscher Bundestag. 2018. *Umsetzungsstrategie der Bundesregierung. Digitalisierung gestalten.* BT-Drucks. 19/5810 vom 15. November 2018. Berlin: Deutscher Bundestag.
- IT-Planungsrat. 2015. *Nationale E-Government-Strategie.* Fortschreibung 2015. Berlin: IT-Planungsrat.
- Nationaler Normenkontrollrat (NKR). 2018. *Deutschland: Weniger Bürokratie, mehr Digitalisierung, bessere Gesetze Einfach machen!* Jahresbericht 2018 des Nationalen Normenkontrollrates. Berlin: Nationaler Normenkontrollrat.
- Seckelmann, Margrit. 2009. „Renaissance“ der Gemeinschaftsaufgaben in der Föderalismusreform II? Zu den Gemeinschaftsaufgaben und den Möglichkeiten kooperativen Handelns im Bundesstaat (insbesondere zu den Art. 91a und b GG n.F. sowie zur Aufnahme der Art. 91c und d GG in das Grundgesetz). *Die Öffentliche Verwaltung* 62(18): 747–757.



---

# Digitalisierung auf Länderebene

Alexander Berzel

## Inhalt

1	Begriffsklärung .....	418
2	Theoretische Grundlagen .....	418
3	Praktische Ausgestaltung: die Steuerungsarrangements .....	420
4	Varianzen in den Digitalstrategien .....	421
5	Umsetzungsstand und Auswirkungen am Beispiel E-Government .....	423
6	Perspektiven der Digitalisierung im Föderalismus .....	425
	Literatur .....	426

---

## Zusammenfassung

Das Gestaltungsmandat der Länder bei der Digitalisierung ist umstritten. In der Föderalismusforschung gelten sie einerseits als innovationsfördernd. Andererseits hat der Bund angesichts der unzureichenden Digitalisierung der Verwaltung in Deutschland Entscheidungsrechte erhalten, um Standardisierungen durchzusetzen. Die Analyse der Digitalisierungsstrategien der Landesregierungen lässt ein dynamisches Wechselspiel zwischen regionaler Differenzierung und Konvergenzprozessen erkennen. Mit ihren Digitalisierungsstrategien haben die Länder bislang vor allem auf der Darstellungsebene eine sichtbare Reaktion gezeigt. Inwieweit die inhaltlichen Schwerpunkte implementiert werden und die adressierten Steuerungsarrangements dies unterstützen, kann noch nicht endgültig abgeschätzt werden.

---

## Schlüsselwörter

Föderalismus · Innovation · Interoperabilität · Digitalstrategien ·  
Steuerungsarrangements

---

A. Berzel (✉)

Gesellschaftswissenschaften, Universität Kassel, Kassel, Deutschland

E-Mail: [alex.berzel@uni-kassel.de](mailto:alex.berzel@uni-kassel.de)

## 1 Begriffsklärung

Der Begriff Digitalisierung umfasst nicht nur den technologischen Wandel, sondern auch die umfassend-transformativen Auswirkungen der durch diesen Wandel induzierten Veränderungs- und Innovationsprozesse auf Politik, Wirtschaft und Gesellschaft. Innerhalb des politisch-administrativen System der sechzehn deutschen Länder bearbeiteten vor allem die Landesregierungen das Thema. Dies gründet sich erstens auf deren im Exekutivföderalismus dominante Stellung, zweitens auf eben jenen die diversen Ressorts herausfordernden Transformationsprozess. Drittens integrieren Regierungen in Strategieprozessen die entstehenden Anforderungen in Form von neuen Steuerungsarrangements sowie problemorientierten Ziel-Maßnahmen-Programmen in ihr Handeln. Diese Prozesse dienen der Abstimmung, Vereinheitlichung, Formulierung und Implementation ihrer Politik (Entscheidungsebene) wie auch der kommunikativen Legitimation und Sichtbarkeit von Alternativen (Darstellungsebene).

---

## 2 Theoretische Grundlagen

Bei der Betrachtung der Gestaltung der Digitalisierung auf Länderebene stellen sich zunächst grundlegende Fragen der föderalen Struktur: Welche Ebene übernimmt welche Aufgabe? *Does federalism matter?* Macht es also einen Unterschied, wenn mehrere Ebenen Verantwortung innehaben und dementsprechend interagieren? In der Forschung zum *Föderalismus* wird dabei für die exekutiv-föderalistisch strukturierte Bundesrepublik die Tendenz zur Unitarisierung – also die Dominanz zentralstaatlicher Gestaltung – als prägend angesehen, wogegen politikfeldspezifisch immer wieder föderale Ausdifferenzierungen aufgezeigt werden können.

Länder nutzen bevorzugt die folgenden Möglichkeiten der Politikgestaltung:

- (1) Beeinflussung der Bundesebene: Die Länder können auf die Bundesgesetzgebung einwirken. Dies findet etwa durch (vertikale) Politikdiffusion von *Best-Practice*-Ansätzen über Bund-Länder-Arbeitsgruppen oder durch die horizontale Koordination zwischen den Ländern und folgend via Bundesrat statt.
- (2) Ausführung von Bundesgesetzen: Darüber hinaus besitzen sie Handlungsspielräume in der Ausführung von Bundesgesetzen, da der Bund in vielen Bereichen zwar die Gesetzgebungskompetenz hat, aber keine ausführenden Behörden vorhält.
- (3) Nutzung von Landeskompotenten: Die Länder können dann eigenständig legislativ tätig werden, wenn sie die alleinige Gesetzgebungskompetenz besitzen (Art. 70 Abs. 1 GG). Länder dürfen auch innerhalb der konkurrierenden Gesetzgebung eigene oder ergänzende Bestimmungen erlassen, wenn für diese Bereiche noch keine Regelungen auf Bundesebene getroffen wurden (Art. 70 Abs. 2 GG). Auch wenn der Bund geltendes Bundesrecht aufhebt und auf eine fortgesetzte Regulierung verzichtet, können Länder tätig werden.

- (4) Ergänzende Handlungsoptionen durch eigene Ressourcen: Zudem haben die Länder die Möglichkeit, z. B. Programme der Europäischen Strukturfonds zu nutzen, um so über die eigene Gesetzgebungskompetenz hinausgehend und bezogen auf die unterschiedlichen Felder der Querschnittsaufgabe Digitalisierung weitere eigene Projekte zu verfolgen.
- (5) Verwaltungsstruktur und -organisation: Schließlich reagieren Landesregierungen insofern auf die digitalen Transformationsprozesse, dass ihre Verwaltungen Dienste, Arbeitsprozesse und ihre interne Organisation neu aufstellen.

Im Bereich der konkurrierenden Gesetzgebung – dem Großteil der staatlichen Regelungssphäre – setzt Art. 72 Abs. 2 GG hingegen auf zentralstaatliche Regelungen, sofern dies im Sinne der „Herstellung gleichwertiger Lebensverhältnisse im Bundesgebiet“ erforderlich ist. Auch wenn die Unitarisierung der Gesetzgebung nicht mehr in vollem Umfang gelten kann und bestimmte Themenfelder infolge der Föderalismusreform I von 2006 in den Bereich der ausschließlichen Landesgesetzgebung überführt worden sind – die Dominanz des Bundes ist kaum zu bestreiten.

Für Digitalisierung ist ein Gestaltungsmandat auf Länderebene nicht umstritten. Der Föderalismus und seine Länder-Varianzen wird in seiner Heterogenität als Komplexitätserhöhend für adäquate Digitalisierungsaktivitäten des Staates wahrgenommen, es drohten „digitale Insellösungen“ (Peuker 2015, S. 63) durch Pfadabhängigkeit infolge sogenannter *Lock-in*-Effekte. Statt sechzehn Ländern, die individuelle Antworten auf diesen Transformationsprozess suchen, sei ein zentralisierter, auf Standardisierungen und Harmonisierungen ausgerichteter Prozess effizienter und zielführender.

Dieser kritischen Sichtweise gegenüber stehen theoretische wie praktische Erkenntnisse, die in der föderalen Konstellation einen Treiber digitaler Anpassungsleistungen erkennen. Bereits die Vorgabe einer „Herstellung gleichwertiger Lebensverhältnisse“ kann auch umgekehrt interpretiert werden: als ein Ansatz, der Vielfalt und Wettbewerb zulässt. In diesem Sinne ziehen die Länder eine höhere Passfähigkeit ihrer Politik aus der Möglichkeit, Lösungen für ihre je eigenen Besonderheiten zu finden. Zudem ist die Funktion des Föderalismus als eine Art Spielwiese für innovative Ansätze zu nennen. Hier wird die gliedstaatliche Heterogenität als Stärke mit dem Ziel der Generierung von *Best Practices* interpretiert. Einerseits werden ein besonderes Problemwissen und folglich spezifische Lösungsideen aufgrund regionaler Nähe unterstellt. Andererseits greift eine überschaubare Reichweite der entsprechenden Entscheidung, was im Falle von misslungenen Reformansätzen die Folgen begrenzt. Im Erfolgsfall können gelungene Lösungen diffundieren – mithin das Gegenargument zu den obigen *Lock-in*-Risiken. Verstärkt wird diese Funktion dadurch, dass das noch junge Handlungsfeld der Digitalisierungspolitiken infolge seines transformativen Charakters nur wenige Gewissheiten bietet (Härtel 2017, S. 200).

Betrachtet man die *Digitalstrategien*, an denen die Länder arbeiten, werden zwei Dinge besonders deutlich: Erstens sind die Unterschiedlichkeiten in den Strategien ein Beispiel für tatsächlich anzutreffende Varianzen auf Länderebene. Zweitens zeigt

sich in diesen Strategien das alle Bereiche von der Politik über die Wirtschaft bis zur Gesellschaft transformierende Wesen der Digitalisierung. Aus Sicht der Politik ist sie eine Querschnittsaufgabe, die alle Ressorts adressieren müssen. Gleichzeitig wird aufgrund der Vielzahl der Länderregelungen zu *Steuerungsarrangements* klar, dass vonseiten der Landesregierungen eine Notwendigkeit zur Gestaltung des bestehenden Akteurs- und Institutionengefuges für diese politikfeldübergreifende Herausforderung wahrgenommen wird.

Insgesamt kann damit ein Wechselspiel als stilprägend für die Rolle der Länder bei der Gestaltung der digitalen Transformation angenommen werden. Der Föderalismus wird einerseits als Hindernis interpretiert aufgrund von isolierten Ansätzen auf Länderebene und der Kosten von Bund-Länder-Verflechtungen. Auf der anderen Seite wird insbesondere die Innovationsfunktion der Länder betont, indem die verschiedenen Landesregierungen durch divergierende Schwerpunkte *Best Practices* schaffen – sei es durch organisatorische oder inhaltlich-strategische Varianzen.

---

### **3 Praktische Ausgestaltung: die Steuerungsarrangements**

Horizontale wie vertikale Kooperation quer zu den bestehenden Ressorts einer Landesregierung setzen eine entsprechende Organisation voraus. Dabei finden sich Varianzen sowohl in der Wahrnehmung von Notwendigkeiten als auch in der operativen Umsetzung von Steuerungs- und Organisationsfragen. Jedoch bilden sich erste gemeinsame Entwicklungsrichtungen von Ländern heraus.

Allen Ländern gemein ist mittlerweile die Position von Beauftragten der Landesregierung für Informationstechnik, auch *Chief Information Officer* (CIO) genannt. Diese können als IT-Verantwortliche der Länder bezeichnet werden, sind sie doch ressortübergreifend für die strategisch-organisatorische Steuerung der IT zuständig. Hessen war 2003 das erste Land, das eine solche Position geschaffen hat, die anderen Länder und auch der Bund (2007) folgten (Westerfeld 2015, S. 55) – ein Beispiel für Innovation, die aus den Ländern hervorgeht. Die Unterschiede beginnen jedoch bereits, wenn es um Kompetenzen und organisatorische Zuordnung geht (für das Folgende gilt: Stand Frühjahr 2019). Es gibt Minister, die gleichzeitig als CIO fungieren wie in Bayern und Hessen, Staatssekretäre, die diese Aufgabe wahrnehmen wie im Saarland oder in Brandenburg – das am häufigsten gewählte Modell –, und Abteilungsleiter als IT-Beauftragte wie in Baden-Württemberg oder Nordrhein-Westfalen. Minister mögen formal eine machtvollere Position einnehmen, müssen das Thema aber nicht zwingend priorisieren und sind häufig auch mit vielen anderen Themen befasst. Staatssekretäre oder Abteilungsleiter, die sich inhaltlich besser auskennen, können strategisch effektiver sein, wenn sie nicht zu viele andere Aufgaben wahrnehmen müssen, brauchen zur Umsetzung aber politische Unterstützung. Wie intensiv die jeweiligen CIOs ihre Anliegen vorantreiben können, hängt auch von finanziellen und personellen Ressourcen ab (Heuermann et al. 2018, S. 101–104). Die CIOs mit ihren Stäben können allgemein als (IT-bezogene) „Organisationsentwickler der Gesamtverwaltung“ (Heuermann et al. 2018, S. 103) verstanden werden, weshalb sie auch für das *E-Government* eine wichtige Rolle einnehmen. Mit wenigen Ausnahmen (Brandenburg, Schleswig-

Holstein) vertreten die CIOs ihre Länder im IT-Planungsrat. Dieser setzt sich aus den Ländervertretern und dem Bundes-CIO zusammen. Er dient der Kooperation und Koordination im bundesrepublikanischen Digital-Föderalismus und kann „als eine Art Architekt des föderalen Digitalhauses“ (Härtel 2018, S. 232) verstanden werden.

Analog zu den Steuerungsarrangements in Unternehmen etabliert sich in den Landesregierungen zunehmend auch die Position des *Chief Digital Officer* (CDO) (Hunnius et al. 2017, S. 13). In Abgrenzung zum CIO kümmert sich dieser weniger um IT-Steuerung, sondern um die übergreifende Steuerung der digitalen Transformation in Wirtschaft und Gesellschaft. Häufig ist der CDO auch für die koordinative Begleitung von Entwicklung, Umsetzung und Evaluation der Digitalstrategien zuständig. Der offizielle Titel des CDO existiert bisher in zwei Ländern: in Baden-Württemberg – dort in Personalunion mit dem CIO-Posten – und in Hamburg. Dazu kommen Steuerungslösungen, die einen impliziten CDO nahelegen. So gibt es etwa in Brandenburg oder Rheinland-Pfalz in der Staatskanzlei Digitalkoordinator\*innen auf Staatssekretärsebene; in Niedersachsen, Sachsen sowie in Sachsen-Anhalt sind diese im jeweiligen Wirtschaftsministerium angesiedelt.

In Baden-Württemberg, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Sachsen-Anhalt, Schleswig-Holstein und Thüringen hingegen kann man insofern von „X-Y-und Digitalministerien“ sprechen, als dass diese für die Steuerung der digitalen Transformation nicht nur eine eigene Abteilung eingerichtet, sondern Digitalisierung auch in den Namen des Ministeriums aufgenommen haben. Bayern und Hessen haben nach den Landtagswahlen im Oktober 2018 dem Namen nach reine Digitalministerien eingerichtet. Dabei ist das hessische „Digitalministerium“ in der Staatskanzlei angesiedelt, dürfte also eher einer Stabsstelle für besondere Aufgaben entsprechen. Dass mit der Aufnahme des Digitalisierungsbegriffs in den Namen des Ministeriums keine umfassende Verantwortlichkeit einhergehen muss, zeigt Sachsen-Anhalt. Trotz eines Ministeriums für Wirtschaft, Wissenschaft und Digitalisierung ist der CIO des Landes weiterhin im Finanzministerium verankert, auch um die Bindung an den Landeshaushalt nicht zu verlieren (Hunnius et al. 2017, S. 19).

Bei der ressortübergreifenden Zusammenarbeit, die bei der Querschnittsaufgabe Digitalisierung vonnöten ist, setzen einige Länder auf sogenannte Digitalisierungskabinette, die folgerichtig häufig auch in der Staatskanzlei institutionell verortet sind. Hierbei handelt es sich um mehr oder weniger regelmäßig tagende Ministerrunden. Rheinland-Pfalz hat eine solche Struktur zuerst installiert, auch Sachsen-Anhalt, Brandenburg und Schleswig-Holstein gehen so vor (Tab. 1) (Härtel 2017, S. 214). Die Bundesregierung greift dieses Steuerungsarrangement der Länderebene in dem Sinne auf, dass sie ihren Kabinettsausschuss für Digitalisierung als Digitalkabinett bezeichnet, auch wenn die Bildung von Kabinettsausschüssen bei anderen ressortübergreifenden Themen ebenso üblich ist (Bundesregierung 2019).

---

## 4 Varianzen in den Digitalstrategien

Beim strategischen Umgang mit der Digitalisierung entwickeln die Landesregierungen ihre inhaltlichen Schwerpunkte derzeit insbesondere in Form von Regierungsstrategien – die Diskussionen drehen sich längst nicht mehr um das „Ob“, sondern

**Tab. 1** Steuerungsarrangements der Digitalisierung in den Ländern

Mandatierung Gremien	Mandatierung Beauftragte	Organisatorische Ansiedlung	
Digitalisierungs-kabinette	CDO	X-Y-und Digitalministerium	Digitalministerium
Baden-Württemberg, Brandenburg, Rheinland-Pfalz, Sachsen-Anhalt, Schleswig-Holstein	Baden-Württemberg, Brandenburg, Hamburg, Niedersachsen, Rheinland-Pfalz, Sachsen, Sachsen-Anhalt	Baden-Württemberg, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Sachsen-Anhalt, Schleswig-Holstein, Thüringen	Bayern, Hessen*

Quelle: Eigene Recherche in den Organisationsplänen und auf den Webseiten der Ministerien sowie in den jeweiligen Digitalstrategien der Länder, angelehnt an die Unterscheidung bei Hunnius et al. 2017, S. 18

\*Hessen: dem Namen nach als Ministerium firmierend, der organisationalen Anbindung an die Staatskanzlei zufolge aber eher als Stabstelle zu interpretieren

um das „Wie“. Sie zielen darauf ab, komplexe, politikfeldübergreifende Problemkonstellationen zu adressieren und dabei aus Akteurssicht vereinheitlichende Lösungsansätze zu bieten, die nicht mit einem Dokument selbst enden, sondern prozessbegleitend angelegt sind. Abhängig vom Zeitpunkt, zu dem die Länder ihre Digitalstrategien erstellt haben, sind diese Strategien bereits auf die ein oder andere Weise vorgeprägt. Das kann durch europäische Strategien wie die „Digitale Agenda für Europa“ (Europäische Kommission 2010) oder Anforderungen der europäischen Strukturfonds, durch Programme auf Bundesebene wie die „Digitale Agenda 2014–2017“ der Bundesregierung (2014) sowie durch Initiativen anderer Länder der Fall sein. Der Blick auf digitale Vorreiter wie Estland, Dänemark oder Singapur, die in internationalen Ranglisten deutlich besser als Deutschland abschneiden, wirkt hier ebenso, auch infolge von Delegationsreisen in diese Länder.

Thematisch beschäftigen sich die Länderstrategien nicht nur mit Fragen der digitalen Infrastruktur oder der Technikausstattung der Verwaltung, sondern richten sich auf zentrale Politikfelder wie Wirtschafts- und Sozialpolitik, Bildung, Gesundheit, Landwirtschaft oder Verkehr. Mit Ausnahme der Stadtstaaten sowie des Saarlands haben (Stand: Frühjahr 2019) alle Länder ausführliche strategische Überlegungen zur digitalen Transformation entwickelt.

Wo zuvor noch ganz unterschiedliche Formate zu finden waren (etwa in Form von themenspezifischen Regierungserklärungen, Teilkapiteln in Koalitionsverträgen oder Maßnahmenprogrammen), setzt sich nun die ressortübergreifende Gesamtstrategie durch (Härtel 2017, S. 204). Bei den inhaltlichen Schwerpunkten lässt sich dagegen eine an unterschiedlichen Problembedarfen und länderspezifischen Prozessen ausgerichtete Eigenständigkeit beobachten, wie ein kurSORISCHER Überblick zeigt.

Schleswig-Holstein etwa hofft als Flächenland auf eine Attraktivitätssteigerung infolge der Flexibilisierung des Arbeitsortes, wenn Bürger\*innen verstärkt von Zuhause aus arbeiten können und entsprechend weniger geneigt sind, in wirt-

schaftsstarken Zentren umzuziehen (Heuermann et al. 2018, S. 115). Einflüsse der geografischen Lage werden in Niedersachsen, Hamburg oder Schleswig-Holstein auch daran deutlich, dass sich diese Länder auf Küsten- und Energiemanagement fokussieren. Nahezu alle Länder legen in ihren strategischen Ansätzen großen Wert auf die Förderung von kleinen und mittelständischen Unternehmen (Härtel 2017, S. 204–211). Berlin als selbsternannte „Start-up-Hauptstadt“ hat als erstes Land eine ausführliche Position zu einem spezifischen Thema der Transformation der Arbeitswelt erarbeitet und Handlungsfelder in Sachen *Crowdwork* und Plattformökonomie identifiziert (Expertise „Faire Arbeit in der Crowd“, Senatsverwaltung für Arbeit, Integration und Frauen, 2016). Im Politikfeld Bildung – einer zentralen Landeskompetenz – entstehen Pilotprojekte zum digitalen Lernen, aber auch, wie in Baden-Württemberg, zur Digital- und Medienkompetenz im Rahmen einer digitalen Bildungsoffensive des Landes (Hopf 2016, S. 39 f.).

Auffällig ist, dass – wie schon bei den diversen Steuerungslösungen – die Stadtstaaten sowie das Saarland abseits von Ausarbeitungen zu spezialisierten Fragen der Digitalisierung bisher keine übergreifenden Strategien entwickelt haben. Ein Grund könnte zumindest bei den Stadtstaaten sein, dass dort der geringere Problembedarf herrscht und davon ausgehend weniger Handlungsimpulse ausgelöst werden als in Flächenländern. Zu diesem Ergebnis kommt zumindest der mehrere Themenfelder abdeckende „Deutschland-Index Digitalisierung“ (Opiela et al. 2019), in dem die Stadtstaaten im Gesamtranking der Länder, aber auch in den meisten Einzelrankings Spitzenpositionen einnehmen. Demgegenüber werden die jeweiligen urbanen Profile zwar mit Konzepten zur Digitalen Stadt konkretisiert. Absichtserklärungen zur Entwicklung von übergreifenden Strategien in Berlin und Ankündigungen in Hamburg (Strategie für Januar 2020; Stellenaufbau im Amt für IT und Digitalisierung in der Senatskanzlei) zeigen aber, dass ein darüber hinaus bestehender Bedarf erkannt wurde.

---

## 5 Umsetzungsstand und Auswirkungen am Beispiel E-Government

Das Anwendungsbeispiel *E-Government* zeigt: Für die Landesverwaltungen bedeutet die digitale Transformation nicht nur eine Veränderung der Zugangswege für die Bürger\*innen via Dienstleistungsplattformen oder einen Wandel von Arbeitsprozessen durch die Einführung der sogenannten eAkte, die an sich schon mit vielen Fragen einhergehen, etwa des Datenschutzes oder des *digital divide*, sondern einen ganzheitlichen Organisationswandel, der Strukturen und Prozesse verändert.

Aus der Bürgersicht als Nutzer\*innen liegen die Schwierigkeiten unter anderem in der Vielzahl an verwendeten Plattformen und Anwendungen. Das Problem ist als generelles politisches Steuerungsproblem der horizontalen und vertikalen Versäulung bekannt. So wie in der Familienpolitik versucht wird, durch die sozialräumliche Bündelung von Unterstützungs- und Beratungsleistungen Zugangswege zu erleichtern und Synergien zu schaffen, sollten die Informationen und Leistungen im Sinne eines *One-Stop-Shops* auf einer zentralen Plattform vorliegen.

Eines der Ziele von *E-Government*-Strategien der Länder besteht deshalb darin, Wege zu finden, die heterogenen Strukturen und Entscheidungsrechte zu verbinden und zu integrieren, ohne technisch beschränkende *One-fits-all*-Lösungen. Statt dessen wird auf *Interoperabilität* gesetzt, d. h. auf eine niedrigschwellige Standardisierung, die vielfältige Anwender\*innen bzw. deren Zugriffswege zulässt. Mit der Föderalismusreform II wurde 2009 in Form des Art. 91c GG eine zusätzliche Gemeinschaftsaufgabe eingeführt, mit der Bund-Länder- bzw. Länder-Länder-Kooperationen bei der Nutzung von IT-Systemen geregelt wurden. Dies war nötig geworden, da der „Grundsatz eigenverantwortlicher Aufgabenwahrnehmung (...) einer gemeinsamem IT-Planung von Bund und Ländern entgegenzustehen“ (Peuker 2015, S. 76) schien. Diese Regelung wurde 2017 mit einer Ergänzung von Art. 91c GG und dem damit einhergehenden Onlinezugangsgesetz (OZG) noch einmal dahingehend spezifiziert, dass bis Ende 2022 nicht nur sämtliche Verwaltungsleistungen von Bund und Ländern über *Online*-Verwaltungsportale nutzbar sein müssen. Die Portale müssen zudem zu einem Portalverbund mit einheitlichem Benutzerkonto zusammengeführt werden. Dabei erhält der Bund Entscheidungsrechte zur Standardsetzung, die er durch Rechtsverordnungen im Benehmen mit dem IT-Planungsrat, aber ohne Zustimmung des Bundesrats vorschreiben kann.

Hier hat sich die föderalismuskritische Sichtweise offensichtlich durchgesetzt, der zufolge die Digitalisierung der Verwaltung zu langsam vonstattengeht. Ein Gutachten für den Normenkontrollrat (Fromm et al. 2015) resümierte in diesem Sinne, dass es über Informations- und vereinzelte Verwaltungsleistungen hinaus praktisch kein *E-Government* in Deutschland gebe. Ob fehlende Schwerpunktsetzung vonseiten der Regierungen oder fehlender Wettbewerbsdruck in den Verwaltungen – klar ist, dass Deutschland einen Nachholbedarf aufweist. Dies zeigt z. B. der Digitalindex der Europäischen Kommission (2018), der die digitalen Entwicklungsstände der EU-Mitgliedsstaaten jährlich in fünf Schwerpunkten misst. Während Deutschland insgesamt mit Platz 14 im Mittelfeld landet, werden die digitalen öffentlichen Dienste mit Rang 22 am schlechtesten von allen fünf Kategorien bewertet.

Auch wenn der gewählte Lösungsansatz für den benötigten Aufholprozess ‚im Schatten des Bundes‘ ausgeführt wird, bezieht die Umsetzung alle föderalen Ebenen ein. Die im Onlinezugangsgesetz identifizierten über 500 Verwaltungsleistungen, die bis Ende 2022 digitalisiert sein müssen, wurden dabei in 14 Themenfelder aggregiert. Für diese Themenfelder – z. B. Familie & Kind, Arbeit & Ruhestand oder Mobilität & Reisen – sollen das jeweilige Bundesministerium und mindestens ein Bundesland gemeinsam federführend Verantwortung übernehmen. Dass diese Kooperationsarrangements als „Digitallabore“ firmieren, weist auf die zugrunde liegende Experimentierfunktion hin. Positiv ist, dass durch die Übernahme der letzten offenen Position durch Bayern („Forschung & Förderung“) mittlerweile alle Themenfelder abgedeckt sind. Die Schwierigkeit der Aufgabe zeigt sich allerdings daran, dass der Normenkontrollrat weiterhin kritisch auf ausstehende Lösungen der Systemarchitektur zur Übertragung der gefundenen Lösungen in andere Länder (*Interoperabilität*) verweist (Nationaler Normenkontrollrat 2019). Während die Länderebene als Innovationslaboratorium also wichtige Impulse geben kann, darf sie bei übergreifenden Projekten

keine Hürde darstellen. Diese Ausprägung kann als eine zentrale föderalistische Vermittlungsleistung zwischen Vielfalt und Angleichung interpretiert werden.

---

## 6 Perspektiven der Digitalisierung im Föderalismus

Das Wechselspiel zwischen Zentralisierungsbedarfen und Innovationslaboratorien im Exekutivföderalismus ist unverkennbar. Insbesondere die Ergänzung von Art. 91c GG mit dem begleitenden Onlinezugangsgesetz zeigt aber auch: Die Innovationsbilanz des deutschen Föderalismus überzeugt noch nicht. Der Bund hat dies erkannt und ‚droht‘ nun mit klaren Fristen im Schatten der Hierarchie, nämlich der Möglichkeit, Standardisierungen im *E-Government* vorzugeben. Ebenso wäre es aber zu einfach, die wenig eindrucksvolle Performanz nur dem Föderalismus zuzuschreiben und damit ausschließlich zentralistischen Ansätzen das Wort zu reden. So zeigt eine international-vergleichende Studie zur Digitalisierung im Gesundheitssektor, die im Föderalismus zunächst ein Hemmnis erwartete, wie die Übernahme regional begrenzter *Best Practices* gegenüber zentralistisch implementierten Maßnahmen Vorteile generiert. Die Innovationsfunktion findet sich in diesem Schweizer Fall wieder. Entscheidend: Die Installation einer akteurs- und ebenenübergreifenden Steuerungsinstanz mit Entscheidungs- und Koordinierungsbefugnissen (Thiel et al. 2018, S. 345).

In der Bundesrepublik gibt es diese Instanz mit dem IT-Planungsrat, zumindest für den IT- und *E-Government*-Bereich. Diesen mit den entsprechenden Kompetenzen auszustatten, wäre ein erster Schritt. Mit den im OZG implementierten Digitallaboren zu 14 Themenfeldern wird durch die Verbindung von Bundesressorts und Landesregierungen überdies bereits angestrebt, horizontale wie vertikale Silostrukturen aufzubrechen. Zudem wäre zu fragen, warum Länder und Bund den Strategien (und den begleitenden Prozessen) zur Digitalisierung der Verwaltung offenkundig eine wichtige Rolle zusprechen, dies aber nicht in Form einer gemeinsamen Strategie weiterentwickeln.

Was die digitale Perspektive über *E-Government* hinaus angeht, ist die Situation noch unklarer. Inwiefern etwa die Digitalisierungskabinette vor allem als aufmerksamkeitsstarke Kommunikationsinstrumente nach außen wirken oder als eine Art digital-strategisches Zentrum mit zugehöriger fest installierter Arbeitsebene reüssieren, muss sich zeigen. Auch ob der Trend in der weitergehenden institutionellen Ausdifferenzierung eines eigenständigen Digitalministeriums wie in Bayern liegt, inwiefern CDOs analog zu den CIOs flächendeckende Einführung erfahren und ob hier dann ebenfalls vernetzende Arrangements entstehen, bleibt offen. Während die legitimatorisch-kommunikative Darstellungsebene mit den Strategiepublikationen adressiert wurde, muss es sich noch zeigen, ob die dort gelisteten Maßnahmen wie auch die gewählten Arrangements geeignet sind, sektorales Denken in den (Landes-) Regierungen zu überwinden, Digitalisierungsaspekte über die Ressorts hinweg zu integrieren und so neue Handlungsspielräume zu generieren.

## Literatur

- Bundesregierung. 2014. Digitale Agenda 2014–2017. [https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-agenda-legislaturbericht.pdf?\\_\\_blob=publicationFile&v=20](https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-agenda-legislaturbericht.pdf?__blob=publicationFile&v=20). Zugriffen am 12.01.2019.
- Bundesregierung. 2019. Digitalisierung. Steuerungs- und Beratungsgremien im Überblick. <https://www.bundesregierung.de/breg-de/themen/steuerungs-und-beratungsgremien-im-ueberblick-1548450>. Zugriffen am 19.02.2019.
- Europäische Kommission. 2010. Eine Digitale Agenda für Europa. <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52010DC0245&from=SK>. Zugriffen am 19.01.2019.
- Europäische Kommission. 2018. Digital Economy and Society Index (DESI) 2018. <https://ec.europa.eu/digital-single-market/en/desi>. Zugriffen am 15.02.2019.
- Fromm, Jens, Christian Welzel, Lutz Nentwig, und Mike Weber. 2015. E-Government in Deutschland. Vom Abstieg zum Aufstieg. <https://www.normenkontrollrat.bund.de/resource/blob/300864/753828/8defe142de7cd9d8cf5732b3258ced4c/2015-11-12-gutachten-egov-2015-data.pdf?download=1>. Zugriffen am 19.01.2019.
- Härtel, Ines. 2017. Digitale Staatskunst: Der Föderalismus als Laboratorium der digitalen Transformation. In *Jahrbuch des Föderalismus 2017*, Hrsg. Vorstand des Europäischen Zentrums für Föderalismus-Forschung Tübingen (EZFF), 197–220. Baden-Baden: Nomos.
- Härtel, Ines. 2018. Digitale Innovation, zweckrationale Organisation, föderale Kooperation: zur Entwicklung des E-Government in Deutschland. In *Jahrbuch des Föderalismus 2018*, Hrsg. Vorstand des Europäischen Zentrums für Föderalismus-Forschung Tübingen (EZFF), 227–240. Baden-Baden: Nomos.
- Heuermann, Roland, Krebs Stefan, Christian D. Kohl, Carsten Jürgens, Johann Bizer, und Michel Golibrzuch. 2018. Digitalisierung auf Landesebene. In *Digitalisierung in Bund, Ländern und Gemeinden. IT-Organisation, Management und Empfehlungen*, Hrsg. Roland Heuermann, Matthias Tomenendal und Christian Bressem, 99–136. Berlin: Springer.
- Hopf, Gregor. 2016. Digitalisierung im föderalen Kontext. Was erwartet die einzelnen föderalen Ebenen durch die Digitalisierung von Wirtschaft und Gesellschaft? In *Jahrbuch des Föderalismus 2016*, Hrsg. Vorstand des Europäischen Zentrums für Föderalismus-Forschung Tübingen (EZFF), 33–49. Baden-Baden: Nomos.
- Hunnius, Sirko, Dirk Stocksmeier, Stephan Löbel, und Tino Schuppan. 2017. *Digitalisierungsministerium oder Staatsminister? Bausteine moderner Steuerung des Politikfelds Digitalisierung im Hinblick auf die 19. Legislaturperiode im Bund*. Berlin: Stein-Hardenberg Institut.
- Nationaler Normenkontrollrat. 2019. Monitor Digitale Verwaltung #3. <https://www.normenkontrollrat.bund.de/resource/blob/72494/1675854/b0a14cedf388ddb05f2b9b9e3827b32d/2019-09-26-monitor-digitale-verwaltung-3-data.pdf>. Zugriffen am 02.01.2020.
- Opiela, Nicole, Jens Tiemann, Jan Dennis Gumz, Gabriele Goldacker, Basanta Thapa, und Mike Weber. 2019. Deutschland-Index der Digitalisierung 2019. <https://www.oeffentliche-it.de/documents/10181/14412/Deutschland+Index+der+Digitalisierung>. Zugriffen am 02.01.2020.
- Peuker, Enrico. 2015. Digitalisierung im Bundesstaat. Die Rolle des Föderalismus auf dem Weg zum digitalen Staat. In *Auf dem Weg zum digitalen Staat – auch ein besserer Staat?* Hrsg. Hermann Hill und Utz Schliesky, 59–86. Baden-Baden: Nomos.
- Thiel, Rainer, Lucas Deimel, Daniel Schmidtmann, Klaus Piesche, Tobias Hüsing, Jonas Rennoch, Veli Stroetmann, Karl Stroetmann, und Thomas Kostera. 2018. #SmartHealthSystems. Digitalisierungsstrategien im internationalen Vergleich. <https://www.bertelsmann-stiftung.de/de/publication/publikation/did/smarthealthsystems/>. Zugriffen am 19.01.2019.
- Westerfeld, Horst. 2015. IT-Governance als Aufgabe des CIO in der Öffentlichen Verwaltung. In *IT-Governance in Staat und Kommunen. Vernetzung, Zusammenarbeit und die Steuerung von Veränderungsprozessen in der öffentlichen Informationstechnik*, Hrsg. Andreas Engel, 55–61. Berlin: edition sigma.



---

# Datenschutzaufsicht

Magnus Römer und Lena Ulbricht

## Inhalt

1 Klärung des Begriffs .....	428
2 Theoretische Grundlagen .....	429
3 Aufsichtspraxis im Datenschutz .....	431
4 Umsetzungsstand und Auswirkungen .....	433
5 Perspektiven für Staat und Verwaltung .....	434
Literatur .....	435

---

## Zusammenfassung

Die digitale Transformation von Wirtschaft, Gesellschaft und Staat fordert die Datenschutzaufsicht grundlegend heraus: Die Erfassung von immer mehr personenbezogenen Daten und neue datenbasierte Geschäftsmodelle müssen mit dem Recht auf informationelle Selbstbestimmung in Einklang gebracht werden. Durch die Digitalisierung hat Datenschutz eine enorme politische Aufwertung erfahren, wie durch die Europäische Datenschutzgrundverordnung deutlich wurde. Doch auch bei einheitlichen rechtlichen Grundlagen können sich unterschiedliche Aufsichtsstile herausbilden, wie die Behördenpraxis im föderalen Deutschland zeigt. Verschiedene Aufsichtsstile haben jeweils Vor- und Nachteile. Sie leisten auch einen Beitrag zur Herausbildung einer Datenschutzkultur.

---

M. Römer

European New School of Digital Studies, Stiftung Europa-Universität Viadrina, Frankfurt (Oder),  
Deutschland

E-Mail: [roemer@europa-uni.de](mailto:roemer@europa-uni.de)

L. Ulbricht (✉)

Weizenbaum-Institut für die vernetzte Gesellschaft, Wissenschaftszentrum Berlin für  
Sozialforschung, Berlin, Deutschland

E-Mail: [lena.ulbricht@wzb.eu](mailto:lena.ulbricht@wzb.eu)

## Schlüsselwörter

Föderalismus · Rechtsdurchsetzung · Beratung · Sanktion · Koordination

### 1 Klärung des Begriffs

Datenschutz ist ein wichtiger Pfeiler des Gestaltungsanspruchs, den Staat und Verwaltung in der Digitalisierung besitzen. Da durch die Digitalisierung immer mehr personenbezogene Daten erhoben und miteinander verknüpft werden, steigt auch die Relevanz des Datenschutzes, der die Rahmenbedingungen für vielfältige digitale Anwendungen von Behörden und Unternehmen formuliert. Anders als der Name suggeriert, meint Datenschutz dabei weniger den Schutz von Daten – dieser Aspekt wird zumeist als Daten- oder Informationssicherheit bezeichnet. Datenschutz bezeichnet vielmehr die Selbstbestimmung von Individuen über Daten, die ihre Person betreffen, also die informationelle Selbstbestimmung. Das Politikfeld Datenschutz umfasst dabei zahlreiche Aspekte des Umgangs mit Daten, wie etwa das Erheben, Speichern, Verarbeiten und Interpretieren. Er ist dabei stets durch ein Spannungsfeld gekennzeichnet: Datenverarbeitung zu ermöglichen und sie zugleich zu begrenzen. Die Europäische Union hat sich des Datenschutzes angenommen, um grenzübergreifende Datentransfers und Innovationen zu ermöglichen (González Fuster 2014). Zugleich hat sie Datenschutz zur Bedingung des Schutzes der Menschwürde erklärt und ihn in der Charta der Grundrechte der EU verankert (Art. 8). Die erfolgreiche *Rechtsdurchsetzung* in der EU, insbesondere der Datenschutzgrundverordnung 2016/679 (DSGVO), der Richtlinie 2016/680 zum Datenschutz der Justiz- und Innenbehörden (JI-Richtlinie) sowie der *e-Privacy*-Verordnung, die die Richtlinie 2002/58/EG ersetzen soll, hängt dabei maßgeblich von der Gestaltung der Datenschutzaufsicht ab. Diese wird in allen EU-Mitgliedstaaten von unabhängigen staatlichen Datenschutzaufsichtsbehörden (*data protection authorities*) geleistet.

Datenschutz wird neben Aufsichtsbehörden durch weitere Akteure geprägt: die Individuen, die personenbezogene Daten generieren, die Organisationen aller Art, die diese erfassen und nutzen, die Datenschutzbeauftragten innerhalb von Organisationen sowie zivilgesellschaftliche Akteure. Die deutsche Datenschutzaufsicht ist *föderal* organisiert: Alle Länder verfügen über eine eigene Aufsichtsbehörde, Bayern über zwei und mit jener des Bundes sind es achtzehn. Im Kleinen ähnelt das deutsche System also den Verhältnissen in der Europäischen Union mit ihren 28 Mitgliedstaaten. Status und Aufgaben der Datenschutzaufsichtsbehörden in der EU wurden durch die DSGVO vereinheitlicht: Ihr Status muss von der Politik, anderen Behörden und Regel-Adressaten unabhängig sein. Ihre Aufgabe ist die Kontrolle der Anwendung der DSGVO. Trotz weitgehend einheitlicher rechtlicher Grundlagen haben Datenschutzaufsichtsbehörden unterschiedliche Praktiken entwickelt, so dass innerhalb der EU, aber auch innerhalb Deutschlands Unterschiede entstanden sind, die für die staatliche Gestaltung der Digitalisierung Vor- und Nachteile mit sich bringen.

## 2 Theoretische Grundlagen

Die föderale Organisation der Datenschutzaufsicht in Deutschland ist umstritten. *Policy-Vielfalt* kann zu Rechtsunsicherheit oder unterschiedlichen Lebensstandards führen. Mit Blick auf den Datenschutz fordert etwa die Wirtschaft, die Datenschutzaufsicht zu zentralisieren, damit aus ihrer Sicht Rechtssicherheit besteht. Sie wehrt sich dagegen, dass die Aufsichtsbehörden unterschiedliche Kontrollverfahren durchführen oder bei der Bewertung von Rechtskonformität unterschiedlich streng sind. Die Niederlassung eines Unternehmens in Berlin soll nicht anderen Standards unterworfen sein als eine Niederlassung in Bayern. Auch hinsichtlich des Lebensstandards besteht in Deutschland traditionell die Erwartung, dass Bürger\*innen sich in allen Regionen auf ein gleichmäßig hohes Datenschutzniveau verlassen können. Für ein dezentrales Modell spricht hingegen, dass föderale Vielfalt innovative Ansätze der Datenschutzaufsicht fördern, regionale Akteursnetzwerke und den Austausch zwischen Aufsichtsbehörden und Datenverarbeitern in einer Region stärken kann. Diese sind wichtig, da die Aufsichtsbehörden darauf angewiesen sind, dass Datenverarbeiter eigenständig darauf achten, Datenschutzrecht umzusetzen.

Ein wichtiges Motiv für die Schaffung unabhängiger Regulierungsbehörden (*independent regulatory agencies*) wie der Datenschutzaufsicht ist es, Märkte zu regulieren, ohne diese dem politischen Wettbewerb auszusetzen. Ein weiteres Motiv ist, dass unabhängige Regulierungsbehörden die Exekutive kontrollieren sollen, die durch die Globalisierung, die Europäisierung und Haushaltzwänge zulasten der Legislative immer stärker wird. Im deutschen Datenschutzregime kontrollieren die Aufsichtsbehörden in der Tat nicht nur Unternehmen, Vereine, oder sonstige nicht-öffentliche Stellen, sondern auch staatliche Behörden, darunter Ministerien und Strafverfolgungsbehörden. Ihre Unabhängigkeit, insbesondere von Ministerien und anderen Behörden, verleiht Datenschutzaufsichtsbehörden somit relativ große Macht. Datenschutzaufsichtsbehörden können z. B. Untersuchungen gegen andere Behörden einleiten oder diese öffentlich kritisieren.

Zwischen unabhängigen Regulierungsbehörden gibt es große Unterschiede: Sie genießen verschiedene Grade an (formaler oder faktischer) Unabhängigkeit, verfügen über unterschiedlich große Handlungsressourcen und wenden unterschiedliche Arbeitsweisen an (Gilardi und Maggetti 2011). Die Arbeit der Datenschutzaufsichtsbehörden ist durch ihre indirekte demokratische Legitimation geprägt: Die Leitung wird durch das Parlament oder die Regierung beauftragt, aber nicht direkt von Bürgerinnen und Bürgern gewählt. Um ihre gesellschaftliche Akzeptanz zu erhöhen, bauen unabhängige Regulierungsbehörden deshalb auf prozedurale Eigenlegitimität. Diese entsteht durch einen vermehrten Austausch mit Regel-Adressaten (Döhler 2006). Dieser Austauschprozess ist zumeist von einem Wechselspiel zwischen *Beratung* und *Sanktion* geprägt, in dem beide Seiten voneinander lernen und Vertrauen aufbauen (Gunningham 2012). Vertrauen entsteht etwa, wenn Regel-Adressaten der Behörde sektorspezifisches Wissen übermitteln und bei der Entwicklung von Leitlinien mitwirken können; allerdings bleibt das Vertrauen durch die Kontrollsituation und die Androhung von Sanktionen stets fragil (Wright und de

Hert 2016). Grundsätzlich sind für einen erfolgreichen Regulierungsprozess Instrumente beider Natur wichtig: Während *sanktionierende* Instrumente eine abschreckende Wirkung haben sollen, dienen *beratende* Maßnahmen der Vertrauensbildung, der Überzeugung und Lernprozessen. Doch die Aufsicht kann nicht allein auf Beratung setzen: Zum einen, weil auf diesem Weg nicht alle Datenverarbeiter zu erreichen sind, zum anderen weil ein zu enges Vertrauensverhältnis zu den Regel-Adressaten die Unabhängigkeit der Aufsicht gefährdet, z. B. wo diese verpflichtet ist, die Öffentlichkeit über Verstöße zu informieren.

In welchem Ausmaß und aus welchen Motiven heraus Aufsichtsbehörden stärker beratend oder sanktionierend handeln und ob sich hier Unterschiede zwischen den Behörden in Bund und Ländern zeigen, ist auch deshalb interessant, weil eine solche Analyse Regel-Adressaten für die Gestaltung der Datenschutzpolitik unter einem vereinheitlichten Rechtsrahmen Impulse liefert. Erkenntnisse über den Föderalstaat Deutschland können somit für die Gestaltung der Datenschutzaufsicht in der EU und ihren Mitgliedstaaten von Bedeutung sein.

In Deutschland besteht ein einheitlicher rechtlicher Rahmen für den Datenschutz bereits länger als auf europäischer Ebene. 1970 wurde das erste Landesdatenschutzgesetz in Hessen geschaffen und seit 1995 hat die Richtlinie 95/46/EG die Datenschutzgesetzgebung in Deutschland vereinheitlicht. Die DSGVO hat diese Vereinheitlichung weiter vorangetrieben. Sie ist bereichsübergreifend und regelt somit den Datenschutz in allen Bereichen – mit Ausnahme des Datenschutzes in den Bereichen Justiz und Inneres, die stattdessen der Richtlinie 2016/680 unterworfen sind. Zusätzlich zum allgemeinen Datenschutz regeln in Deutschland verschiedene nationale Gesetze den bereichsspezifischen Datenschutz, z. B. im Arbeits-, Gesundheits- oder Asylrecht.

Neben den europäischen Rechtsnormen wird das Datenschutzrecht für den nicht-öffentlichen Bereich, z. B. für private Unternehmen, durch das Bundesdatenschutzgesetz geregelt (BDSG). Auch das Datenschutzrecht für Post, Telekommunikation sowie Bundesbehörden wird auf Bundesebene entschieden. Die Landesgesetzgeber entscheiden über den Datenschutz bei Landesbehörden und Kommunen, weshalb jedes Land über ein eigenes Landesdatenschutzgesetz (LDSG) verfügt. Die Kirchen sind davon ausgenommen und regeln den Datenschutz eigenverantwortlich. Ein Vergleich der Landesgesetze vor ihrer Anpassung an die DSGVO im Mai 2016 zeigte, dass die Aufgaben und Kompetenzen der Aufsichtsbehörden in den Ländern in vielen Aspekten übereinstimmten. Schon der Aufbau der Gesetze zeigte große Gemeinsamkeiten, was auf eine Orientierung am Bundesgesetz zurückging. Weitere Übereinstimmungen sind die informationelle Selbstbestimmung, das Zweckbindungsprinzip und das Bekenntnis zu einer institutionalisierten, unabhängigen Kontrolle (Simitis 2011, S. 79 ff.). Auch das Bundesverfassungsgericht hat durch seine Entscheidungen dazu beigetragen, dass die Landesdatenschutzgesetze nicht drastisch voneinander abweichen.

Zu den allgemeinen Aufgaben der Aufsichtsbehörden gehören die Beratung von Datenverarbeitern, einschließlich Zertifizierung und Auditierung einzelner Produkte bzw. Verfahren, ihre Überprüfung sowie das Bereitstellen von Expertise in Gerichtsverfahren und in Gesetzgebungsprozessen. Im Bereich der Prüfungen gibt es erheb-

liche Unterschiede zwischen öffentlichen und nicht-öffentlichen Datenverarbeitern, dies ist jedoch in allen Ländern ähnlich geregelt: Können Verstöße durch Unternehmen mit Bußgeldern und Gerichtsverfahren geahndet werden, gibt es im öffentlichen Bereich keine entsprechenden Möglichkeiten, sondern nur Mahnungen. Weitere Aufgaben der Aufsicht sind die öffentliche Kommentierung gesellschaftlicher und technischer Entwicklungen sowie die Sensibilisierung und Bildung der Bevölkerung.

Vor dem Inkrafttreten der DSGVO zeigten sich moderate Unterschiede in den Datenschutzgesetzen der Länder und des Bundes. So schufen manche Länder die Rechtsgrundlage für Datenschutzaudits, d. h. die Prüfung des Datenschutzkonzepts einer öffentlichen Stelle, das erstmals von Datenschutzaufsichtsbehörden in Schleswig-Holstein und Brandenburg eingeführt wurde (Simitis 2011, S. 112). Auch die maximale Höhe potenzieller Geldbußen gegen Unternehmen unterschied sich; sie schwankte zwischen 25.000 (Sachsen, Hamburg, Bremen, Baden-Württemberg) und 250.000 Euro (Sachsen Anhalt). Darüber hinaus gab es nur noch Detailunterschiede zwischen den Landesgesetzen (Römer und Ulbricht 2018). In den Landesgesetzen ab 2018 finden sich die Bestimmungen zu Audits im Übrigen nicht mehr, da die entsprechenden Prozesse über die DSGVO festgelegt werden und die jeweiligen Verfahren neu bestimmt werden müssen.

---

### 3 Aufsichtspraxis im Datenschutz

Trotz der größtenteils einheitlichen Rechtslage ist die Praxis der Datenschutzaufsicht in Deutschland durch Vielfalt geprägt und es haben sich regionale Tätigkeitsschwerpunkte und Expertisen herausgebildet. Für die Gestaltung der Datenschutzaufsicht ist die föderale *Koordination* wichtig. Obwohl sie dazu rechtlich nicht verpflichtet waren, haben sich die Aufsichtsbehörden von Bund und Ländern 1978 ein Koordinationsforum gegeben: die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK). Sie tagt etwa im halbjährlichen Rhythmus unter Ausschluss der Öffentlichkeit; seit 2015 operiert die Konferenz mit einer Geschäftsordnung. Unter ihrem Dach haben sich zahlreiche Arbeitskreise zu einzelnen Themenbereichen gebildet. Am prominentesten ist der „Düsseldorfer Kreis“, der sich mit der Datenschutzaufsicht im nicht-öffentlichen Bereich befasst. Ein zentrales Ziel der Konferenz ist es, die Aufsicht über den Datenschutz in Deutschland konsistent zu gestalten. Zu ihren Ergebnissen gehören gemeinsame Publikationen zur Gestaltung des Datenschutzes und zur Bewertung von Rechtskonformität, die sich an Daten verarbeitende Unternehmen und Behörden sowie an die Aufsichtsbehörden richten. Dazu zählen etwa zahlreiche „Kurzpapiere“ zur Auslegung der DSGVO, Entschließungen, Beschlüsse und Orientierungshilfen, zum Beispiel zu datenschutzkonformer Videoüberwachung (DSK 2014). Nicht zuletzt erarbeitet die Konferenz politische Positionen, die dann von ihren gewählten Vertreter\*innen in Gesetzgebungsprozessen und auf europäischer Ebene vertreten werden. Die formale Bindungskraft der DSK-Beschlüsse ist unterschiedlich. Allgemein gilt, dass die Landesbehörden geringen Druck verspüren, Beschlüsse der Konferenz umzusetzen, da keine Sanktionen zu befürchten sind. Lange Jahre galt die Praxis, Beschlüsse einstimmig zu fällen, was zu Kompromissen führte,

aber die Bereitschaft förderte, diese auch umzusetzen. In letzter Zeit, gestärkt durch die neue Geschäftsordnung, werden zunehmend Mehrheitsbeschlüsse gefasst. Dies kann bei Meinungsverschiedenheiten zu einer geringen Umsetzungsmoral führen. Die DSK ist somit durchaus ein Treiber einheitlicher Datenschutzpolitiken, lässt den einzelnen Behörden jedoch Handlungsspielräume.

Trotz des regelmäßigen Austauschs untereinander haben die deutschen Aufsichtsbehörden unterschiedliche Praktiken und Schwerpunkte entwickelt. Die Leitungen der Behörden pflegen unterschiedliche Selbstverständnisse, welche sich zwischen den Idealtypen „beratend“ und „sanktionierend“ bewegen und sich auf die Aufsichtspraxis auswirken. Insbesondere vier Instrumente gelten als sanktionierend: Unangekündigte Kontrollen, Bußgelder, die Klage bzw. das Anrufen von Untersuchungsausschüssen sowie das Publik machen von Verstößen, z. B. in Jahresberichten. Zu den beratenden Maßnahmen zählen schriftliche Orientierungshilfen, Bildungsprogramme, Schulungen, Sprechstunden, das Verleihen von Datenschutzzertifizierungsgütesiegeln für IT-Produkte und -Dienstleistungen sowie Audits für Daten verarbeitende öffentliche Stellen und ihre IT-Verfahren.

In der Praxis zeigt sich, dass alle Aufsichtsbehörden sowohl sanktionierende als auch beratende Maßnahmen einsetzen, jedoch in unterschiedlicher Gewichtung. Besonders die Instrumente der anlasslosen sowie der unangekündigten Kontrolle werden unterschiedlich häufig eingesetzt. Aufsichtsbehörden, die Sanktionen bewusst einsetzen, waren etwa jene in Schleswig-Holstein unter Thilo Weichert (2004–2015), jene in Rheinland-Pfalz unter Edgar Wagner (2007–2015), jene des Bundesbeauftragten für den Datenschutz und die Informationssicherheit (BfDI) Peter Schaar (2003–2013) sowie bis heute die Behörden in Berlin und Hamburg. Entsprechend gibt es ein Nord-Süd-Gefälle der Aufsichtspraxis, mit einem tendenziell stärker sanktionierenden Norden und einem eher beratenden Süden. Diese Dichotomie ist allerdings nicht umfassend und scheint sich in den letzten Jahren aufzuweichen (Römer und Ulbricht 2018).

Allgemein werden Sanktionen jedoch selten eingesetzt. Dies hängt zum Teil mit den mangelnden Ressourcen der Behörden zusammen. Ein Mangel an Personal führt dazu, dass die Aufsicht nur einen Bruchteil der Regel-Adressaten tatsächlich kontrollieren kann und Datenschutzverstöße nicht entdeckt werden. Kontrollen folgen meist auf konkrete Beschwerden und münden aufgrund der Ressourcenlastigkeit des Rechtsweges nur selten in Sanktionen. Auch das für den öffentlichen Bereich vorgesehene Instrument der Beanstandung wird nur angewendet, wenn keine Veränderung auf eine von der Aufsicht geäußerte Beschwerde folgt. Die für Bundesbehörden als *ultima ratio* verstandene Anrufung des Parlaments hat noch nie stattgefunden. Während sanktionierende Instrumente im Bundesvergleich ungleich eingesetzt werden, herrscht hinsichtlich beratender Maßnahmen relative Einheitlichkeit: Alle Landesbehörden haben diesen Tätigkeitsschwerpunkt in den letzten fünf bis zehn Jahren ausgebaut. Diese gemeinsame Tendenz wird zum einen mit gestiegenen Anforderungen begründet: Das gesellschaftliche Interesse an Datenschutz und die damit einhergehende Zunahme an Eingaben, also die Bitte um Prüfung von datenschutzrechtlichen Sachverhalten, erfordert strategische und vorbeugende Maßnahmen.

Weitere Unterschiede gibt es mit Blick auf die Bereitschaft, sich in mediale Debatten einzubringen. Auch hier lassen sich die Aufsichtsbehörden bzw. ihre Leitungspersonen in jene aufteilen, die in offene Konfrontation treten, und jene, die sich als Vermittler verstehen. Als besonders medienpräsent galten in jüngerer Vergangenheit etwa Peter Schaar, Thilo Weichert und Johannes Caspar (Hamburg seit 2009). Andrea Voßhoff (BfDI 2013 bis 2018) sowie andere Landesbeauftragte nutzten die Medienöffentlichkeit eher moderat.

Jenseits der Balance zwischen Beratung und Sanktion haben die Landesbehörden auch bestimmte Expertisen entwickelt. So legen Rheinland-Pfalz und Hessen ein besonderes Augenmerk auf den Datenschutz bei Polizei und Justiz, während Schleswig-Holstein sich auf die Kontrolle von Unternehmen konzentriert. Andere Aufsichtsbehörden kümmern sich besonders um Bildung und Selbstdatenschutz, etwa Hamburg, Thüringen, Rheinland-Pfalz, Berlin und Mecklenburg-Vorpommern. Einen Schwerpunkt auf die Gesundheitswirtschaft legen Berlin, Nordrhein-Westfalen und Bayern. Baden-Württemberg, Thüringen, Niedersachsen, Bayern und Schleswig-Holstein spezialisieren sich auf autonomes Fahren. Hessen überprüft besonders Banken und Versicherungen. Manche Behörden entwickeln darüber hinaus spezielle technische Fähigkeiten: Mecklenburg-Vorpommern leitet den Arbeitskreis Technik der DSK und Schleswig-Holstein hat umfassende Expertise im technologischen Datenschutz aufgebaut. Diese Schwerpunkte entstehen durch das Engagement innerhalb von Behörden, werden aber zum Teil auch zwischen den Behörden koordiniert. Bereichsspezifisches Fachwissen wird in Fachkreisen und Arbeitsgruppen der DSK sowie bei Bedarf bilateral geteilt. Nicht zuletzt gibt es besondere Verfahrensexpertisen: Die Bayerische Behörde für den nicht-öffentlichen Bereich hat zahlreiche länderübergreifende Prüfungen angestoßen und Berlin pflegt seit Jahren die weltweite Vernetzung von Datenschutzaufsichtsbehörden. Trotz weitgehend einheitlicher Rechtslage sowie der DSK als Gremium freiwilliger Koordination hat die föderale Architektur der deutschen Datenschutzaufsicht also in mehrfacher Hinsicht auch Vielfalt hervorgebracht.

---

## 4 Umsetzungsstand und Auswirkungen

Über die Gründe für die Unterschiede innerhalb der deutschen Datenschutzaufsichtspraxis ist wenig bekannt. Eine explorative Studie (Römer und Ulbricht 2018) hat erste Determinanten identifiziert: Eine relevante Dimension betrifft die allgemeine Regulierungskultur eines Landes. So haben behördliche Anweisungen in einigen Bundesländern mehr Gewicht als in anderen und Mahnungen der jeweiligen Datenschutzaufsichtsbehörde an öffentliche Stellen wird schneller Folge geleistet. Der zweite Einflussfaktor ist die regionale Wirtschaftsstruktur, die die Grundlage für die Herausbildung bestimmter Expertisen, etwa bezüglich des Datenschutzes in der Gesundheitswirtschaft, in der Automobilindustrie oder im Bankenwesen bietet. Nicht zuletzt scheint die Persönlichkeit der Behördenleitung aufgrund der geringen

Mitarbeiterzahl vieler Datenschutzaufsichtsbehörden eine überdurchschnittlich große Bedeutung für die Aufsichtspraxis zu haben. Anders als in anderen Politikfeldern spielt die parteipolitische Zusammensetzung der jeweiligen Landesregierung nach jetzigem Kenntnisstand keine Rolle für die Datenschutzaufsicht. Dies könnte an der weitreichenden Unabhängigkeit der Datenschutzaufsichtsbehörden liegen. Darüber hinaus weisen die Parteien zwar geringfügige Unterschiede in ihrer datenschutzpolitischen Programmatik auf (etwa bezüglich der Vorratsdatenspeicherung), doch nicht bezüglich der Aufsichtspraxis.

Welcher Mix aus beratenden und sanktionierenden Maßnahmen das beste Datenschutzniveau zeitigt, ist bislang nicht erforscht. Gleiches gilt für die besten Bedingungen für Innovationen durch Datenverarbeitung. Entsprechende Studien müssen mit dem Problem umgehen, dass es keine Statistik der Datenschutzverstöße in Deutschland und in der EU gibt und die Aufsichtsbehörden keine einheitlichen Tätigkeitsberichte verfassen. Für EU-weite Vergleiche lassen sich zumindest Eurobarometer-Fragen heranziehen, die Einstellungen zum Datenschutzniveau und zur Datenschutzpolitik messen – allerdings nicht im Bundesländervergleich. Bei der Bewertung des Datenschutzniveaus und der Datenschutzaufsicht ist jedoch zu beachten, dass sich die Struktur der Datenverarbeiter regional unterscheidet und Aufsichtsbehörden somit mit ganz unterschiedlichen Herausforderungen konfrontiert sind. Datenverarbeiter, deren Geschäftsmodell auf der Verletzung von Datenschutzrecht beruht, sind nicht in der Mehrheit. Sie sind jedoch besonders schwer kontrollierbar und machen sanktionsrerende Elemente notwendig. Viele andere Datenverarbeiter benötigen hingegen Beratung, weil sie klein sind und über wenig datenschutzrechtliche Expertise verfügen, wie es etwa bei Arztpaxen der Fall ist. Vor diesem Hintergrund ist es zweckmäßig, dass sich unterschiedliche Aufsichtsstile herausgebildet haben.

---

## 5 Perspektiven für Staat und Verwaltung

Digitalisierung fordert die Datenschutzaufsicht grundlegend heraus: Die ständige und unsichtbare Erhebung von Daten und deren Verknüpfung lassen immer mehr Daten zu personenbezogenen Daten werden. Und immer mehr Unternehmen entwickeln datenbasierte Geschäftsmodelle, die leicht mit Datenschutzrecht in Konflikt geraten können. Eine besondere Herausforderung für die Datenschutzaufsicht sind international agierende Technologie-Konzerne und monopolistisch strukturierte Märkte. Im internationalen Vergleich setzt das EU-Recht der Verarbeitung von Daten besonders enge Grenzen und schützt die informationelle Selbstbestimmung seiner Bürger\*innen.

Die gestiegenen Anforderungen an die Datenschutzaufsicht führen zu einem verschärften Ressourcenproblem. Wo unabhängige Behörden aufgrund von Personalmangel von Sanktionen Abstand nehmen, scheitert der staatliche Gestaltungsspruch in der Digitalisierung. Die in Deutschland etablierte Arbeitsteilung zwischen den Aufsichtsbehörden in Bund und Ländern schafft ein wenig Abhilfe, kann das Problem jedoch nicht lösen. Darüber hinaus ist eine vergleichbare Ausstattung der Behörden eine Voraussetzung für produktive Kooperation – dies gilt im besonderen Maße für die innereuropäische Zusammenarbeit der Datenschutzaufsichtsbehörden. Sowohl inner-

halb Deutschlands als auch innerhalb der EU sind Aufsichtsbehörden mit Blick auf die Personalstärke pro Einwohner noch sehr unterschiedlich ausgestattet.

Durch die Digitalisierung hat Datenschutz aber auch eine enorme politische Aufwertung erfahren. So war die DSGVO, eine der größten Reformen in der Geschichte der Datenschutzgesetzgebung in der EU, in erster Linie durch die technische Entwicklung motiviert. Durch die Vorbereitung der Reform wurde auch innerhalb Deutschlands der Datenschutz weiter politisiert und die Aufsichtsbehörden haben eine Profilschärfung durchlaufen. Die Erfahrung der Datenschutzaufsicht in Deutschland hat gezeigt, dass sich auch bei einheitlichen rechtlichen Grundlagen verschiedene Aufsichtsstile herausbilden können. Diese haben ihre jeweiligen Vor- und Nachteile und jede Behörde entwickelt den Mix, den sie für ihre Region angemessen findet. Mit Blick auf ein hohes Datenschutzniveau ist jedoch wichtig, dass kein Regulierungswettbewerb entsteht, in dem Aufsichtsbehörden durch eine laxe Regeldurchsetzung Unternehmen anlocken. Einen solchen Unterbietungswettbewerb abzustellen, war eines der Ziele der DSGVO. In Deutschland allerdings ist Datenschutzaufsicht bislang kein Standortfaktor für Unternehmen – trotz der Vielfalt in der Aufsichtspraxis. Dies liegt daran, dass die deutschen Aufsichtsbehörden sich eng abstimmen und eine gemeinsame Datenschutzkultur erarbeitet haben.

Auch auf EU-Ebene existierte seit 1996 ein Koordinierungsgremium der Datenschutzaufsichtsbehörden, die sogenannte Artikel-29-Arbeitsgruppe. Mit Umsetzung der DSGVO wurde sie zum Europäischen Datenschutzausschuss (EDSA), der als festes Gremium weitreichende Kompetenzen besitzt: Sind sich nationale Aufsichtsbehörden uneins, wie in einem Fall grenzübergreifender Datenverarbeitung gehandelt werden soll, kann der Ausschuss EU-weit bindende Beschlüsse fällen, um eine einheitliche Rechtsdurchsetzung zu gewährleisten. Nur durch engen Austausch können die vielen Behörden mit sehr verschiedenen Datenschutzkulturen eine europäische Datenschutzkultur schaffen. Diese ist notwendig, um das geltende Recht auch zu implementieren. Datenschutzaufsicht im digitalen Zeitalter kann nur dort erfolgreich sein, wo sie auf einem Minimalkonsens hinsichtlich so vielfältig aufgeladener Konzepte wie unternehmerischer Freiheit, Privatheit und Menschenwürde beruht.

---

## Literatur

- Döhler, Marian. 2006. Regulative Politik und die Transformation der klassischen Verwaltung. In *Politik und Verwaltung. Politische Vierteljahresschrift Sonderheft 37*, Hrsg. Jörg Bogumil, Werner Jann und Frank Nullmeier, 208–227. Wiesbaden: Springer.
- DSK. 2014. Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen der Datenschutzkonferenz des Bundes und der Länder. [https://www.datenschutzkonferenz-online.de/media/oh/20140219\\_oh\\_videoueberwachung.pdf](https://www.datenschutzkonferenz-online.de/media/oh/20140219_oh_videoueberwachung.pdf).
- Gilardi, Fabrizio, und Martino Maggetti. 2011. The independence of regulatory authorities. In *Handbook on the politics of regulation*, Hrsg. David Levi-Faur, 201–214. Cheltenham: Edward Elgar Publishing.
- González Fuster, Gloria. 2014. *The emergence of personal data protection as a fundamental right of the EU*. Dordrecht: Springer.

- Gunningham, Neil. 2012. Enforcement and Compliance Strategies. In *The Oxford Handbook of Regulation*, Hrsg. Robert Baldwin, 120–145. Oxford: Oxford University Press.
- Römer, Magnus, und Lena Ulbricht. 2018. Vielfalt und Einheitlichkeit in der deutschen Datenschutzaufsicht. Zwischen Beratung und Kontrolle. Konferenzpapier vorgestellt auf dem VI. Interdisciplinary Workshop Privacy, Data Protection & Surveillance, Bochum.
- Simitis, Spiros. 2011. Einleitung – Geschichte – Ziele – Prinzipien. Geschichte der Datenschutzgesetzgebung. In *Bundesdatenschutzgesetz: Kommentar*, 7. Aufl. Baden Baden: Nomos.
- Wright, David, und Paul de Hert, Hrsg. 2016. *Enforcing privacy. regulatory, legal and technological approaches*. Cham: Springer.



---

# Digitalisierung von Verwaltungsleistungen in Bürgerämtern

Christian Schwab, Jörg Bogumil, Sabine Kuhlmann und  
Sascha Gerber

## Inhalt

1 Klärung der Begriffe .....	438
2 Theoretischer Bezug .....	439
3 Digitale Leistungserbringung in Bürgerämtern .....	439
4 Umsetzungsstand und Auswirkungen .....	441
5 Perspektiven für Staat und Verwaltung .....	444
Literatur .....	447

---

## Zusammenfassung

Die Digitalisierung der öffentlichen Leistungserbringung für die Bürger bildet gegenwärtig einen Schwerpunkt der Modernisierungsaktivitäten in Staat und Verwaltung. Hinsichtlich der digitalen Informationsbereitstellung hat es zwar deutliche Fortschritte gegeben, insgesamt zeigt sich jedoch eine allenfalls moderate „E-Government-Performanz“ bei der digitalen Kommunikation zwischen Verwaltung und Bürgern sowie bei Transaktionen, d. h. der medienbruchfreien Abschließbarkeit von Verwaltungsvorgängen. Als wesentliche Gründe für die ernüchternde Bilanz der lokalen Verwaltungsdigitalisierung sind neben techni-

---

C. Schwab (✉)

Universität Potsdam, Potsdam, Deutschland

E-Mail: [chschwab@uni-potsdam.de](mailto:chschwab@uni-potsdam.de)

J. Bogumil

Ruhr-Universität Bochum, Bochum, Deutschland

E-Mail: [joerg.bogumil@rub.de](mailto:joerg.bogumil@rub.de)

S. Kuhlmann

Universität Potsdam, Potsdam, Deutschland

E-Mail: [sabine.kuhlmann@uni-potsdam.de](mailto:sabine.kuhlmann@uni-potsdam.de)

S. Gerber

Fakultät für Sozialwissenschaft, Ruhr-Universität Bochum, Bochum, Deutschland

E-Mail: [sascha.gerber@rub.de](mailto:sascha.gerber@rub.de)

ischen, rechtlichen, finanziellen und personellen Barrieren insbesondere politische und institutionelle Hürden zu nennen. Viele Probleme sind zudem auch bei *E-Government*-Funktionen (z. B. der *Online*-Formulare oder elektronischen Bezahlmöglichkeiten) zu verzeichnen. Positiv schneidet dagegen die elektronische Terminvergabe ab, die in den Bürgerämtern zu wesentlichen Prozess- und Serviceverbesserungen geführt hat. Allerdings sind neben positiven Effekten, wie beispielsweise schnelleren Bearbeitungszeiten und kürzeren Wartezeiten, auch dysfunktionale Digitalisierungseffekte zu verzeichnen, wie erhöhter Arbeitsstress aufgrund eines gestiegenen Kommunikationsaufkommens (v. a. durch *Email*) und der damit einhergehenden Verlagerung des Arbeitsaufkommens vom *Frontoffice* ins *Backoffice*.

---

### Schlüsselwörter

E-Government · Verwaltungsmodernisierung · Bürgerämter · Verwaltungsdigitalisierung · Digitale Leistungserbringung

---

## 1 Klärung der Begriffe

Die Digitalisierung von Verwaltungsvorgängen, oft auch als *E-Government* (oder seltener *E-Governance*) bezeichnet (Homburg 2018, S. 348), ist schon seit Jahrzehnten ein beliebtes Modernisierungsthema. Dabei geht es nicht nur um die schon seit den 1990er-Jahren weit fortgeschrittene Überführung analoger Daten in digitale Speicherformate, sondern um die Einführung neuer Organisationsmodelle, die eine möglichst vollständige elektronische Abbildung der Kommunikationswege zwischen Kunden/Bürgern und Anbietern/Behörden leisten (Heuermann et al. 2018, S. 1).

Bürgerämter sind mittlerweile in allen deutschen Kommunen mit über 15.000 Einwohnern implementiert und können als eines der wichtigsten Erfolgsmodelle der lokalen Verwaltungsmodernisierung in Deutschland herausgestellt werden (Kuhmann und Wollmann 2014, S. 222 ff.). Sie zeichnen sich dadurch aus, dass sie die meisten publikumsintensiven Dienstleistungen für die Bürger an einer Stelle bündeln und es ihnen somit ermöglichen, für diese Dienstleistungen nur ein Amt aufzusuchen zu müssen (*one-stop-shop*). In fast allen Bürgerämtern hat sich zudem ein kombiniertes Angebot zwischen einem meist im Rathaus ansässigen zentralen Bürgeramt mit einigen dezentralen Außenstellen herauskristallisiert. Bürgerämter sind daher die zentrale Kontaktfläche der Kommunalverwaltung mit den Bürgern und haben sich vor diesem Hintergrund zu einem wesentlichen Dreh- und Angelpunkt der Digitalisierung in Kommunen entwickelt.

Die Digitalisierung hat die kommunale Leistungserbringung in Bürgerämtern zweifellos verändert. Wie ist der Stand der Umsetzung von digitalisierten Verwaltungsvorgängen, welche Hemmnisse treten dabei auf und welche Wirkungen sind erkennbar (vgl. Bogumil et al. 2019; Schwab et al. 2019).

## 2 Theoretischer Bezug

Um den Grad der Digitalisierung von Verwaltungsleistungen und die „Digitalisierungstiefe“ analytisch zu erfassen, empfiehlt sich ein Rückgriff auf *E-Government*-Entwicklungsmodelle (für einen Überblick siehe Coursey und Norris 2008, S. 524). Diese unterscheiden in der Regel verschiedene Stufen der Digitalisierungstiefe und bilden damit unterschiedliche „Fortschrittsgrade“ der digitalen Leistungserstellung in Bezug auf deren Komplexität und Wertschöpfungstiefe ab (vgl. Wirtz und Piehler 2010, S. 12 f.). Bei der Digitalisierung von Verwaltungsleistungen in deutschen Bürgerämtern erscheint eine dreistufige Klassifikation ausreichend und angemessen. Demnach lässt sich die Digitalisierungstiefe abstuften in: a) *Information* (reine Informationsfunktion z. B. auf behördlichen Internetseiten), b) *Kommunikation* (Funktion der elektronischen Kommunikation etwa durch die Beantwortung von Bürgeranfragen durch *Emails*) und c) *Transaktion* (Abwicklungsfunktion der Dienstleistung, d. h. Angebote der Verwaltung können komplett *online* in Anspruch genommen werden). Diese Entwicklungsstufen sind in den Kommunalverwaltungen bislang in unterschiedlichem Grad erreicht worden. Die beiden weiteren oftmals unterschiedenen Stufen der *Partizipation* (Teilhabefunktion der Bürger z. B. durch ein *Online*-Vorschlagswesen) und *Integration* (über Verwaltungsebenen hinweg, z. B. durch eine automatisierte Umzugsmeldung zwischen mehreren zuständigen Behörden), sind bei Dienstleistungen von Bürgerämtern weniger relevant.

## 3 Digitale Leistungserbringung in Bürgerämtern

Es ist inzwischen weitgehend unstrittig, dass der Umsetzungsstand von *E-Government*-Anwendungen in Deutschland deutlich hinter den weitreichenden Hoffnungen zurücksteht, die mit diesem Modernisierungsthema verbunden sind (Köhler et al. 2014; Fromm et al. 2015). Zwar gibt es mittlerweile diverse IT-Unterstützungen im Rahmen der Verwaltungsprozesse, aber in der Regel bleibt dem Bürger der Weg zur Verwaltung nicht erspart. *E-Government* als medienbruchfreies, vollständig digitalisiertes Transaktions- und Interaktionsangebot zur Abwicklung von Verwaltungsverfahren existiert weitgehend noch nicht. Auch der *eGovernment*-Monitor (Krcmar et al. 2017) zeigt ähnlich kritische Entwicklungen auf. So kommt beispielsweise die Nutzung von entsprechenden Angeboten nicht voran (minus 4 % Nutzung gegenüber dem Vorjahr), bei entsprechend starker Abnahme der Zufriedenheit der Bürgerinnen und Bürger (minus 8 %) und einer Zufriedenheit mit digitalen Verwaltungsangeboten von insgesamt lediglich 54 %. Portale für Verwaltungsleistungen sind am stärksten auf kommunaler Ebene verbreitet. Eine Untersuchung in Rheinland-Pfalz zeigt, dass die Bürger kommunale Portale zu 43 % im Vergleich zu Landesportalen (15 %) und Bundesportalen (8%; vgl. ISIM 2015) nutzen. Dies ist wenig verwunderlich, werden doch 75–90 % der ausführungspflichtigen Bundesgesetze hier implementiert und wesentliche Entscheidungen gefällt, die die Lebensumstände der Bürger prägen. Es deutet sich allerdings an, dass in bestimmten Anwendungsfeldern der Grad der digitalen Bearbeitung mittlerweile zunimmt.

### ***Online-Anwendungen: Terminmanagement, Formulare***

Die Bürgerämter gehören zu den am weitesten fortgeschrittenen Anwendern von digitalen Instrumenten in deutschen Verwaltungen. Nachdem hier in den letzten Jahren zunächst vor allem *Online-Formulare* eingesetzt wurden, experimentieren die Kommunen inzwischen zunehmend mit neuen Digitalisierungselementen. Zu nennen sind hier insbesondere das *Online-Terminmanagement* sowie die *komplett elektronische oder online-gestützte Abwicklung ganzer Verwaltungsvorgänge*, welche durch eine elektronische Aktenführung ergänzt wird.

Das *Online-Terminmanagement*, also die Möglichkeit des Bürgers, sich vorab über das Netz einem Termin seiner Wahl (soweit verfügbar) für bestimmte Verwaltungsdienstleistungen beim Bürgeramt zu reservieren, gibt es mittlerweile vor allen in den Großstädten über 100.000 Einwohner (knapp 90 %). In den Kommunalverwaltungen, deren Bürgeramt mit diesem Instrument arbeitet, wird dieses durchweg als positiv eingeschätzt. Führungskräfte wie Mitarbeiter stellen den Vorteil der besseren Steuerung des Kundenaufkommens, schnellere Bearbeitungszeiten, geringere Wartezeiten, einen planbareren Einsatz der Mitarbeiter und deren bessere fachliche und zeitliche Einteilung und damit insgesamt eine höhere Kunden- und Mitarbeiterzufriedenheit heraus. Probleme gibt es lediglich bei Ausfällen der Anzeigetechnik oder mit unzufriedenen Spontankunden, die feststellen müssen, dass Terminkunden, welche später das Amt betreten, vor ihnen an die Reihe kommen. Allerdings lohnt sich ein Terminmanagementsystem erst ab einer bestimmten Größe der Stadtverwaltung, da die mit der Einführung einhergehenden Kosten zu berücksichtigen sind. Weiterhin kommt der Ausgestaltung der Funktionalität eine große Bedeutung zu. Den größten positiven Effekt weisen solche Systeme auf, welche in der Lage sind, nicht nur Termine für eine bestimmte Außenstelle zu berücksichtigen, sondern alle Außenstellen des Bürgeramtes zu integrieren und so dem Bürger auch Alternativtermine in anderen Außenstellen vorzuschlagen.

Ein anderes Bild ergibt sich bei den *Online-Formularen*. Zwar erfreuen sie sich einer großen Beliebtheit. Allerdings ist dieses Instrument sehr angebotsorientiert und berücksichtigt nicht die Nachfrage und den konkreten Bedarf der Bürger/Nutzer. Das bedeutet, dass die Verwaltungen oft sehr viele Formulare *online* anbieten, diese aber vom Bürger kaum genutzt werden. Als konkretes Beispiel können Zahlen einer Stadtverwaltung angeführt werden, in der über 600 Formulare angeboten werden, aber 85 % keine Zugriffszahlen aufweisen. Oft steht hinter dem hohen Angebot der politische Wunsch, nach außen eine scheinbare digitale Fortschriftlichkeit des Verwaltungsangebots vorzuweisen (*window-dressing*), ohne dass die tatsächliche Funktionalität in den Blick genommen wird. Weiterhin führt dieser „Angebotsüberhang“ zu einem Auffindbarkeitsproblem von Seiten der Leistungsadressaten, da beliebtere Formulare nicht (oder nicht schnell genug) aufgefunden werden können. Die Nutzungsproblematik wiegt umso schwerer, wenn man bedenkt, dass *Online-Formulare* aus einer Prozessperspektive heraus nur dann sinnvoll sind, wenn die Dateneingabe und Weitergabe, d. h. die Integration der Daten in die jeweilige Fachsoftware der Fachverfahren, vollständig medienbruchfrei erfolgt. Oft werden lediglich Formulare als PDF zum *Download* angeboten welche dann unterschrieben werden müssen und mittels regulärem Postversand an die Verwaltung zu schicken sind. Da bei der

Prozessgestaltung insofern oftmals nicht auf die Automatisierbarkeit geachtet wird, bleiben Medienbrüche unvermeidbar.

### **Digitalisierungstiefe: Information, Kommunikation, Transaktion**

Greift man auf das oben eingeführte Drei-Stufen-Modell der Digitalisierungstiefe (*Information, Kommunikation, Transaktion*) zurück, so ergibt eine Kommunalumfrage aus dem Jahr 2017 ein eindeutiges Bild. Während die Informationsfunktion, d. h. die Bereitstellung von Informationen über die von den Bürgerämtern angebotene Dienstleistung, fast flächendeckend durch alle Kommunen erfüllt wird, ist die Interaktion und demnach die zumindest in Teilen digitale Abwicklung der verwaltsseitigen Dienstleistung (durch *Emails*, Formulare etc.) eher selten und die vollständige *Online*-Abwicklung der Dienstleistung kaum möglich. Fast jede Kommune bietet mittels *Homepage* oder eigenem Verwaltungsportal Informationen über die Verwaltungsleistungen in den Bürgerämtern an. So sind für die zehn häufigsten von Bürgerämtern erbrachten Leistungen in über 70 % aller Kommunen *online* Informationen verfügbar. Geringfügig niedrigere Werte liegen nur im Bereich der Informationen zu einer An-/Um- und Abmeldung einer Wohnung vor (Anteilswert von 61 %). Spitzenreiter ist dabei die Beglaubigung von Zeugnissen mit fast 90 % Informationsverfügbarkeit. Eine teilweise *Online*-Erledigung der Aufgaben lässt sich im Mittel in etwa einem Viertel aller Kommunen erledigen, wobei hier ein Höchstwert für die An-/Um- und Abmeldung einer Erstwohnung und der Tiefstwert für die Zeugnisbeglaubigung zu verzeichnen ist. Die finale Abschließbarkeit der Verwaltungsleistung ist allgemein nur sehr schwach ausgeprägt. Keine einzige Dienstleistung wird in mehr als 14 % aller Kommunen vollständig *online* abgewickelt. Am besten schneiden noch die Dienstleistungen Beantragung eines Führungszeugnisses (13 %; allerdings genügt hier von Seiten der Kommunen ein *Link* zum Bundesamt für Justiz, zudem wird der neue Personalausweis benötigt), einer Urkunde (9 %) und eines Anwohnerparkausweises (9 %) ab. In besonders fortgeschrittenen Untersuchungsstädten waren die Möglichkeiten der Information und Interaktion stärker ausgeprägt. Hinsichtlich der dritten Transaktionsfunktion, also einer medienbruchfreien, vollständigen Abschließbarkeit der Dienstleistung, ergibt sich aber auch in den fortgeschrittenen Untersuchungsstädten ein ähnliches schwaches Nutzungsbild wie in der Masse der Bürgerämter. Insgesamt decken sich unsere empirischen Befunde mit jenen anderer Erhebungen, wie z. B. dem *eGovernment Monitor* der Initiative D21 oder dem *E-Government Development Index* der Vereinten Nationen (Tab. 1).

---

## **4 Umsetzungsstand und Auswirkungen**

Betrachtet man die Nutzung und Wirkung der digitalen Angebote, so wird eine Reihe von Problempunkten erkennbar. Teilweise erhebliche Nutzungsprobleme erwachsen im Bereich der digitalen *Informationsbereitstellung* daraus, dass die Auffindbarkeit und Zugänglichkeit von Informationen unzureichend sind. So erschweren eine mangelhafte Suchfunktionalität und die inhaltliche Überfrachtung

**Tab. 1** Digitalisierungstiefe in deutschen Bürgerämtern

Dienstleistung	Online sind Informationen verfügbar	kann teilweise online erledigt werden (Formulare, E-Mails)	lässt sich online final abschließen	N
Passangelegenheiten	74,80 %	25,20 %	4,80 %	210
Urkunden (Geburtsurkunden/ Eheurkunden)	71,40 %	25,20 %	9,20 %	119
Führungszeugnis	70,70 %	27,10 %	13,30 %	188
An-/Ab-/ Ummeldungen	60,50 %	36,00 %	7,10 %	197
Zeugnisse beglaubigen	89,30 %	10,10 %	2,70 %	149
Hundesteueranmeldung	71,30 %	32,80 %	5,70 %	122
Anwohnerparkausweis	75,70 %	18,40 %	8,70 %	103
Parkausweis für Schwerbehinderte	80,20 %	20,80 %	0,90 %	106
Wohngeld	75,60 %	21,80 %	3,80 %	78
Kfz an-/ab-/ummelden (nur Kreisstädte)	75,00 %	23,50 %	7,40 %	68

Quelle: Bogumil et al. 2019 (Angaben als Prozent der Fälle)

von *Websites* deren Nutzung durch den Bürger zur Informationsgewinnung. Hinzu kommt, dass der Bürger aufgrund der Unübersichtlichkeit des Angebots und schlechten Auffindbarkeit von spezifischen Informationen oftmals auf gut funktionsfähige Angebote der Kommune nicht zugreift, da diese im allgemeinen „Angebotsdschungel“ untergehen. Die gebotene Entschlackung des Angebots, ggf. durch Extrapolate mit gut funktionierenden medienbruchfreien Angeboten, steht hier noch aus.

Betrachtet man die *Kommunikationsfunktion*, wird deutlich, dass die Digitalisierung von Verwaltungsleistungen auch zu nicht-intendierten dysfunktionalen Effekten in Bezug auf die Arbeitsbelastung der Beschäftigten im Bürgeramt führen kann. Diese sehen momentan die Digitalisierung (noch) nicht als Arbeitsentlastung – im Gegenteil. Die teilweise permanente Erreichbarkeit (v. a. durch *Emails*) und die dadurch erhöhte Arbeitstaktung führen eher zu einer steigenden Arbeitsbelastung, die in einigen Kommunen bereits zu spezifischen Regelungen zur (Begrenzung der) elektronischen Erreichbarkeit, etwa über Dienstvereinbarungen, geführt haben. Außerdem kommt es vielfach zu einer Verlagerung des Arbeitsaufkommens vom *Front*-ins *Backoffice*, ohne dass sich für die Mitarbeiter erkennbare Vorteile ergeben. Der eher wenig spürbare Entlastungseffekt aus Sicht der Mitarbeiter ist aber auch dadurch zu erklären, dass der persönliche Kontakt für die Bürger nach wie vor den bevorzugten Verwaltungszugang darstellt, da so Sachverhalte schneller und weniger fehleranfällig bearbeitet werden könnten. Allerdings hängt dies wiederum damit zusammen, dass die meisten *Online*-Angebote bislang nicht attraktiv und nutzerfreundlich genug sind, um auf den persönlichen Verwaltungskontakt verzichten zu können. Aus Sicht der Führungskräfte stellen sich die Wirkungen der digitalen Außenkommunikation in den Bürgerämtern hingegen positiver dar und es werden

u. a. schnellere Bearbeitungszeiten, geringere Wartezeiten, geringere Fehlerhäufigkeiten (beispielsweise bei Formularübertragungen) berichtet. Die Sachbearbeiter-Ebene bekommt diese Vorteile jedoch oftmals nicht zu spüren, da lediglich der absolute, nicht aber der individuelle Arbeitsaufwand pro Mitarbeiter sinkt, wenn u. a. Formulare bereits vorausgefüllt sind oder nur kritische, nicht automatisierbare Sonderfälle an die Mitarbeiter herangetragen werden.

Die Ausprägung der *Transaktionsfunktion* und damit die vollständig medienbruchfreie Abwicklung von Verwaltungsdienstleistungen ist kaum realisiert bzw. nur sehr selten möglich. Die Gründe hierfür sind vielfältig und reichen von technischen, rechtlichen, finanziellen, personellen bis hin zu politischen Hürden und Problemen (vgl. Scholl und Klischewski 2007; Thapa und Schwab 2017). Ein Grundproblem liegt in der oftmals rechtlichen Notwendigkeit des persönlichen Kontakts. Dies bedeutet, dass an irgendeinem Punkt in der Bearbeitung des Verwaltungsvorgangs eine Form der Authentifizierung erforderlich ist. Da die Funktionen des elektronischen Personalausweises aufgrund erheblicher Nutzungshürden eine äußerst geringe Akzeptanz und Anwendungshäufigkeit genießen, ist eine persönliche Anwesenheit unvermeidlich und bleiben Medienbrüche zwingend. Es steht außer Frage, dass dieser ohne substanzelle Verbesserungen in der Nutzerfreundlichkeit (*usability*) auch weiterhin nicht genutzt wird, da er immer noch teilweise Kosten durch zu erwerbende Lesegeräte erzeugt (AusweisApp2 ist nicht für alle Handys verfügbar), ein relativ hohes technisches Verständnis des Nutzers voraussetzt (Treiber- und Softwaredownloads), und zudem – und das ist vielleicht am wichtigsten – kaum Nutzungsmöglichkeiten bereitstellt. Hinzu kommt, dass bei bestimmten Verwaltungstätigkeiten ein medienbruchfreies Handeln prinzipiell nicht möglich ist. So muss z. B. ein Reisepass bei der Beantragung persönlich unterschrieben werden. Hinzu kommen im Bereich der rechtlichen Hindernisse Datenschutzbestimmungen, Auskunftssperren und Aufbewahrungspflichten. Weitere Barrieren einer medienbruchfreien Nutzung liegen in der mangelnden Verbreitung elektronischer Bezahlmöglichkeiten in den Kommunen, da die meisten Verwaltungsvorgänge mit einer Gebühr verbunden sind und ohne sofortige Bezahlung nicht medienbruchfrei abgeschlossen werden können.

### **Politische und institutionelle Hürden**

Neben den genannten rechtlichen und finanziellen Problemlagen gibt es Hinweise aus den Kommunen, dass von politischer Seite – sei es von Seiten des Bundes oder der Länder – kaum ein Handlungsdruck aufgebaut wird und es ganz allgemein an einer strategischen Ausrichtung oder an Zielvorgaben fehlt. Falls es doch sporadisch zu *E-Government*-Initiativen kommt, werden diese eher inkrementell umgesetzt. Zudem agiert die Gesetzgebungsebene (Bund und Länder) oft „realitätsfern“ und die Sichtweise der kommunalen Praxis findet sich in den entsprechenden Gesetzgebungsverfahren, die Auswirkungen auf Verwaltungstätigkeiten haben, oft nicht wieder. Aber auch auf kommunaler Ebene mangelt es oft an einer Befürworter-Koalition, um die Digitalisierung voranzutreiben. So bestimmen teilweise politische oder persönliche Abhängigkeiten darüber, ob z. B. Digitalisierungsbudgets bereitgestellt werden oder nicht – je nach Sichtweise des verantwortlichen Bürgermeisters

oder Dezernenten. In organisatorischer und personeller Hinsicht besteht das Problem, dass neben einer nicht immer ausreichenden Ressourcenbereitstellung für die Digitalisierung auch Personalengpässe bestehen. Zwar sind die Kommunalbedienten gegenüber der Digitalisierung aufgeschlossen. Jedoch haben sich die potenziellen Vorteile, wie Arbeitsvereinfachungen, E-Arbeit (*Homeoffice*) oder E-Fort- und Weiterbildung, derzeit noch nicht eingestellt, sodass eine eher kritische Einstellung gegenüber Digitalisierungselementen überwiegt. Darüber hinaus fehlt es vielfach an fachlich geeignetem Personal und *Know-how* für anspruchsvollere Digitalisierungsprojekte und für das Bewerben von bereits implementierten *E-Services*, beispielsweise durch Marketingkonzepte. Hinzu kommt speziell für den Bereich der Bürgerämter eine teils recht hohe Personalfluktuation, auch angetrieben durch interkommunalen Wettbewerb, sowie generell das Problem des Fachkräftemangels, der sich in Qualität und Quantität von Bewerbungen niederschlägt.

---

## 5 Perspektiven für Staat und Verwaltung

Der Umsetzungsstand hinsichtlich der Digitalisierung von Verwaltungsleistungen in Kommunalverwaltungen liegt nach wie vor deutlich hinter den weitreichenden Hoffnungen und ständigen politischen Ankündigungen zurück. Während es in den letzten Jahren insbesondere gelungen ist, das Einstellen von Onlineformularen auf den Internetplattformen als erster Stufe der Digitalisierung zu verbessern, bestehen nach wie vor erhebliche Lücken und Defizite im Bereich der digitalen Kommunikation zwischen Verwaltung und Bürgern und vor allem in der medienbruchfreien Transaktion. Die Gründe hierfür sind vielfältig. Ein zentraler Bereich sind die zahlreichen Schriftformerfordernisse, Dokumentationspflichten und die mangelnde Nutzbarkeit und Anwenderfreundlichkeit bestehender elektronischer Angebote, wie etwa die Identifikationsmöglichkeiten über den elektronischen Ausweis. Um diesen Problemen Abhilfe zu verschaffen, kommen für die Zukunft u. a. die folgenden Handlungsfelder in den Blick.

Zum einen sind auf Bundes- und Länderebene die rechtlichen, prozeduralen und finanziellen Bedingungen zu schaffen, damit die Verwaltungsdigitalisierung auf der lokalen Ebene und im direkten Bürgerkontakt besser funktionieren kann. Hierzu bedarf es neben gesetzgeberischer Aktivität, etwa im Bereich der Reduzierung von Schriftformerfordernissen, Dokumentations- und Anwesenheitspflichten, einer verbesserten ebenenübergreifenden Zusammenarbeit und Koordination der unterschiedlichen Politik- und Verwaltungsebenen zur Steuerung der verwaltungsbezogenen Digitalpolitik. Die Vorteile der Digitalisierung für Bürger und Verwaltung werden nur dann spürbar zur Geltung kommen, wenn es einheitliche Standards gibt, auf die sich Bund, Länder und Kommunen einigen müssen und die auch in anderen europäischen Ländern üblich sind. Andernfalls besteht die Gefahr der Fragmentierung, Unübersichtlichkeit und Inkompatibilität von zahlreichen Einzellösungen, die dann eher einem Flickenteppich als einem nutzerfreundlichen digitalen Serviceangebot aus einem Guss entsprechen (vgl. NKR 2017a, S. 35). Dies gilt nicht nur für die Konzeption und Entwicklung der verschiedenen Online-Angebote, die der-

zeit in den ebenenübergreifenden Entwicklungsgemeinschaften im Rahmen der OZG-Umsetzung erfolgt. Vielmehr ist eine solche Standardisierung und Homogenisierung von Lösungen vor allem bei der Umsetzung und beim flächendeckenden Roll Out der neuen digitalen Angebote wichtig, aber angesichts der föderalen Vielfalt und Dezentralität öffentlicher Verwaltung in Deutschland auch eine besondere Herausforderung.

Zwar gibt es bereits erste vertikal integrierte Lösungen auf Länderebene, wie beispielsweise die Service-Portale der Länder Berlin (<https://service.berlin.de/>) oder Baden-Württemberg (<https://www.service-bw.de/>). Weiterhin haben Bund und Länder versucht, über eine Reihe von Gesetzen, wie den E-Government-Gesetzen, dem Ziel stärker integrierter und gebündelter elektronischer Verwaltungsleistungen näherzukommen. Durchschlagende Erfolge sind allerdings bisher nicht feststellbar. So wurde auf Bundesebene entgegen den Zielvorstellungen des letzten Koalitionsvertrages keine einzige Verwaltungsleistung bundesweit koordiniert, flächendeckend digitalisiert und einheitlich angeboten, wenn man von den ersten Fortschritten bei der elektronischen KFZ-Zulassung einmal absieht. Von einer medienbruchfreien Digitalisierung der Top-100-Verwaltungsleistungen für Bürger und Unternehmen ist man in Deutschland nach wie vor weit entfernt.

Das im August 2017 verabschiedete OZG (Onlinezugangsgesetz) ist sicherlich ein Schritt in die richtige Richtung, da es den Implementationsdruck auf Bund und Länder erhöht, indem es beide Ebenen dazu verpflichtet, alle Verwaltungsleistungen bis zum 31.12.2022 elektronisch im Portalverbund des Bundes anzubieten. Durch die gesetzliche Verankerung wurde eine rechtliche Grundlage geschaffen, die für mehr Verbindlichkeit in der ebenenübergreifenden Digitalisierung der Verwaltung sorgen soll, indem sie die Länder verpflichtet, die technischen und organisatorischen Voraussetzungen für diesen Portalverbund zu schaffen. Erhebliche Unklarheiten bestehen allerdings nach wie vor in Bezug auf die praktische Umsetzung des Portalverbunds und den damit einhergehenden Konsequenzen für die kommunale Verwaltungsdigitalisierung. Der aktuelle OZG-Umsetzungskatalog identifiziert ca. 575 Leistungen, die durch die öffentliche Verwaltung bis Ende 2022 online angeboten werden müssen. Weiterhin wurden 14 Themenbereiche definiert, für welche in Federführung einzelner Länder elektronische Umsetzungslösungen entwickelt werden sollen. Der Vollzug der im OZG-Umsetzungskatalog gelisteten Leistungen (vgl. Stocksmeier und Hunnius 2018, S. 9) liegt ganz überwiegend (ca. 76 %) bei Ländern und Kommunen, wobei eine Vielzahl kommunaler Angebote (z. B. Geburtsurkunde/-bescheinigung, Kfz-Zulassung/-um-/abmeldung, Meldebestätigung, Registerauskunft, Personalausweis, Wohnsitzmeldungen, Aufenthaltsauskunft/-karte, Bauvorbescheid/-genehmigung, Elterngeld, Führerschein etc.) zu den prioritären OZG-Leistungen gehört. Deshalb erscheint eine Einbindung der kommunalen Praxis in Konzeption und Implementation dieser Online-Verwaltungsleistungen zwingend, um sicherzustellen, dass Praxistauglichkeit und Nutzerfreundlichkeit gewährleistet werden. Die Kommunen selbst sehen in einigen OZG-Leistungsfeldern, wie Führerscheinwesen, Ausländer- bzw. Staatsangehörigkeitswesen und Einbürgerung die größten Potenziale für künftige Digitalisierungsvorhaben. Hier bietet es sich besonders an, über eine stärkere Vernetzung, Modula-

risierung und Registerbildung die Integration von *E-Government* voranzubringen, da es sich bei diesen Leistungen vorwiegend um Pflichtaufgaben des übertragenen Wirkungskreises handelt. Dabei muss dies nicht zwangsläufig über Gesetzesänderungen geschehen, sondern kann auch in einer gemeinsamen Nutzung der Infrastruktur, der Definition von Standards oder der Entwicklung von (übertragbaren) Prozessmodulen erfolgen (vgl. Köhl et al. 2014, S 188). Ob und in welchem Ausmaß dabei die Harmonisierung und Bündelung der 575 OZG-Leistungen und die Einhaltung von Mindeststandards tatsächlich angestrebt wird und realisierbar ist, muss bislang offenbleiben.

Als weiteres Zukunftsthema der Verwaltungsdigitalisierung (kommunaler) Leistungen ist die Registermodernisierung zu nennen, die laut Nationalem Normenkontrollrat stärker in den Mittelpunkt der Digitalisierungspolitik auf Bundes- und Länderebene rücken sollte (vgl. NKR 2017b). Viele (kommunale) Verwaltungsleistungen basieren auf öffentlichen Registern, wie z. B. den Melde- oder den Gewerberegistern. Diese sind aber bislang kaum auf digitale Prozesse ausgelegt und zudem, den fachlichen und territorialen Zuständigkeiten folgend, oft genauso dezentral und heterogen organisiert wie andere öffentliche IT-Komponenten. Die Bürger sind gezwungen, sich z. B. eine Geburtsurkunde als papiergebundenen Auszug aus dem Geburtenregister zu besorgen, um sie danach bei einer anderen Stelle für die Beantragung von Kinder- und Elterngeld wieder einzureichen. Würden diese Daten mit Zustimmung der Bürger und unter Wahrung datenschutzrechtlicher Standards zwischen den betroffenen Verwaltungsstellen ausgetauscht (wie dies beispielsweise in Österreich möglich ist), könnten die betreffenden Verwaltungsleistungen digital angeboten und Verwaltungsprozesse erheblich vereinfacht werden. Die zielkonforme Umsetzung des OZG scheint erst auf dieser Grundlage möglich. Auch das geforderte *Once-Only*-Prinzip, wonach die Bürger der öffentlichen Verwaltung lediglich einmalig bestimmte Standardinformationen zukommen lassen müssen, auf die dann – unter Einhaltung spezifischer Zugangsbedingungen und mittels Verschlüsselungsmechanismen – in weiteren Fachverfahren zurückgegriffen werden kann, ist nur so realisierbar. Inzwischen liegen auch Lösungsansätze vor, mit denen die bestehenden datenschutz- und verfassungsrechtlichen Bedenken überwunden werden können, die es aufgrund des Volkszählungsurteils von 1983 und des Rechts auf informationelle Selbstbestimmung bis heute gegen die Einführung von einheitlichen Identifikationsnummern gibt. So könnte sich zur Umsetzung des *Once-Only*-Prinzips eine Art Stammzahlenregistersystem mit bereichsspezifischen Personenkennzeichen (nach österreichischem Vorbild) anbieten, das den Datenaustausch zwischen Bürger und Behörde sowie zwischen den Behörden erleichtert, qualitativ verbessert und welches datenschutzrechtliche Standards sogar besser erfüllt als analoge Prozesse. Auch die bislang sehr aufwändige Durchführung des Zensus, der in Deutschland mehr als 700 Mio. EUR kostet, ließe sich deutlich vereinfachen, wenn dieser auf der Basis moderner Register genauso automatisiert durchgeführt würde wie in Österreich, der Schweiz oder Dänemark.

Insgesamt sollte das Modernisierungstempo im Bereich der elektronischen Verwaltungmodernisierung im Sinne konkreter Umsetzungsschritte erhöht werden. Um zu erreichen, dass der angestrebte Portalverbund nicht ein bloßer „Verlinkungs-

verbund“ wird, ist eine Verwaltungskultur erforderlich, die Innovationen fördert, dabei fach- und ebenenübergreifend orientiert ist, die kommunale Ebene stärker einbezieht und die Nutzersicht in den Vordergrund stellt. Darüber hinaus muss den Verwaltungsbeschäftigten und ihren Arbeitsbedingungen bei zukünftigen Digitalisierungsprojekten mehr Aufmerksamkeit zugewandt werden, da die Digitalisierung aus ihrer Sicht bislang nur sehr begrenzt (etwa durch das Online-Terminmanagement) zu Verbesserungen und Entlastungen geführt hat. Dabei erscheint nicht nur die verstärkte Einbindung der Beschäftigten und ihrer Vertretungen in die organisationsinternen Veränderungsprozesse geboten, sondern es müssen auch die Verwaltungsprozesse und -strukturen so umgestaltet werden, dass digitale Innovationen für die Beschäftigten mit spürbaren Arbeitsentlastungen und Vereinfachungen sowie für die Bürger mit deutlichen Serviceverbesserungen und Zeiteinsparungen einhergehen.

---

## Literatur

- Bogumil, Jörg, Sascha Gerber, Sabine Kuhlmann, und Christian Schwab. 2019. *Bürgerämter in Deutschland*. Baden-Baden: Nomos.
- Coursey, David, und Donald F. Norris. 2008. Models of E-Government: Are they correct? An empirical assessment. *Public Administration Review* 68(3): 523–536.
- Fromm, Jens, Christian Welzel, Lutz Nentwig, und Mike Weber. 2015. *E-Government in Deutschland. Vom Abstieg zum Aufstieg, Gutachten für den Nationalen Normenkontrollrat*. Berlin: Kompetenzzentrum Öffentliche IT/Fraunhofer FOKUS.
- Heuermann, Roland, Matthias Thomendahl, und Christian Bressem, Hrsg. 2018. *Digitalisierung in Bund, Ländern und Gemeinden. IT-Organisation, Management und Empfehlungen*. Berlin: Springer.
- Homburg, Vincent. 2018. ICT, E-Government and E-Governance. Bits & bytes for public administration. In *The palgrave handbook of public administration and management in Europe*, Hrsg. Eduardo Ongaro und Sandra van Thiel, 347–361. London: Palgrave Macmillan.
- ISIM (Ministerium des Innern, für Sport und Infrastruktur Rheinland-Pfalz). 2015. *E-Government – Perspektiven des kommunalen E-Government*. Mainz: Ministerium des Innern, für Sport und Infrastruktur.
- Köhł, Stefanie, Klaus Lenk, Stephan Löbel, Tino Schuppan, und Anna-Katharina Viehstädt. 2014. *Stein-Hardenberg 2.0. Architektur einer vernetzten Verwaltung mit E-Government*. Berlin: Edition Sigma.
- Krcmar, Helmut, Cigdem Akkaya Türkavci, Lena-Sophie Müller, Sabrina Dietrich, Michael Boberach, und Stefanie Exel. 2017. *eGovernment MONITOR 2017. Nutzung und Akzeptanz digitaler Verwaltungsangebote – Deutschland, Österreich und Schweiz im Vergleich*. Berlin: Initiative D21 e.V./München: fortiss.
- Kuhlmann, Sabine, und Hellmut Wollmann. 2014. *Introduction to comparative public administration. Administrative systems and reforms in Europe*. Cheltenham/Northampton: Edward Elgar.
- Nationaler Normenkontrollrat (NKR). 2017a. *Bürokratieabbau, Rechtsetzung, Digitalisierung. Erfolge ausbauen – Rückstand aufholen. Jahresbericht 2017 des NKR*. Berlin: Nationaler Normenkontrollrat.
- Nationaler Normenkontrollrat (NKR). 2017b. *Mehr Leistung für Bürger und Unternehmen. Verwaltung digitalisieren. Register modernisieren*. Berlin: Nationaler Normenkontrollrat.
- Scholl, Hans J., und Ralf Klischewski. 2007. E-Government integration and interoperability. Framing the research agenda. *International Journal of Public Administration* 30(8–9): 889–920.

- Schwab, Christian, Sabine Kuhlmann, Jörg Bogumil, und Sascha Gerber. 2019. *Digitalisierung der Bürgerämter in Deutschland*. Düsseldorf: Hans-Böckler-Stiftung.
- Stocksmeier, Dirk, und Sirko Hunnius. 2018. *OZG-Umsetzungskatalog. Digitale Verwaltungsleistungen im Sinne des Onlinezugangsgesetzes*. Berlin: init AG im Auftrag des Bundesministeriums des Innern, für Bau und Heimat.
- Thapa, Basanta E. P., und Christian Schwab. 2017. Herausforderung E-Government Integration. Hindernisse von E-Government-Reformen im Berliner Mehrebenensystem. In *Verwaltungspraxis und Verwaltungswissenschaft. Schriften der Deutschen Sektion des Internationalen Instituts für Verwaltungswissenschaften*, Hrsg. Jan Ziekow, Bd. 41, 171–206. Baden-Baden: Nomos.
- Wirtz, Bernd W., und Robert Piehler. 2010. E-Government. In *E-Government. Grundlagen, Instrumente, Strategien*, Hrsg. Bernd W. Wirtz, 3–18. Wiesbaden: Springer Gabler.



---

# Watchdog-Organisationen

## Der Staat unter Beobachtung

Karsten Mause

### Inhalt

1 Klärung des Begriffs .....	450
2 Theoretische Grundlagen .....	451
3 Praxisbeispiele .....	453
4 Chancen, Grenzen und Gefahren .....	455
5 Perspektiven für Staat und Watchdogs .....	457
Literatur .....	458

---

### Zusammenfassung

In Deutschland und anderen Ländern existieren Nichtregierungsorganisationen (NGOs) wie *Abgeordnetenwatch*, *LobbyControl* oder *Transparency International*, die Missstände in Politik und Verwaltung aufdecken und Machtmissbrauch verhindern wollen. Durch die Digitalisierung haben sich für derartige Watchdog-Organisationen die Möglichkeiten, Informationen zu sammeln, zu verarbeiten, aufzubereiten und zu verbreiten, erheblich verbessert. Zudem sind neue Typen solcher „Wachhunde der Demokratie“ entstanden, die Internet und Social Media nicht bloß zur Informationsverbreitung nutzen, sondern die interaktive Online-Tools entwickelt haben, um politisch-administrative Akteure zu befragen oder politische Kampagnen zu verschiedenen Themen zu organisieren. Aufbauend auf einer genaueren Begriffsklärung gibt der Beitrag einen Überblick über die Chancen und Gefahren, die sich im digitalen Zeitalter aus den Aktivitäten von Watchdog-NGOs für das Bürger-Staat-Verhältnis ergeben.

---

K. Mause (✉)

Institut für Politikwissenschaft, Universität Münster, Münster, Deutschland  
E-Mail: [karsten.mause@uni-muenster.de](mailto:karsten.mause@uni-muenster.de)

## Schlüsselwörter

Nichtregierungsorganisationen · NGOs · Zivilgesellschaft · Transparenz · Machtkontrolle · Accountability · Digitalisierung

---

### 1 Klärung des Begriffs

Organisationen wie *Abgeordnetenwatch*, *Foodwatch* oder *Finance Watch* haben es sich zur Aufgabe gemacht, das Handeln von Akteuren in Politik, Verwaltung, Wirtschaft und anderen Gesellschaftsbereichen zu beobachten bzw. zu überwachen, um Fehlverhalten (z. B. politische Korruption oder andere Formen des Machtmisbrauchs) aufzudecken. Sie stellen somit eine Form der Machtkontrolle dar und übernehmen aus eigener Initiative eine „Wachhund“- bzw. Kontrollfunktion, da sie die institutionalisierten Kontrollinstanzen (wie Oppositionsparteien, Medien, Rechnungshöfe oder Gerichte) nicht für ausreichend erachten (Speth 2018a). Bestimmte Watchdog-Organisationen sind gezielt mit dem Zweck gegründet worden, das Verhalten von Akteuren in Politik und Verwaltung zu beobachten, um auf diese Weise einen Beitrag zur Kontrolle staatlicher bzw. politischer Macht zu leisten (z. B. *Abgeordnetenwatch*, *LobbyControl*, *Transparency International*).

In der gesellschaftswissenschaftlichen Literatur bezieht sich der Begriff der Watchdog-Organisationen in der Regel auf Nichtregierungsorganisationen (NGOs) bzw. zivilgesellschaftliche Organisationen, die unabhängig sind von den politisch-administrativen oder anderen Akteuren, die sie beobachten und kontrollieren (Speth 2018b). Hingegen fallen Rechnungshöfe, Kommunalaufsichtsbehörden, Gerichte, Oppositionsparteien und andere Akteure, die innerhalb des politisch-administrativen Systems Kontrollfunktionen wahrnehmen, üblicherweise nicht unter diesen Begriff (Greef und Kiepe 2018). Gleichermaßen gilt für Medienbetriebe, insbesondere die investigativen Journalisten in Presse, Rundfunk und Fernsehen, die nach ihrem Selbstverständnis ebenfalls eine „Wächterrolle“ übernehmen (Drücke 2018), sowie die allgemeine Öffentlichkeit. Umwelt-, Verbraucher-, Arbeitgeberverbände, Gewerkschaften sowie ähnliche „klassische“ Interessengruppen mögen sich mitunter auch als „Wachhunde der Demokratie“ betrachten, da sie Politik und Verwaltung in „ihren“ Politikfeldern (Umweltpolitik, Verbraucherpolitik, Arbeitsmarktpolitik usw.) kritisch beobachten und sich an der öffentlichen Diskussion beteiligen. Primär geht es ihnen jedoch nicht um den Aufbau einer Infrastruktur zur Beobachtung politisch-administrativer Akteure, sondern darum, dass ihre Verbandsinteressen bzw. die Interessen ihrer Mitglieder so weit wie möglich beim „Policy-Making“ in den jeweiligen Politikfeldern berücksichtigt werden.

Auch im vordigitalen Zeitalter gab es Watchdog-Organisationen wie den *Bund der Steuerzahler* (gegründet 1949) oder *Transparency International Deutschland* (1993). Im Zuge der digitalen Revolution haben sich die technischen Möglichkeiten, Machtkontrolle auszuüben und Gegenmacht aufzubauen, für derartige Organisationen allerdings erheblich verbessert. Beispielsweise können sie ihre Informationen via Internet und Social Media (d. h. Facebook, Twitter & Co.) einfacher und kosten-

günstiger verbreiten als zuvor. Zudem liegen viele relevante Informationen (u. a. offizielle Dokumente aus dem Politik-/Verwaltungsapparat) inzwischen nicht nur in Papierform, sondern auch oder ausschließlich in digitaler Form vor, was die Informationsverarbeitung erleichtert. Von daher ist es wenig überraschend, dass sich im digitalen Zeitalter weitere Watchdogs wie z. B. *Abgeordnetenwatch* (Gründungsjahr 2004) oder *LobbyControl* (2005) gegründet haben. Zudem ist mit Organisationen wie *Campact* (2004) und *FragDenStaat* (2011) ein neuer Typus entstanden, der die neueren Entwicklungen in der Informations- und Kommunikationstechnik nicht nur zur Sammlung, Verarbeitung und Verbreitung von Informationen (via Webseiten, E-Mail-Verteiler, Social-Media-Accounts etc.) verwendet, sondern insbesondere zur Mobilisierung der Bürger für politische Kampagnen nutzt. Wie in Abschn. 3 näher erläutert, unterscheiden sich die hier interessierenden „Wachhunde“ heutzutage u. a. dahingehend, wie sie die Plattform „Internet“ für ihre Zwecke nutzen.

---

## 2 Theoretische Grundlagen

Konzeptionell erfasst werden Watchdog-Organisationen vor allem in der Principal-Agent-Theorie der Politik und Verwaltung, die insbesondere in der Wirtschafts-, Verwaltungs- und Politikwissenschaft entwickelt wurde (siehe als Überblick Besley 2006). In dieser (demokratie-)theoretischen Perspektive erbringen politisch-administrative „Agenten“ (d. h. Politiker und Staatsdiener in der Verwaltung) bestimmte Dienstleistungen für ihre „Prinzipale“, die Bürger. Letztere sind sozusagen die „Chefs“ bzw. Auftraggeber der politisch-administrativen Akteure. Ein Grundproblem dieser Beziehung ist, dass Agenten meist besser über die Quantität und Qualität der von ihnen erbrachten Dienstleistungen und Güter informiert sind als die Prinzipale. In der Regel besteht ein Informationsnachteil bzw. eine Informationsasymmetrie zu Ungunsten der Bürger in ihrer Rolle als Auftraggeber.

Zwar kann es sein, dass politisch-administrative Agenten von sich aus freiwillig Informationen bereitstellen, um diese Informationsasymmetrie auszugleichen. Beispielsweise könnten Abgeordnete Informationen (i) über ihre An-/Abwesenheit bei Plenardebatten, namentlichen Abstimmungen und Ausschuss-Sitzungen, (ii) über die Anzahl ihrer außerparlamentarischen Nebentätigkeiten, (iii) über die Höhe ihrer Nebeneinkünfte oder (iv) über Kontakte zu Lobbyisten bzw. Interessengruppen veröffentlichen. In der Vergangenheit hat sich jedoch gezeigt, dass Politiker und Parlamente häufig von sich aus kein oder nur ein geringes Interesse haben, entsprechendes Informationsmaterial bereitzustellen und dafür Gründe wie den Schutz der Privatsphäre, die Freiheit des Abgeordnetenmandats oder den zur Erstellung derartiger Informationen anfallenden Verwaltungsaufwand vorbringen (Geys und Mause 2012, 2019). Obwohl z. B. die in den vergangenen Jahrzehnten schrittweise verschärften Veröffentlichungsregeln des Deutschen Bundestages bezüglich Parteispenden und Abgeordneten-Nebentätigkeiten/Nebeneinkünften mehr Transparenz geschaffen haben, werden bestimmte Informationen (u. a. die genaue Höhe der Nebeneinkünfte) weiterhin nicht veröffentlicht.

An dieser Stelle kommen Watchdog-Organisationen ins Spiel, die vor allem deshalb gegründet wurden und werden, um die Informationslücke zwischen den Bürgern und ihren politisch-administrativen Agenten so weit wie möglich zu schließen. Internet-Plattformen wie *Abgeordnetenwatch* sammeln Informationen über Politiker, bereiten diese möglichst leserfreundlich auf und stellen dieses Informationsmaterial (Studien, Datenbanken etc.) der Öffentlichkeit (nicht zuletzt Journalisten) zur Verfügung. Beim Verdacht auf Korruption, illegale Parteispenden und ähnlichen Delikten können sie ihre Informationen auch an Polizei und Justiz weitergeben, damit diese Verdachtsfällen nachgehen und ggf. Sanktionen verhängen können (Greef und Kiepe 2018). Aus Sicht der Prinzipal-Agent-Theorie stellen Watchdog-Organisationen intermediäre Organisationen bzw. Informationsintermediäre dar, die als dritte Partei (daher auch der in diesem Kontext bisweilen gebrauchte Begriff „Third-party-Monitoring“) einen Beitrag dazu leisten möchten, dass bürgerseitige Informationsnachteile gegenüber Politik und Verwaltung weitestgehend beseitigt werden. Durch den technischen Fortschritt (Computer, Internet, E-Mail, Social Media etc.) haben sich für solche Intermediäre (a) die Möglichkeiten erweitert und (b) die Kosten reduziert, Informationen zu sammeln, zu verarbeiten und zu verbreiten. Dieser Tatbestand ist einer der Gründe für das in den letzten Jahren vermehrt zu beobachtende Aufkommen von Organisationen wie *Abgeordnetenwatch* oder *LobbyControl*.

An solche „Wachhunde der Demokratie“ knüpfen sich also Hoffnungen, Macht besser kontrollieren zu können, wobei ihnen insofern eine ambivalente Rolle zukommt, als dass sie selbst wiederum über Machtpotenziale verfügen (u. a. Möglichkeit der Nutzung des Internets für politische Kampagnen, Rufschädigung, Skandalisierung), die unter Umständen von Watchdog-NGOs missbraucht werden könnten (mehr dazu in den Abschn. 4 und 5). Im Übrigen ist keineswegs selbstverständlich, dass derartige NGOs überhaupt entstehen und sich dauerhaft etablieren können. Zwar dürfte es in Demokratien eher selten zu beobachten sein, dass „der“ Staat bzw. die herrschenden „Machthaber“ die Gründung solcher Organisationen verbieten oder ihre Arbeit behindern; aber diejenigen, die eine solche Initiative ergreifen, stehen aus ökonomischer Sicht vor einem Kollektivgut- bzw. Trittbrettfahrer-Problem (vgl. dazu grundlegend Olson 1965).

So mögen in einer Gesellschaft einige oder gar viele Bürger durchaus ein Interesse daran haben, möglichst viel über die (Un-)Tätigkeit bzw. „Machenschaften“ von Politik und Verwaltung zu erfahren (Stichworte: Lobbyismus, Korruption). Geht man jedoch theoretisch von der Verhaltensannahme des *homo oeconomicus* (also eigennutzorientierten Individuen) aus, so ist zu erwarten, dass der einzelne Bürger selbst keine Zeit, Mühe und Geld in den Aufbau von Watchdog-Organisationen investieren wird – in der Hoffnung, dass seine Mitbürger entsprechende Investitionen tätigen. Dann käme man/frau nämlich in den Genuss der Informationen über Politiker, Parlamente oder Verwaltungen, ohne einen eigenen Beitrag zur Sammlung, Aufbereitung und Verbreitung dieser Informationen geleistet zu haben. Dass in Deutschland und anderswo zivilgesellschaftliche „Wachhunde“ existieren, zeigt jedoch, dass es unter bestimmten Bedingungen möglichst ist, das Kollektivgut- bzw. Trittbrettfahrer-Problem zu überwinden. In der Realität verhalten sich offenbar nicht überall und immer alle so, wie es die *Homo oeconomicus*-Annahme voraussagt.

### 3 Praxisbeispiele

Um einen Einblick in deren Arbeitsweise zu geben, präsentiert Tab. 1 einige Basisinformationen zu den bekanntesten Watchdog-NGOs, die in Deutschland Politik und Verwaltung kritisch beobachten. Dabei machen sie in unterschiedlicher Weise Gebrauch von den im Internet-Zeitalter vorhandenen Möglichkeiten (E-Mail, Social Media, Big Data etc.). *Abgeordnetenwatch* wird von *Parliamentwatch e.V.* getragen. Über eine Dialog-Plattform können Bürger Fragen stellen und Abgeordnete sowie Wahlkandidaten können antworten, wobei der Deutsche Bundestag, die Parlamente der Länder sowie die deutschen Abgeordneten im Europäischen Parlament einbezogen werden. Zusätzlich zu den Fragen und Antworten finden sich auf der Webseite weitere Informationen zu den Parlamentariern, wie biografische Angaben (berufliche Qualifikation etc.), Abstimmungsverhalten bei namentlichen Abstimmungen oder Angaben zu Nebentätigkeiten und der Mitgliedschaft in Parlamentsausschüssen. Diese Informationen können u. a. dazu genutzt werden, um mögliche Interessenkon-

**Tab. 1** Beispiele für deutsche Watchdog-NGOs

Name (Gründungsjahr)	Rechts-form	Instrumente	Themenschwerpunkte
Abgeordnetenwatch (2004) <a href="http://www.abgeordnetenwatch.de">www.abgeordnetenwatch.de</a>	e.V.	- Internet-Befragungstool - Recherchen, Studien - Petitionen, Klagen	- Politikerverhalten (Nebeneinkünfte etc.) - Parteispenden - Lobbyismus
FragDenStaat (2011) <a href="http://www.fragdenstaat.de">www.fragdenstaat.de</a>	e.V.	- Internet-Befragungstool - Recherchen - öff. Kampagnen, Klagen	- Transparenz in Politik & Verwaltung - Lobbyismus
Campact (2004) <a href="http://www.campact.de">www.campact.de</a>	e.V.	- Online-Petitionen - Kampagnen - Demonstrationen, Proteste	- Transparenz in Politik - Politikziele (u. a. soziale Gerechtigkeit, Nachhaltigkeit)
LobbyControl (2005) <a href="http://www.lobbycontrol.de">www.lobbycontrol.de</a>	e.V.	- Recherchen, Studien - öff. Kampagnen	- Lobbyismus - Politikfinanzierung - Politikerverhalten (Nebeneinkünfte etc.)
Transparency International Deutschland (1993) <a href="http://www.transparency.de">www.transparency.de</a>	e.V.	- Recherchen, Studien - öff. Kampagnen	- Bekämpfung + Prävention (polit.) Korruption - Transparenz in Politik & Verwaltung
Bund der Steuerzahler Deutschland (1949) <a href="http://www.steuerzahler.de">www.steuerzahler.de</a>	e.V.	- Recherchen, Studien - öff. Kampagnen, Klagen	- Steuergeldver(sch)wendung - Politikfinanzierung - Transparenz in Politik & Verwaltung

*Quelle:* Eigene Zusammenstellung auf Basis der (Selbst-)Angaben auf den Organisationswebseiten.  
Stand: 02/2020

flikte zwischen dem Abgeordnetenmandat und privatwirtschaftlichen Nebentätigkeiten aufzudecken (Geys und Mause 2012; Buzogány 2016). Zudem stellt *Abgeordnetenwatch* eigene Recherchen zur Aufdeckung von Missständen an und verfasst Studien zu Themen wie Lobbyismus, Parteispenden und Abgeordneten-Nebeneinkünfte. Neben der Bereitstellung von Informationen werden auch Petitionen initiiert und Klagen angestrengt, insbesondere in den genannten Themenbereichen.

Ähnlich arbeitet die Internet-Plattform *FragDenStaat*, die von der *Open Knowledge Foundation Deutschland e.V.* getragen wird. Bürger können über ein Befragungstool Anfragen an staatliche Akteure (z. B. Behörden) zu verschiedenen Bereichen der Politik-/Verwaltungspraxis stellen und dabei auch um die Veröffentlichung bestimmter Dokumente und Informationen bitten. Zusätzlich zu dieser Dialog-Plattform stellt die Organisation eigene Recherchen an und versucht mittels Kampagnen und Klagen, staatliche Dokumente (z. B. Stellungnahmen von Interessenverbänden im Gesetzgebungsprozess, Gutachten des Wissenschaftlichen Dienstes des Deutschen Bundestages) für die Öffentlichkeit zugänglich zu machen. *Campact e.V.* versteht sich als „Bürgerbewegung“, die sich bei als wichtig erachteten anstehenden Politikentscheidungen (z. B. in der Umwelt-, Handels- und Rüstungspolitik) mit sog. „Online-Appellen“ (d. h. Unterschriftensammlungen in der Bevölkerung via Internet) direkt an die verantwortlichen Akteure in Regierungen, Parlamenten und Unternehmen wendet. Das Mobilisierungspotenzial des Internet macht sich der Verein auch in der Form zunutze, dass Bürger via E-Mail und Social Media zur Teilnahme an Demonstrationen und Protestaktionen aufgerufen werden.

Während die gerade genannten Watchdogs die im digitalen Zeitalter zur Verfügung stehenden Instrumente auch dazu verwenden, die Bürger selbst in ihre Aktivitäten einzubeziehen (z. B. mittels Online-Befragungstools, Online-Petitionen), nutzen die weiteren exemplarisch aufgeführten Organisationen das Internet in der Regel lediglich als Informationskanal mit großer Reichweite (E-Mail-Newsletter, Facebook, Twitter etc.). *LobbyControl – Initiative für Transparenz und Demokratie e.V.* nimmt verschiedene Formen des Lobbyismus, verstanden u. a. als (unzulässige) Einflussnahme von Unternehmen und Interessenverbänden auf Legislative und Exekutive, in den Blick. Dazu werden eigene Recherchen angestellt (z. B. zu verdeckten Parteispenden, verschwiegenen Abgeordneten-Nebeneinkünften), wird Informationsmaterial veröffentlicht (wie das Online-Lexikon „Lobbypedia“ oder das Buch „LobbyPlanet Berlin“) und es werden Kampagnen gestartet, etwa um Regulierungen zu erwirken, die für mehr Transparenz bei Parteispenden, Abgeordneten-Nebeneinkünften oder den Kontakten von Politikern und Ministerien zu Lobbyisten (Stichwort: Lobbyregister) sorgen sollen. Zudem werden „lobbykritische Stadtführungen“ durch Berlin angeboten. Ähnlich wie *LobbyControl* arbeitet auch *Transparency International Deutschland e.V.*, wobei die thematischen Schwerpunkte hier bei der Bekämpfung und Vorbeugung von Korruption sowie generell auf „mehr Transparenz“ in Politik und Verwaltung liegen. Und als letztes Praxisbeispiel sei der *Bund der Steuerzahler Deutschland e.V.* erwähnt, der sich speziell als Watchdog in puncto Ver(sch)wendung von Steuergeldern in Politik und Verwaltung versteht.

Bei allen genannten zivilgesellschaftlichen Organisationen handelt es sich um eingetragene Vereine. Alle betonen in ihren Selbstdarstellungen, politisch unabhän-

gig und überparteilich zu arbeiten. Und alle bekommen nach eigenen Angaben keine staatlichen Zuschüsse, sondern finanzieren sich aus privaten Quellen (Spenden, Mitglieds-/Förderbeiträge, Zuwendungen von Stiftungen). Der Staat fördert seine (kritischen) Beobachter allerdings insofern und leistet damit einen Beitrag zur Überwindung der Trittbrettfahrer-Problematik, als dass ein Spenden-Anreiz gesetzt wird: aufgrund des staatlich gewährten Status der Gemeinnützigkeit sind Spenden an fast alle „Wachhund“-Vereine steuerlich absetzbar. Derartige Spenden senken die Steuerlast der Spender und reduzieren somit die Steuereinnahmen des Staates. Eine Ausnahme bildet *Campact e.V.* Dieser NGO wurde 2019 der Status der Gemeinnützigkeit aberkannt, da bezweifelt wird, dass deren politische Kampagnen überwiegend im Sinne der Allgemeinheit seien.

---

## 4 Chancen, Grenzen und Gefahren

Zusätzlich zu den Kontrollmechanismen, die sich Politik und Verwaltung selbst gegeben haben (Rechnungshöfe, parlamentarische Untersuchungsausschüsse etc.), erfüllen Watchdog-Organisationen ihrem Selbstverständnis nach eine wichtige Überwachungs- und Kontrollfunktion. Und durch die technischen Möglichkeiten des digitalen Zeitalters haben derartige zivilgesellschaftliche Machtkontrolleure noch an Bedeutung gewonnen. Beispielsweise erlauben es Internet-Befragungstools wie *Abgeordnetenwatch* oder *FragDenStaat*, eine große Zahl von Bürgeranfragen zu bündeln und mitsamt den Antworten der jeweiligen politisch-administrativen Akteure einer breiten Öffentlichkeit bereitzustellen. Die digitale Revolution verändert die Rahmenbedingungen für Politik und Verwaltung insofern, als nun jeder Bürger bequem und schnell vom heimischen Computer oder unterwegs vom Mobiltelefon aus per E-Mail, Social-Media-Account oder über eine Watchdog-Plattform Fragen an Politiker und Behörden richten kann. Auf der einen Seite mag die Vielzahl an E-Mails und Social-Media-Anfragen aus Sicht staatlicher Akteure bisweilen „nervig“ sein. Auf der anderen Seite ermöglichen es ihnen die neu entstandenen, internetbasierten Kommunikationskanäle mit ihrer großen Reichweite jedoch auch, das Handeln von Politik und Verwaltung einer großen Masse an Bürgern besser zu erklären und zu rechtfertigen (Stichwort: Rechenschaftslegung bzw. *Accountability*).

Der Kontrolle von Politik und Verwaltung durch Watchdog-Organisationen sowie deren Einflussmöglichkeiten sind allerdings auch Grenzen gesetzt. Was die Reichweite der von ihnen veröffentlichten Informationen betrifft, sind sie trotz der ihnen im digitalen Zeitalter zur Verfügung stehenden Internet-Kanäle häufig weiterhin darauf angewiesen, dass die klassischen Medien Fernsehen, Radio und Presse ihre Recherchen aufgreifen, wenn sie breite Teile der Bevölkerung erreichen möchten. Zudem können diese Wachhunde zwar „bellen“, also auf wahrgenommene Missstände aufmerksam machen, aber – um im Bild zu bleiben – vielfach nicht „beißen“ bzw. nicht richtig zubeißen. Sie können zwar die gesammelten Informationen über Politiker, Behörden und andere Akteure der Öffentlichkeit zur Verfügung stellen und die Betroffenen somit unter Rechtfertigungsdruck setzen. Aber sie haben neben dem Instrument des sog. „Naming, Blaming & Shaming“ und der Möglichkeit, Kampagnen oder Petitionen zu initiieren, meist keine

weitergehenden Sanktionsmöglichkeiten; sondern sie sind darauf angewiesen, dass Gerichte oder andere, jeweils rechtlich zuständige Akteure überprüfen, (i) ob es sich bei dem wahrgenommenen und aufgedeckten Missstand wirklich um illegales Verhalten handelt und (ii) ob dieses Verhalten in irgendeiner Form bestraft werden kann bzw. muss (z. B. Entlassung eines Ministers, Disziplinarverfahren gegen Verwaltungsmitarbeiter; vgl. zu diesem Punkt auch Greef und Kiepe 2018). Einige Watchdogs nutzen auch die Möglichkeit, selbst Klagen einzureichen.

Als Ergebnis der juristischen Prüfung kann freilich auch herauskommen, dass die von der Watchdog-Organisation angeprangerte Praktik überhaupt nicht gesetzeswidrig war. Auf der einen Seite besteht demnach die Gefahr, dass derartige Organisationen auch überreagieren bzw. zu schnell „anschlagen“ und zu laut „bellern“ können (vgl. zur Skandalisierungsproblematik z. B. Pörksen und Detel 2012; Wewer 2015; Mause 2018). Auf der anderen Seite können deren Aktivitäten aber auch dazu führen, dass Regeln für Akteure in Politik und Verwaltung verschärft werden, so dass Praktiken, die bislang in einem Gemeinwesen lediglich als „bedenklich“, „problematisch“ oder „illegitim“, aber nicht als rechtswidrig galten, aufgrund der Hinweise zivilgesellschaftlicher „Wachhunde“ von nun an als illegal eingestuft werden. Beispielsweise haben die Aktivitäten von *Abgeordnetenwatch*, *LobbyControl* und *Transparency International* mit dazu geführt, dass in Deutschland in den vergangenen Jahren die Transparenzregeln für Parteidaten und die Nebentätigkeiten von Parlamentariern verschärft sowie Karenzzeit-Regelungen für ausscheidende Mitglieder der Bundesregierung (Stichwort: „Drehtür-Effekt“) eingeführt wurden (Geys und Mause 2012; Schiffers 2018).

Nicht unerwähnt bleiben soll auch, dass die Watchdogs selbst wiederum kritisch beobachtet werden. So weisen manche darauf hin, dass die immer genauere Beobachtung von Politikern, ihre immer stärkere Regulierung sowie die durch das Internet gegebenen Veröffentlichungs-/Skandalisierungsmöglichkeiten einige davon abschrecken könnte, ein öffentliches Amt anzustreben (siehe für eine Diskussion dieses, der folgenden und weiterer Kritikpunkte ausführlich Wewer 2015). Auch wird kritisiert, dass es sich bei manchen der von Watchdogs als unzulässiger „Lobbyismus“ bzw. illegitime Einflussnahme angeprangerten Praktiken aus politikwissenschaftlicher bzw. demokratietheoretischer Sicht um legitime Formen der Interessenvertretung bzw.-vermittlung handele. Eine derartige Skandalisierung fördere nicht die Demokratie, sondern schüre eher alte Vorurteile gegenüber der Politik, und könnte mithin die Politik(er)verdrossenheit weiter erhöhen. Und bei manchen Watchdog-Kampagnen (z. B. gegen Freihandelsabkommen, Gentechnik, Privatisierungen) stellt sich die Frage, ob die sich selbst als neutral und überparteilich verstehenden Beobachter nicht selbst zu politischen Aktivisten bzw. zu Lobbyisten werden, indem sie für bestimmte politische Ziele und Partikularinteressen Partei ergreifen. Die Legitimationsfrage, ob eine angeblich dem Gemeinwohl bzw. dem öffentlichen Interesse dienende Kampagne oder Position der zumeist als gemeinnützige Vereine operierenden Watchdog-NGOs tatsächlich (a) von allen Bürgern oder zumindest einer großen Mehrheit der Bevölkerung unterstützt wird und (b) dem Wohl aller oder zumindest einer großen Mehrheit dient, lässt sich freilich nicht theoretisch abstrakt ein für alle Male, sondern nur empirisch am konkreten Einzelfall klären.

## 5 Perspektiven für Staat und Watchdogs

Schon im vordigitalen Zeitalter existierten Organisationen, die den Staat kritisch beobachtet haben (z. B. *Bund der Steuerzahler Deutschland* oder *Transparency International Deutschland*). Allerdings haben es – wie oben erläutert – die in den vergangenen Jahrzehnten zu verzeichnenden Entwicklungen im Bereich Informations- und Kommunikationstechnik den „Wachhunden der Demokratie“ erleichtert, große Mengen an Informationen über Organisationen und Einzelpersonen in Politik und Verwaltung zu sammeln und öffentlich zu verbreiten. Ihre Berichte über (vermeintliches oder tatsächliches) politisch-administratives Fehlverhalten können sie heutzutage direkt an ztausende Nutzer von E-Mail, Facebook, Twitter und anderen Internet-Diensten versenden; und die Empfänger solcher Nachrichten können diese selbst wiederum an eine Vielzahl weiterer Personen weiterleiten (Stichworte: Multiplikator-/Schneeballeffekt, Candy-/Shitstorm). Die digitale Revolution hat politisches und administratives Handeln in dem in diesem Beitrag betrachteten Kontext also insbesondere insofern verändert, als dass viele Akteure in Politik und Verwaltung angesichts der den Watchdogs nun zur Verfügung stehenden, verbesserten Kontroll- und Veröffentlichungsmöglichkeiten noch genauer darauf achten werden, was sie tun oder nicht tun.

Zwar haben sich in Deutschland, Großbritannien, den USA und anderen Ländern einige Watchdog-Organisationen etabliert. Aber genauso wie im Falle von Wirtschaftsunternehmen, staatlichen Behörden oder politischen Parteien kann es natürlich sein, dass eine Watchdog-NGO „stirbt“ bzw. geschlossen wird. Zum einen könnten – was oben unter dem Stichwort Kollektivgut- bzw. Trittbrettfahrer-Problematik angesprochen wurde – solche Organisationen in finanzielle Schwierigkeiten geraten, so dass sich der aufgenommene Organisationsbetrieb (Büros, Mitarbeiter für Recherchen usw.) nicht aufrechterhalten lässt. Zum anderen könnte auch der Fall eintreten, dass eine Watchdog-Organisation überflüssig wird und geschlossen wird, da der betrachtete Politik-/Verwaltungsbereich inzwischen so transparent geworden ist, dass die bereitgestellten Informationen aus Sicht von Journalisten und anderen Bürgern keinen Mehrwert mehr erzeugen.

Warum sollte man – um ein Beispiel zu geben – noch auf das Informationsmaterial von *Abgeordnetenwatch* zurückgreifen, wenn der Deutsche Bundestag und die Länderparlamente entscheiden würden, von nun an selbst die Informationen in puncto Abgeordneten-Nebentätigkeiten, Lobbykontakte, Parteispenden etc. zu veröffentlichen, die bislang mühsam von Watchdogs recherchiert werden? Gerade solche Organisationen, deren Aktivitäten maßgeblich zu einer immer weitergehenden Verschärfung von Offenlegungsvorschriften in Politik und Verwaltung beigetragen haben, könnten sich quasi selbst überflüssig machen und sozusagen zum Opfer ihres eigenen Erfolges werden. Denn die Instrumente zur Sammlung, Verarbeitung und Verbreitung von Informationen, die Watchdogs im digitalen Zeitalter nutzen, stehen im Prinzip auch den politisch-administrativen Akteuren zur Verfügung. Letztere müssten allerdings garantieren können, dass das von ihnen bereitgestellte Informationsmaterial die eigenen Aktivitäten genauso korrekt und wahrheitsgemäß darstellt, wie das – zumindest im Idealfall – die Materialien politisch unabhängiger, zivilgesellschaftlicher „Wachhunde“ tun.

Dies leitet über zu einem weiteren Problem, dass sich in Gegenwart und Zukunft in Hinblick auf die Aktivitäten von Watchdog-Organisationen stellt: Wie kann in Zeiten von „Fake News“ sichergestellt werden, dass diese „Demokratiewächter“ nicht selbst Falschmeldungen bzw. Fehlinformationen verbreiten? Anders gefragt: Wer überwacht die Überwacher? Zwar dürften sich falsche Behauptungen über Parlamentarier, Minister, Bürgermeister oder Behördenleiter kaum dauerhaft halten. Aber wenn Akteure in Politik und Verwaltung fälschlicherweise in Misskredit geraten, kann das ihr „Image“ bzw. ihre Reputation schädigen und ihre Karriere beenden, bevor eine Klärung erfolgt. Sie können zwar selbst die klassischen Medien, das Internet und Social Media nutzen, um ihre Sicht der Dinge unter das Volk zu bringen; und sie können auch Gerichte anrufen, wenn ein falsches Zeugnis über sie verbreitet wird. Medien und Justiz stellen somit – zumindest im Idealfall – ein Korrektiv dar. Aber die Nutzung dieser Korrekturmechanismen kostet Zeit, wohingegen es relativ schnell und einfach möglich ist, einen „Shitstorm“ auszulösen. Und ein Gerücht, da habe etwas nicht gestimmt, bekommt man mitunter nie wieder ganz aus der Welt (und aus dem *World Wide Web*).

Wenn sich allerdings herausstellen sollte, dass eine Watchdog-Organisation Falschmeldungen bzw. unwahre Behauptungen verbreitet hat, dann schadet dies ihrer Reputation. Die Überwacher haben, sofern sie länger im Geschäft bleiben möchten, demnach selbst einen Anreiz, möglichst korrekte, wahrheitsgetreue Informationen anzubieten. Denn angesichts der Vielzahl an Informationsanbietern, die heutzutage in den klassischen Medien sowie im virtuellen Raum um die Aufmerksamkeit der Bürger wetteifern und sich gegenseitig korrigieren können, dürfen sich langfristig nur solche Anbieter durchsetzen, die glaubwürdige Informationen anbieten (Schnellenbach 2018). Ob die Mechanismen „Reputation“ und „Wettbewerb“ im digitalen Zeitalter wirklich ausreichen, um zu verhindern, dass selbst ernannte „Demokratiewächter“ selbst zur Gefahr für die Demokratie werden – etwa, weil sie die öffentliche Meinung mittels der Verbreitung von „Fake News“ zu ihren Gunsten zu manipulieren versuchen –, muss sich zeigen.

---

## Literatur

- Besley, Timothy. 2006. *Principled agents? The political economy of good government*. Oxford: Oxford University Press.
- Buzogány, Aron. 2016. Wer hat Angst vor Abgeordnetenwatch? Repräsentation, Responsitivität und Transparenzforderungen an Abgeordnete des Deutschen Bundestages. *Zeitsch Vergleich Politikwissensch* 10(Suppl. 2): 67–89.
- Drücke, Ricarda. 2018. Medien, Öffentlichkeit und Demokratie: Zur Watchdog-Funktion von Medien. *Forschungsjournal Soz. Bewegung*. 31(3): 19–28.
- Geys, Benny, und Karsten Mause. 2012. Delegation, accountability and legislator moonlighting: Agency problems in Germany. *German Politics* 21(3): 255–273.
- Geys, Benny, und Karsten Mause. 2019. Politicians. In *Encyclopedia of law and economics*, Hrsg. Alain Marciano und Giovanni B. Ramello, 1607–1610. New York: Springer.
- Greef, Samuel, und Lukas Kiepe. 2018. Staatsnahe Watchdog-Organisationen. *Forschungsjournal Soz. Bewegung*. 31(3): 28–37.

- Mause, Karsten. 2018. Korruption – Zur Notwendigkeit und Gefahr der Einzelfall-Analyse. In *Korruptionsbekämpfung vermitteln: Didaktische, ethische und inhaltliche Aspekte in Lehre, Unterricht und Weiterbildung*, Hrsg. Sebastian Wolf und Peter Graeff, 49–77. Wiesbaden: Springer VS.
- Olson, Mancur. 1965. *The logic of collective action: Public goods and the theory of groups*. Cambridge: Harvard University Press.
- Pörksen, Bernhard, und Hanne Detel. 2012. *Der entfesselte Skandal. Das Ende der Kontrolle im digitalen Zeitalter*. Köln: Halem.
- Schiffers, Maximilian. 2018. Zivilgesellschaftliche Aufpasser brauchen langen Atem: Die watchdog-Funktion von NGOs am Beispiel von LobbyControl. *Forschungsjournal Soziale Bewegungen* 31(3): 53–63.
- Schnellenbach, Jan. 2018. On the behavioral political economy of regulating fake news. *ORDO – Jahrbuch für die Ordnung von Wirtschaft und Gesellschaft* 68:159–178.
- Speth, Rudolf. 2018a. Machtkontrolle durch Watchdogs. *Forschungsjournal Soziale Bewegungen* 31(3): 6–18.
- Speth, Rudolf. 2018b. Zivilgesellschaftliche Watchdogs. *Forschungsjournal Soz. Bewegung* 31(1–2): 204–214.
- Wewer, Göttrik. 2015. *Die Lobby des Guten: Interesse und Gemeinwohl im digitalen Zeitalter*. Kiel: Lorenz-von-Stein-Institut.

---

## **Teil VI**

### **Politikfelder und Instrumente**



---

# Digitalpolitik

Samuel Greef

## Inhalt

1 Klärung des Begriffs .....	464
2 Theoretische Grundlagen .....	465
3 Praktische Anwendung .....	466
4 Auswirkungen .....	471
5 Künftige Entwicklungen .....	472
Literatur .....	473

---

## Zusammenfassung

Aus der Digitalisierung von Wirtschaft, Gesellschaft und Politik erwachsen vielfältige Herausforderungen. Das politische Handlungsfeld, das auf die Bearbeitung, Steuerung und Gestaltung dieses Bereichs in seiner inhaltlichen, institutionellen und prozessualen Dimension abzielt, ist die Digitalpolitik. Dieser Gegenstands- und Problembereich stellt jedoch kein etabliertes, eigenständiges *Politikfeld* dar. Zwar findet eine Institutionalisierung auf Bundesebene statt, bislang fehlen aber klare Zuständigkeiten, Entscheidungskompetenzen und ein starkes Steuerungszentrum für eine koordinierte Gestaltung der *digitalen Transformation*.

---

## Schlüsselwörter

Digitale Transformation · Netzpolitik · Politikfeld · Governance · Digitalpolitik

---

S. Greef (✉)

Gesellschaftswissenschaften, Universität Kassel, Kassel, Deutschland

E-Mail: [greef@uni-kassel.de](mailto:greef@uni-kassel.de)

## 1 Klärung des Begriffs

Die Digitalisierung wird als ein – wenn nicht sogar der zentrale – Megatrend dieses Jahrtausends identifiziert. Vielfach ist von einer digitalen Revolution oder dem digitalen Zeitalter die Rede. Dabei macht die unbestimmte Benutzung des Begriffs deutlich, dass das grundlegende Phänomen der „Verdatung“ – die Umwandlung von analogen Werten in digitale Daten – in seinen Auswirkungen weit über den zugrunde liegenden technischen Vorgang hinausgeht. Der Wirkungsradius der mit der Digitalisierung verbundenen Wandlungsprozesse kennt keine Grenzen. Sie diffundieren sowohl zwischen den gesellschaftlichen, wirtschaftlichen und politischen Sphären innerhalb der Nationalstaaten, als auch über Staatsgrenzen hinweg. Dabei eröffnen die rasanten, sich gegenseitig verstärkenden technologischen Entwicklungen und damit einhergehenden Veränderungen vielfältige Herausforderungen (Problemwahrnehmung). Diese finden in Form komplexer Problemlagen Eingang in das politische System (Agenda Setting und Problemdefinition). Die Bearbeitung dieser Probleme (Politikformulierung und -implementierung) findet in einem politischen Prozess unter Beteiligung von staatlichen Akteuren und – in aller Regel – nicht-staatlichen Akteuren statt. Hier treffen das Digitale und die Politik wechselseitig aufeinander. Mit den Gestaltungsnotwendigkeiten und -perspektiven (insbesondere in Form von Steuerung, regulativen Eingriffen, Koordinierung und Selbstregulierung), die sich aus diesem Aufeinandertreffen ergeben, beschäftigt sich Digitalpolitik.

Der Begriff umfasst dabei die inhaltliche, institutionelle und prozessuale Ebene der Herbeiführung allgemein verbindlicher Entscheidungen, soweit diese eine digitale Dimension haben. Er umreißt also zunächst ein politisches Handlungsfeld. Aus dieser Perspektive handelt es sich bei Digitalpolitik um ein Querschnittsthema, das alle *Politikfelder* beeinflusst. Gleichzeitig ist es ein (thematisch) begrenztes, neues Handlungsfeld, welches allerdings kein eigenständiges, abgrenzbares *Politikfeld* darstellt. Insbesondere der ubiquitäre und vielfach unbestimmte Gebrauch des Begriffs macht es notwendig, zu klären, welche Themen und Inhalte unter „Digitalpolitik“ fallen. Dabei ist Digitalpolitik von dem in der medialen Darstellung häufig gebrauchten Begriff der *Netzpolitik* abzugrenzen, der sich auch bei vielen zivilgesellschaftlichen Akteuren etabliert hat. Digitalpolitik ist der deutlich weiter gefasste Begriff und lässt sich in vier inhaltliche Ebenen untergliedern, wohingegen sich *Netzpolitik* primär auf die ersten beiden Ebenen bezieht:

1. Die erste Ebene von Digitalpolitik ist die (Netz-)Infrastrukturpolitik. Ihr Bezugspunkt ist das Internet als elementare Infrastruktur, auf dem dann die digitalen Dienste und Inhalte aufbauen.
2. Die zweite Ebene stellt die Dienst- und Inhaltspolitik dar. Sie bezieht sich auf Policies, die im Zusammenhang mit Internet-Diensten (Webseiten, E-Mail, Soziale Netzwerke und andere Plattformen) sowie den über diese vermittelten Inhalten stehen.
3. Digitalpolitik beschäftigt sich auf einer dritten Ebene mit der Herausbildung und Ausgestaltung einer digitalen Verwaltung, welche die technischen Möglichkeiten des digitalen Zeitalters effizient und effektiv nutzt (E-Government).

- 
4. Eine vierte Ebene bilden Fragen der digitalen Teilhabe und politischen Partizipation (E-Democracy).

Da das Internet und die Digitalisierung globale Phänomene sind, muss sich staatliche Digitalpolitik auch mit europäischen Entscheidungen und internationalen Vereinbarungen beschäftigen. Darin unterscheidet sie sich nicht von anderen *Politikfeldern*. Während beispielsweise die europäische Datenschutz-Grundverordnung (DSGVO) für EU-Mitglieder unmittelbar geltendes Recht darstellt, müssen Fragen der Internet *Governance* (im deutschen Kontext bisweilen auch als Internetpolitik bezeichnet), international ausgehandelt werden. Aber auch unterhalb der nationalstaatlichen Ebene müssen sich Länder und Kommunen mit Digitalpolitik beschäftigen.

---

## 2 Theoretische Grundlagen

Für die Frage, wie gesellschaftliche Probleme politisch bearbeitet werden, spielt unter anderem die Gestalt des Problemfeldes eine zentrale Rolle. Etablierte *Politikfelder* sind durch vier Merkmale gekennzeichnet:

1. *Politikfelder* sind inhaltsbezogene (Policy-Dimension) politische Handlungsfelder. Sie stellen daher einen abgegrenzten Gegenstands- und Problembereich dar. Dieser vereint (komplexe) Problemzusammenhänge (Issues) und darauf gerichteten Diskurse, Policies, Maßnahmen und (Steuerungs-)Instrumente.
2. Konstitutiv für *Politikfelder* sind spezifische Akteurskonstellationen. Sie stellen die komplexen Interaktionsstrukturen zwischen konkreten, problembereichsrelevanten und etablierten Akteuren dar.
3. Die Interaktion zwischen den Akteuren wird durch den institutionellen Kontext strukturiert. Für das *Politikfeld* spezifische Institutionen, (Entscheidungs-)Verfahren und Ressourcenzuweisungen beschränken die Gestaltungsoptionen und den strategischen Handlungsspielraum der Akteure.
4. *Politikfelder* sind durch eine (begrenzte) Autonomie gekennzeichnet, die eine politikfeldspezifische Problemlösungsfähigkeit mit sich bringt. Dazu sind nicht nur Ressourcen notwendig, sondern den Akteuren müssen auch entsprechende Handlungs- und Entscheidungskompetenzen vorliegen beziehungsweise zugewiesen werden.

Ein so begrenztes Problem- und Handlungsfeld – ein *Politikfeld* – wird häufig mit einem „sprechenden Namen“ wie Sozialpolitik oder Umweltpolitik bezeichnet. Komplexe Problemlagen sind jedoch gerade dadurch gekennzeichnet, dass ihr Problembereich über einzelne *Politikfelder* hinausreicht. Wenn von der Digitalisierung aller Lebensbereiche die Rede ist, deutet das schon darauf hin, dass gesellschaftliche Herausforderungen und politische Themen heute fast immer auch eine digitale Dimension besitzen. Insofern sind alle Ressorts durch die digitale Transformation gefordert. Nicht beantwortet ist damit jedoch die Frage, wie die Digitalpolitik innerhalb der Parteien, des Parlaments und der Regierung am besten zu

koordinieren ist. Man kann das Thema, wie in einigen Ländern geschehen, federführend einem Ministerium zuordnen, oder ein gesondertes „Digitalministerium“ gründen und dort alle davon berührten Fachaufgaben bündeln. Man kann die Koordinierung der Digitalpolitik aber auch zur „Chefsache“ erklären und in der Regierungszentrale übernehmen. Alle diese Ansätze haben ihre spezifischen Vorteile und Nachteile.

---

### 3 Praktische Anwendung

Zentrale Fragen in der (Netz-)Infrastrukturpolitik drehen sich um technische Aspekte und infrastrukturelle Grundlagen wie die Netzarchitektur und -infrastruktur (insbesondere Breitbandausbau durch Glasfaser, Vektorung und 5G), die Etablierung von Standards, Schnittstellen, Protokollen und Sicherheitskonzepten. Im weitesten Sinne können auch die Themen Elektromobilität, autonomes Fahren und die unter dem Schlagwort Industrie 4.0 verhandelten Aspekte (Automatisierung und Robotik in der Smart Factory, Internet der Dinge, 3D-Druck) unter diesem Teilbereich verortet werden. Weitere hier anzusiedelnde Themen sind die Debatte um Netzneutralität sowie Regulierungsfragen in Bezug auf Wettbewerb und Netzzugang.

Zu den konkreten Themen in der Dienst- und Inhaltspolitik zählen das Urheberrecht, Datenschutz und informationelle Selbstbestimmung oder Jugendmedienschutz und Sicherheitsfragen. Gerade für die genannten Themen gilt, dass sie in ihrem Kern nicht erst mit der Digitalisierung, sondern bereits in der analogen Welt zum Gegenstand politischer Steuerung- und Regulierungsprozesse geworden sind. Aber auch die aktuellen Debatten um den Umgang mit Fake News und Hate Speech in sozialen Netzwerken sind hier zu verorten. Genauso gehören neue Themen wie Big Data, Algorithmen, Künstliche Intelligenz und Machine Learning sowie die Diskussionen um die Regulierung von automatisierten Entscheidungsprozessen oder plattformvermittelter digitaler Arbeit (Crowd-, Cloud- und Gigworking) in diesen Teilbereich.

Zentrale Themenfelder einer digitalen Verwaltung sind zum einen deren Öffnung, etwa im Sinne einer größeren Transparenz von Verwaltungshandeln, leichter verfügbaren Daten und einfacheren Zugängen zu Informationen (Open Data, Open Government, Informationsfreiheit) (siehe Kap. ► „Offene Daten (Open Data)“ in diesem Handbuch). Zum anderen geht es um die Digitalisierung der Schnittstellen und die intelligente Vernetzung sowohl zwischen den Verwaltungsinstanzen als auch zwischen Verwaltung und Bürgerinnen. Konkrete Themen sind hier etwa der elektronische Personalausweis, die elektronische Gesundheitskarte (E-Health), die elektronische Steuererklärung und die Bereitstellung internetbasierter Bürgerportale zur Digitalisierung von Behördengängen.

Der Bereich der *digitalen Teilhabe* und politischen Partizipation umfasst einerseits die möglichen Partizipationsangebote über das Internet (*E-Participation* und *E-Democracy*), vom Einreichen von elektronischen Petitionen beim Deutschen Bundestag bis hin zu Fragen der Anwendbarkeit von elektronischen Wahlverfahren (*E-Voting*) (siehe Kap. ► „Elektronische Wahlen und Abstimmungen (Electronic

Voting)“ sowie Kap. ► „E-Democracy“ in diesem Handbuch). Andererseits stellt die Digitalisierung aber auch jede/n einzelne/n BürgerIn vor höhere Anforderungen. Die Gestaltung der damit notwendigen Qualifizierungs- und (Weiter-)Bildungsbedarfe werden ebenfalls im Aufgabenbereich der Digitalpolitik verortet. Zu den zu bearbeitenden Problemen gehört etwa der *Digital Divide* in der Bevölkerung (siehe Kap. ► „Digitale Ungleichheiten und digitale Spaltung“ in diesem Handbuch). Dabei geht es nicht nur um den physischen Zugang zu einem leistungsfähigen Internet, und damit den Breitbandausbau, sondern um die Fähigkeiten zum reflektierten Umgang mit Technik, Internetmedien und digitalen Angeboten. Die konkreten Themen gehen über die Nutzung digitaler Lehr- und Lernmittel genauso weit hinaus, wie über die reine Vermittlung von Medienkompetenz. Vielmehr wird unter dem Schlagwort der *Digital Literacy* neben dem kritischen Umgang mit Informations(über)angeboten, dem sicheren Bewegen im Netz auch ein grundlegendes Verständnis zentraler digitaler Mechanismen – wie die prinzipiellen Funktionsweise von Algorithmen – verstanden.

Mit dieser großen Bandbreite an digitalpolitischen Themen sind auf der Bundesebene eine Vielzahl von Institutionen betraut. Die Gestaltungsperspektive und digitalpolitische Leitlinien werden unter anderem in folgenden Dokumenten deutlich: die „Digitale Agenda 2014–2017“ (BMI/BMWi/BMVI 2017) und die ihr nachfolgende „Digitalstrategie“ der Bundesregierung, die „Digitale Strategie 2025“ des Bundesministeriums für Wirtschaft und Energie (BMWi) sowie die „Hightech-Strategie“ zur Forschungs- und Innovationspolitik des Bundesministeriums für Bildung und Forschung (BMBF). Federführend für die Digitale Agenda waren das BMWi, das Bundesministerium des Innern (BMI) sowie das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI). Daneben beschäftigen sich aber alle Ressorts mit digitalen Themen (siehe Tab. 1). Die Antwort des BMVI (vom Februar 2018) auf eine Kleine Anfrage der Fraktion Bündnis 90/Die Grünen verwies auf insgesamt 482 MitarbeiterInnen, die sich mit digitalen Fragen beschäftigten – verteilt auf 244 Teams in 76 Abteilungen in 14 Bundesministerien. In diesen breit gestreuten Zuständigkeiten kommt deutlich der Querschnittscharakter von Digitalpolitik zum Ausdruck.

Der Zuschnitt der Ministerien findet seine Entsprechung in den ständigen Ausschüssen des Deutschen Bundestages. Der Sonderausschuss „Digitale Agenda“ wurde aufgrund einer Empfehlung der Enquete-Kommission „Internet und digitale Gesellschaft“ (2010–2013) in der 18. Legislaturperiode ohne vorhandenes Gegenstück in der Regierung eingerichtet. Im Unterschied zu anderen Ausschüssen hat er nur eine mitberatende Funktion bei allen Themen, die eine digitale Dimension haben. Mit der Neuauflage der Großen Koalition in der 19. Legislaturperiode (2018–2021) wurde der Ausschuss erneut eingesetzt. Innerhalb der Bundesregierung wurde darüber hinaus ein Kabinettsausschuss für Digitalisierung installiert, dem unter Vorsitz der Kanzlerin alle Ministerinnen angehören. Des Weiteren wurde zur Koordinierung der Digitalpolitik im Kanzleramt eine „Staatsministerin für Digitalisierung“ ohne eigenes Ressort berufen. Zusätzliche Expertise erhofft sich die Bundesregierung durch die Einsetzung eines Digitalrats, dem Persönlichkeiten aus Wirtschaft und Wissenschaft, nicht aber aus der Zivilgesellschaft, angehören.

**Tab. 1** Staatliche Institutionen und staatsnahe Akteure der Digitalpolitik in der 19. Legislaturperiode (2018–2021) auf Bundesebene

Institution	Rolle/Kompetenzen/Zuständigkeiten
Bundeskanzleramt	(Fach- und Dienstaufsicht über: BND)
Staatsministerin für Digitalisierung	Beauftragte der Bundesregierung für Digitalisierung, kommunikative Funktion
	Ressortübergreifende Beratung, Austausch und Koordination
	Bündelung der kultur- und medienpolitischen Aktivitäten
Bundesministerien	
Bundesministerium für Verkehr und digitale Infrastruktur (BMVI)	Netzinfrastruktur, Breitbandausbau (Netzallianz Digitales Deutschland); (Fachaufsicht über: BNetzA)
Bundesministerium des Inneren, für Bau und Heimat (BMI)	IT- und Cybersicherheit, Vorratsdatenspeicherung, E-Government; (Dienstaufsicht über: BfDI, Aufsicht über: BSI, ADIC)
Bundesministerium für Wirtschaft und Energie (BMWi)	Industrie 4.0, Digitalisierung der Wirtschaft, (Beirat Junge Digitale Wirtschaft, Digitalbotschafterin), Branchenförderung, Leistungsschutzrecht, Netzneutralität, Digitaler Mittelstand, Telekommunikationspolitik; (Gesamtaufsicht über: BNetzA)
Auswärtiges Amt (AA)	Cyber-Außenpolitik
Bundesministerium für Justiz und Verbraucherschutz (BMJV)	Verbraucher(daten)schutz, informationelle Selbstbestimmung, Urheberrecht
Bundesministerium für Arbeit und Soziales (BMAS)	Arbeiten 4.0, digitale Arbeitsformen, Beschäftigtendatenschutz
Bundesministerium für Bildung und Forschung (BMBF)	Forschungs-, Innovationspolitik (Hightech-Strategie, Internet-Institut), Digitale Bildung, Medienkompetenz
Bundesministerium für Gesundheit (BMG)	Digitale Gesundheitsinfrastruktur (elektronische Gesundheitskarte), E-Health
Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ)	Jugend(medien)schutz, Digitale Gesellschaftspolitik; (Aufsicht über: BPJM)
Bundesministerium der Verteidigung (BMVg)	Cybersicherheit, Cyberabwehr; (Aufsicht über: ADIC)
Bundesministerium der Finanzen (BMF)	Digitaler Finanzmarkt, FinTech (Rechts-/ Fachaufsicht: BaFin)
Bundesbehörden	
Agentur für Disruptive Innovationen in der Cybersicherheit und Schlüsseltechnologien (ADIC)	Forschungs- und Entwicklungsförderung für Cybersicherheit
Bundesnetzagentur (BNetzA)	Wettbewerbsregulierung Telekommunikation, Verbraucherschutz
Bundesprüfstelle für jugendgefährdende Medien (BPJM)	Jugendmedienschutz

(Fortsetzung)

**Tab. 1** (Fortsetzung)

Institution	Rolle/Kompetenzen/Zuständigkeiten
Bundesamt für Sicherheit in der Informationstechnik (BSI)	IT-Sicherheit, Nationales Cyber-Abwehrzentrum
Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)	Datenschutz, informationelle Selbstbestimmung
Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)	FinTech
Bundestag	
Ständige Ausschüsse	Spiegelbildlich zum jeweiligen Ministerium/Ressort
Ausschuss Digitale Agenda	Alle Themen (ausschließlich beratende Funktion)

Quelle: Eigene Zusammenstellung; Greef 2017, S. 34; Rieger 2014, S. 5–11

Zusätzlich erarbeiten eine Datenethikkommission sowie eine Enquete-Kommission „Künstliche Intelligenz“ Handlungsempfehlungen zu digitalen Themen, die ethische Fragen und Fragen gesellschaftlicher Verantwortung aufwerfen (siehe Kap. ► „Digitale Ethik“ in diesem Handbuch). Ähnliche Gremien existieren teilweise auch in den Ländern.

Unterhalb der Ministerien beschäftigen sich weitere Behörden mit digitalen Fragen. Für die wettbewerbliche Regulierung der digitalen Wirtschaft und von Netzinfrastruktur Anbieter ist neben dem Bundeskartellamt die Bundesnetzagentur (BNetZA) zuständig. Um Datenschutzfragen kümmert sich die bzw. der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI). In der IT-Sicherheit spielt das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine wichtige Rolle, etwa durch Empfehlungen zum sicheren Einsatz von technischen Systemen und die Meldepflicht von Sicherheitsvorfällen durch Betreiber kritischer Infrastruktur. Zusätzlich wird eine Agentur für Disruptive Innovationen in der Cybersicherheit und Schlüsseltechnologien (ADIC) aufgebaut.

In der Konsequenz verteilen sich die Zuständigkeiten für die verschiedenen Facetten von Digitalpolitik in der 19. Legislaturperiode relativ unübersichtlich. Weitere wichtige Akteure in der Digitalpolitik sind die Parteien. Zwar konnten sich die Piraten aus verschiedenen Gründen nicht dauerhaft in den Parlamenten etablieren, ihr kurzzeitiger Höhenflug trug jedoch maßgeblich dazu bei, dass VerfechterInnen digitalpolitischer Themen auch in den etablierten Parteien an Relevanz gewinnen konnten. Inzwischen existieren in allen Parteien SprecherInnen für Digitalpolitik und parteiinterne Arbeitsgruppen zu diesem Thema. Darauf hinaus entstanden parteinahme Organisationen, wie beispielsweise der SPD-nahe Verein „D64 – Zentrum für Digitalen Fortschritt“ oder „cnetz – Verein für Netzpolitik“ im Umfeld der CDU.

Neben diesen parteinahmen Akteuren existieren verschiedene weitere zivilgesellschaftliche Organisationen mit digitalpolitischen Schwerpunkten, die in drei Organisierungswellen entstanden (siehe Tab. 2). Das Spektrum beginnt bei Verbänden und Vereinen der ersten Generation (1980/90er-Jahre) mit Querschnittscharakter,

**Tab. 2** Zivilgesellschaftliche und parteinahe Akteure der Digitalpolitik

Zivilgesellschaftliche Organisation	Gründung	Themenschwerpunkt
Chaos Computer Club (CCC)	1981	Querschnitt
Digitalcourage (ehem. FoeBuD)	1987	Querschnitt
netzpolitik.org	2004	Querschnitt
Wikimedia	2004	Open Knowledge
AK Vorrat	2005	Vorratsdatenspeicherung
AK Zensur	2009	Netzsperren
Digitale Gesellschaft (digiges)	2010	Querschnitt
Gesellschaft für Freiheitsrechte (GFF)	2015	Informationelle Selbstbestimmung, Informations-, Meinungs- und Pressefreiheit
<b>Parteinahe Organisationen</b>		
C-Netz (CDU-nahe)	2012	Querschnitt
D64 (SPD-nahe)	2012	Querschnitt
LOAD (FDP-nahe)	2014	Querschnitt
netzbegründung (Grünen-nahe)	2014	Querschnitt

Quelle: Eigene Zusammenstellung; Dobusch [2014](#), S. 5

wie dem Chaos Computer Club (CCC) oder des FoeBuD (Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs; heute Digitalcourage). In der zweiten Generation (2000er-Jahre) entstanden sowohl Organisationen mit spezifischen Schwerpunkten (wie die Wikimedia zur Förderung offenen Wissens) als auch fluide organisierte Arbeitskreisen, die sich gegen konkrete Gesetzesvorhaben richteten, wie der AK Vorrat oder der AK Zensur. In der dritten Generation (seit den 2010er-Jahren) kamen dann zum einen weniger formalisierte Protestbewegungen hinzu. Diese bildeten sich etwa angesichts des von Edward Snowden enthüllten Überwachungs- und Spionageskandals, des Zugangserschwerungsgesetzes oder des Handelsabkommens gegen Produktpiraterie ACTA. Zum anderen entstanden aber auch neue Vereine, die dezidiert eine große Bandbreite digitalpolitischer Themen bearbeiten, wie etwa die Digitale Gesellschaft, sowie hybride Typen wie die zwischen Journalismus und advokatorischer Interessenvertretung einzuordnende Plattform netzpolitik.org.

Neben netzaktivistischen, bürgerrechtlichen oder verbraucherschutzorientierten Akteuren steht die wirtschaftsbezogene Interessenvertretung. Im Feld der Digitalpolitik sind dies im Bereich der organisierten Interessen vor allem die IT-Branchenverbände Bitkom und Eco – Verband der Internetwirtschaft e.V., der Bundesverband Deutsche Startups e.V., der Bundesverband Digitale Wirtschaft (BVDW), der Bundesverband IT-Mittelstand (BITMi), die Internet Economy Foundation (IEF), die Initiative D21 sowie Organisationen aus der Medienbranche. Darüber hinaus spielen

---

die technologiefokussierten Unternehmen und Konzerne als Advokaten ihrer Eigeninteressen eine bedeutende Rolle.

Die Digitalpolitik zeichnet sich aber nicht nur durch eine ausgeprägte Organisationslandschaft und Akteurskonstellation aus. Vielmehr ist sie auch durch eigene Arenen und eine eigenlogische Ausgestaltung der Aushandlungsprozesse geprägt. Für die Gestaltungs- und Regulierungsperspektive von Digitalpolitik spielen unterschiedliche Verhandlungsarenen und Steuerungsformen sowie -instrumente eine Rolle. Neben der direkten hierarchischen Steuerung durch den Staat sind in digitalpolitischen Problembereichen vielfach deutlich stärker *governance*-orientierte Formen der Aus- und Verhandlung vorzufinden. Damit sind Konzepte von Steuerung gemeint, in denen nicht der Staat von oben „durchregiert“, sondern gemeinsam mit betroffenen Akteuren gestaltet oder diesen eine Selbstregulierung ermöglicht. Dies trifft nicht nur auf die internationale Ebene zu, auch wenn dort, aufgrund nationalstaatlicher Souveränität, Aushandlungen in der Regel in koordinierenden und standardisierenden Gremien stattfinden. Dabei wird teilweise in Multi-Stakeholder-Prozessen versucht, neben den Nationalstaaten, technischen Expertinnen, wirtschaftlichen Interessengruppen und Konzernen, eine breitere Zahl an relevanten Akteurinnen aus der Zivilgesellschaft mit einzubinden. Auch in Deutschland finden sich vielfach auf den Koordinationsmodus der Verhandlung setzende Gremien und Dialogprozesse, in denen der Staat eher als Moderator denn als Steuerungssubjekt auftritt. Die Bandbreite reicht dabei von einer Öffnung der politischen Problembearbeitung durch Formen einer offenen Konsultation bis hin zu Gremien der Selbst- und Ko-Regulierung. Beispiele hierfür sind die Dialogprozesse zur Plattformökonomie (Grün-/Weißbuch Digitale Plattformen des BMWi) oder zu digitaler Arbeit (Grün-/Weißbuch Arbeiten 4.0 des BMAS) sowie themenspezifische Arbeitsgruppen zur Etablierung von technischen Standards in der digitalisierten Industrie (Plattform Industrie 4.0 von BMWi und BMBF). Im Primat des Verhandlungsmodus in der Digitalpolitik spiegelt sich die Komplexität der mit der Digitalisierung einhergehenden Herausforderungen wider.

Diese Komplexität wird noch einmal dadurch potenziert, dass unterschiedliche oder gegeneinanderstehende Regulierungsziele eine Rolle spielen können. Besonders deutlich zeigen sich diese etwa im Spannungsverhältnis von Freiheit und Sicherheit oder bei der Abwägung zwischen dem Datenschutz von VerbraucherInnen und Beschäftigten auf der einen und wirtschaftlicher Innovations- und Wettbewerbsfähigkeit auf der anderen Seite. Aber selbst beim klassischen Thema des Urheberrechts geht es um den Ausgleich der unterschiedlichen Interessen von NutzerInnen, UrheberInnen und VerwerterInnen.

---

## 4 Auswirkungen

Digitalpolitik lässt sich als ein abgegrenzter Gegenstands- und Problembereich, nicht jedoch als eigenständiges *Politikfeld* verstehen. Vielmehr verläuft Digitalpolitik quer zu allen anderen *Politikfeldern*, da letztlich alle gesellschaftlichen Bereiche von der *digitalen Transformation* betroffen sind. Dass ein Handlungsfeld einen solchen

Querschnittscharakter besitzt, ist freilich auch bei anderen Themen gegeben. Allerdings wird in den Debatten um Digitalpolitik immer wieder – so etwa auch im Rahmen der Regierungsbildung nach der Bundestagswahl 2017 – von verschiedenen Akteuren die Forderung erhoben, diesen Querschnittsbereich in einem federführend zuständigen Digitalministerium *politikfelder*-übergreifend zu koordinieren. Die fehlende Koordinierung wird von mehr als 50 Akteuren aus Wirtschaft, Zivilgesellschaft, Wissenschaft und parteinahen Verbänden aber auch von einzelnen Abgeordneten, welche die Petition zur Ernennung einer/s DigitalministerIn ([digitalministerium.org](http://digitalministerium.org)) unterstützen, mit dafür verantwortlich gemacht, dass Deutschland droht, die Digitalisierung zu „verschlafen“ und „endgültig den Anschluss zu verlieren“.

Dass bezogen auf die bisherigen Ergebnisse der Digitalpolitik der Bundesregierung noch erhebliches Verbesserungspotenzial besteht, weist etwa der Digital Economy and Society Index (DESI) aus, der alle 28 EU-Mitgliedsstaaten in ihrer digitalen Performanz und Wettbewerbsfähigkeit in fünf Schwerpunktbereichen vergleicht. Im Report 2018 kommt Deutschland etwa im Bereich „Konnektivität“ (Breitband) auf Platz 13 von 28, eine Verschlechterung um 2 Plätze im Vergleich zu 2017, da die anderen EU-Mitgliedsstaaten hier schnellere Fortschritte gemacht haben. Bei den „Digitalen öffentlichen Diensten“ steht Deutschland, insbesondere aufgrund der sehr geringen Verbreitung internetbasierter Interaktion zwischen BürgerInnen und Verwaltung, weiterhin auf Platz 21. Trotz etwas größerer Fortschritte in den anderen Bereichen, etwa durch die verstärkte Integration der Digitaltechnik durch die deutsche Wirtschaft und die gestiegene Nutzung von Internetdiensten durch die Bevölkerung, verbleibt Deutschland im Gesamtvergleich auf Platz 14 von 28 Europäische Kommission (2018).

Die hierin sichtbar werdenden Entwicklungsprobleme sind auch auf das Fehlen einer kongruenten Gesamtstrategie zum Umgang mit der *digitalen Transformation* zurückzuführen. Eine autonome Problemlösungsfähigkeit im Handlungsfeld der Digitalpolitik hat sich bisher nicht herausgebildet, nicht zuletzt aufgrund zwischenministerieller Kompetenzstreitigkeiten. Allerdings befindet sich der institutionelle Kontext weiterhin in Bewegung.

---

## 5 Künftige Entwicklungen

Der zur Neukonstituierung des Ausschusses Digitale Agenda von dessen Vorsitzenden geforderte Zuwachs an Kompetenzen und eine mögliche (geteilte) Federführung bei einzelnen Gesetzesentwürfen sind bislang ausgeblieben. Auf der Ebene des Parlaments unterliegt Digitalpolitik damit auch zukünftig der Konkurrenz zwischen den Fachausschüssen.

Dagegen haben auf der Ebene der Regierung die regelmäßige wiederkehrenden Forderungen nach einer stärker zentrierten Koordinierung durchaus Widerhall gefunden. Zwar fehlt auch weiterhin ein zum Bundestagsausschuss Digitale Agenda kongruentes Steuerungszentrum auf der Ressortebene. Allerdings ist eine koordinierte Digitalpolitik „aus einer Hand“ auch in anderen Modellen als einem eigenständigen Digitalministerium denkbar. So sind auch die Versuche einer stärkeren

Institutionalisierung digitalpolitischer Themen auf der Bundesebene einzuordnen. Der Kabinettsausschuss für Digitalisierung und die neue Staatsministerin sollen für eine bessere Koordinierung der Digitalpolitik innerhalb der Regierung sorgen. Ob sie den Erwartungen an ihre koordinierende Rolle gerecht werden und sich zu einem Steuerungszentrum entwickeln können, wird sich erst noch zeigen müssen. So könnte das Büro der Staatsministerin in die Rolle eines Spiegelreferats zum Bundestagsausschuss Digitale Agenda hineinwachsen. Nicht überzeugt davon scheint die FDP-Fraktion zu sein, die im Mai 2019 mit dem Antrag „Smart Germany“ erneut die Etablierung eines Bundesministeriums für Digitalisierung fordert. Die Institutionalisierung der Digitalpolitik auf der Regierungsebene folgt damit weiterhin dem Trial and Error Ansatz - freilich auch in anderen Handlungsfeldern kein unbekanntes Vorgehen.

Auf der inhaltlichen Ebene hat das Kanzleramt das in den letzten Jahren sichtbar geworden strategische Defizit im Umgang mit der Digitalisierung erkannt. So zeugen die Umsetzungsstrategie zur Gestaltung des digitalen Wandels (digital-made-in.de), die zum Digitalgipfel Ende 2018 vorgestellte Strategien für Künstliche Intelligenz, die Strategie zur digitalen Arbeit 4.0 und die im Sommer 2019 erscheinende Nationale Blockchain-Strategie vom Ringen um die Entwicklung kohärenter Gestaltungsperspektiven auf als zentral identifizierten Zukunftsfeldern.

---

## Literatur

- BMI/BMWi/BMVI. 2017. *Legislaturbericht Digitale Agenda 2014–2017*. Frankfurt a. M.: Zarbock. [www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-agenda-legislaturbericht.pdf](http://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-agenda-legislaturbericht.pdf).
- Dobusch, Leonhard. 2014. *Digitale Zivilgesellschaft in Deutschland. Stand und Perspektiven 2014*. Berlin: FU Berlin. [http://edocs.fu-berlin.de/docs/servlets/MCRFileNodeServlet/FUDOCS\\_derivate\\_00000003411/discpaper2014\\_7.pdf](http://edocs.fu-berlin.de/docs/servlets/MCRFileNodeServlet/FUDOCS_derivate_00000003411/discpaper2014_7.pdf).
- Europäische Kommission. 2018. Index für die digitale Wirtschaft und Gesellschaft (DESI). 2018. Länderbericht Deutschland. [http://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=52332](http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=52332). Zugegriffen am 30.11.2018.
- Greef, Samuel. 2017. *Netzpolitik. Entsteht ein Politikfeld für Digitalpolitik?* Kassel: kup. [www.upress.uni-kassel.de/katalog/Download.php?ISBN=978-3-7376-0316-4&type=pdf-d](http://upress.uni-kassel.de/katalog/Download.php?ISBN=978-3-7376-0316-4&type=pdf-d).
- Rieger, Sebastian. 2014. *Wie verankert man Digitalpolitik in der Bundesregierung? Zuständigkeiten, Entstehungsprozess und Führungsmodell der digitalen Agenda*. Berlin: stiftung neue verantwortung. [www.stiftung-nv.de/sites/default/files/policy\\_brief\\_digitale\\_agenda.pdf](http://www.stiftung-nv.de/sites/default/files/policy_brief_digitale_agenda.pdf).

## Weiterführende Literatur

- Betz, Joachim, und Hans-Dieter Kübler. 2013. *Internet Governance. Wer regiert wie das Internet?* Wiesbaden: Springer VS.
- Busch, Andreas, Yana Breindl, und Tobias Jakobi. 2019. *Netzpolitik. Ein einführender Überblick*. Wiesbaden: Springer VS.
- Hösl, Maximilian, und Abel Reiberg. 2016. Netzpolitik in statu nascendi. Eine Annäherung an Wegmarken der Politikfeldgenese. In *Text Mining in den Sozialwissenschaften. Grundlagen und*

- Anwendungen zwischen qualitativer und quantitativer Diskursanalyse*, Hrsg. Matthias Lemke und Gregor Wiedmann, 315–342. Wiesbaden: Springer VS.
- Jaume-Palasi, Lorena, Julia Pohle, und Matthias Spielkamp. 2017. *Digitalpolitik. Eine Einführung*. Berlin: Wikimedia Deutschland e.V. und iRights.international. [https://irights.info/wp-content/uploads/2017/05/Digitalpolitik\\_-\\_Eine\\_Einfuehrung.pdf](https://irights.info/wp-content/uploads/2017/05/Digitalpolitik_-_Eine_Einfuehrung.pdf). Zugegriffen am 10.09.2018.
- Scheffel, Folke. 2016. *Netzpolitik als Policy Subsystem? Internetregulierung in Deutschland 2005–2011*. Baden-Baden: Nomos.



---

# Die Auswirkung von Digitalisierung auf Bildungs- und Sozialpolitik

Marius R. Busemeyer

---

## Zusammenfassung

In öffentlichen Debatten zu den Auswirkungen der digitalen Revolution auf die Arbeitsmärkte dominieren häufig pessimistische Zukunftsszenarien, die einen massiven Abbau von Beschäftigung und zunehmende Ungleichheit erwarten lassen. Im Gegensatz dazu gibt dieser Beitrag eine kurze Einführung in die sozialwissenschaftliche Forschung zu diesem Thema, die wesentlich differenziertere Befunde liefert. Ein weiterer Schwerpunkt dieses Kapitels ist die Diskussion der bildungs- und sozialpolitischen Reaktionen auf strukturelle Veränderungen im Zusammenhang mit der Digitalisierung. Hier werden unterschiedliche Policy-Lösungen wie Weiterbildung, lebenslanges Lernen, aktive Arbeitsmarktpolitik und das bedingungslose Grundeinkommen angesprochen. Das Kapitel schließt mit einer These zu den künftigen Entwicklungen, die besagt, dass politische Faktoren und Entscheidungen einen maßgeblichen Einfluss darauf haben werden, ob die Digitalisierung zu einer Verschärfung sozio-ökonomischer Ungleichheit beiträgt oder diese lindert.

---

## Schlüsselwörter

Bildung · Sozialpolitik · Ungleich · Automatisierung · Policy-Analyse

Radikaler technologischer Wandel in Form von Digitalisierung und Automatisierung hat zunehmend Auswirkungen auf den Arbeitsmarkt und damit indirekt auf Bildungs- und Sozialpolitik. Die exponentielle Verbreitung neuer Technologien eröffnet einerseits neue Beschäftigungsmöglichkeiten und generiert wirtschaftlichen Wohlstand. Andererseits werden zunehmend Befürchtungen geäußert, dass der radikale technologische Wandel einen neuen massiven Rationalisierungsprozess

---

M. R. Busemeyer (✉)

Fachbereich Politik- und Verwaltungswissenschaft, Universität Konstanz, Konstanz, Deutschland  
E-Mail: [Marius.Busemeyer@uni-konstanz.de](mailto:Marius.Busemeyer@uni-konstanz.de)

befördern könnte, der mit dem Abbau von Arbeitsplätzen und der Prekarisierung von bestehenden Arbeitsverhältnissen einhergehen würde.

Hier sollen die Konturen dieser noch am Anfang stehenden Debatten nachgezeichnet werden. Zunächst sind begrifflich und konzeptionell die unterschiedlichen Entwicklungen aufzuarbeiten, die in öffentlichen Diskussionen häufig mit dem Schlagwort „Digitalisierung“ der Arbeitswelt im Verbindung gebracht werden. Hierbei handelt es sich um durchaus unterschiedliche Phänomene – wie etwa das Aufkommen neuer Informations- und Kommunikationstechnologien, Fortschritte in der Robotik, Entwicklungen in der künstlichen Intelligenz, die Plattform-Ökonomie, das Internet der Dinge und neue Produktions- und Regelsysteme („Industrie 4.0“) –, deren unterschiedliche Auswirkungen auf Arbeitsmärkte, Bildungs- und Sozialpolitik in wesentlich differenzierter Form diskutiert werden müssen als es teilweise heute geschieht.

Der zweite Abschnitt des Artikels gibt einen kurzen Einblick in die aktuelle Forschung zu den Auswirkungen von Digitalisierung und Automatisierung auf den Arbeitsmarkt. Auch wenn die Untersuchung von technologischem Wandel auf sozio-ökonomische Arbeitsmarkt-Outcomes ein klassisches Thema in der Literatur ist, ist die Zahl der Arbeiten, die sich mit den Konsequenzen der Digitalisierung und Automatisierung im engeren Sinne befassen, noch recht überschaubar. Im dritten Abschnitt werden dann die sozial- und bildungspolitischen Implikationen dieser Veränderungsprozesse diskutiert. Auch wenn die realen Auswirkungen von Digitalisierung und Automatisierung auf den Arbeitsmärkten schwer vorherzusagen sind, werden bereits heute und mit zunehmender Intensität politische Debatten über die notwendigen Policy-Reaktionen geführt. Von daher sollte sich die vergleichende Policy-Forschung in diesem Bereich jetzt schon der Analyse dieser Debatten widmen.

### Klärung des Begriffs

Die Auswirkungen von technologischem Wandel im digitalen Zeitalter auf Wirtschaft, Politik und Gesellschaft sind vielfältig und multidimensional. Begriffe wie Digitalisierung, Automatisierung, „Industrie 4.0“, die Plattform- und „Sharing“-Ökonomie bezeichnen Teilespekte dieses umfassenden Veränderungsprozesses, ohne diesen in seiner Gesamtheit erfassen zu können. Die weiteren Ausführungen konzentrieren sich auf die durch Rationalisierung und Umorganisation von Arbeitsprozessen oder Umverteilung von Arbeit direkt bewirkten Effekte auf den Arbeitsmarkt.

Hierbei werden drei Aspekte des technologischen Wandels in den Vordergrund gestellt:

- (1) Die fortschreitende Entwicklung von Informations- und Kommunikationstechnologien (ICT), die durch die exponentielle Vergrößerung von Datenverarbeitungs- und -speicherkapazitäten („Big Data“) massive Auswirkungen auf die Organisation von Arbeitsprozessen haben wird;
- (2) neue Möglichkeiten zur Automatisierung von manuellen Fertigungsprozessen, die durch das Zusammenwirken von „Big Data“, künstlicher Intelligenz und dem Internet der Dinge entstehen; sowie

- (3) das Aufkommen der Plattform- oder „Sharing“-Ökonomie, die neue Formen projektorientierter und -zentrierter Zusammenarbeit ermöglicht (daher ist in diesem Kontext auch oft der Begriff der „Gig-Economy“ zu hören, der auf die Kurzfristigkeit der Arbeitsprojekte verweist).

Diese drei Aspekte technologischen Wandels schließen sich natürlich nicht gegenseitig aus, sondern verstärken sich wechselseitig. Auch sind die begrifflichen Abgrenzungen der einzelnen Dimensionen nicht immer eindeutig möglich. Wechselseitige Komplementaritäten bestehen beispielsweise zwischen „Big Data“ und künstlicher Intelligenz („Machine Learning“) sowie zwischen dem Aufkommen neuer Informations- und Kommunikationstechnologien (insbesondere den sozialen Medien) und der Plattform-Ökonomie. Diese funktionalen Komplementaritäten zwischen den unterschiedlichen Dimensionen sind – so könnte man argumentieren – ein wesentlicher Grund dafür, dass sich die aktuelle Phase technologischen Wandels qualitativ von früheren Phasen unterscheiden könnte, denn die Gleichzeitigkeit radikaler technologischer Veränderungen in verschiedenen Bereichen befördert selbst wiederum exponentiell verlaufende Wachstums- und Veränderungsprozesse.

Abgesehen von den Auswirkungen der digitalen Revolution auf den Arbeitsmarkt, um die es hier primär gehen soll, hat die Digitalisierung auch Konsequenzen für die Organisation und Erbringung von wohlfahrtsstaatlichen Dienstleistungen selbst. Es ist z. B. zu erwarten, dass die Digitalisierung von gesundheitsrelevanten Daten die Finanzierung und Erbringung von Gesundheitsdiensten verändern wird. Die Digitalisierung von Gesundheitsdaten ermöglicht dabei einerseits personalisierte Dienstleistungen und eine bessere Vernetzung zwischen Gesundheitsanbietern, kann aber andererseits dazu führen, dass Krankenversicherungen ihre Risikokalkulationen sehr viel stärker auf individuelle Risiken hin zuschneiden können und damit Diskussionen um risikoabhängige Versicherungsprämien befördert werden. Im Bildungsbereich wird das Schlagwort der Digitalisierung häufig mit der Einführung von neuen, technologiezentrierten Lehr- und Lernmitteln gleichgesetzt. Auch die Einführung neuer Lerninhalte – wie etwa die Vermittlung von Programmierkenntnissen im Rahmen des Schulunterrichts – wird diskutiert.

### **Theoretische Grundlagen: Überblick über den Stand der Forschung zu Auswirkungen von Digitalisierung und Automatisierung**

Die Auswirkungen der oben angesprochenen technologischen Veränderungsprozesse auf den Arbeitsmarkt sind ambivalent. In den öffentlichen Diskussionen zu diesen Themen dominieren häufig die pessimistischen Zukunftsszenarien, die den Wegfall einer großen Zahl von Arbeitsplätzen vorhersagen. Es gibt jedoch auch gute Gründe dafür anzunehmen, dass radikale technologische Veränderungen neue Beschäftigungspotenziale erschließen. Zwar hat die Verbreitung von neuen ICT und des Internets viele etablierte Branchen unter Druck gesetzt, gleichzeitig sind allerdings neue Beschäftigungspotenziale und gänzlich neue Berufs- und Beschäftigungskategorien (wie etwa Blogger oder You Tube „Influencer“) entstanden. Der Zugang zu vormals elitär geschlossenen Märkten für Musik, Film und Publizistik hat sich

geöffnet. In gleicher Weise hat das Aufkommen von Unternehmen der Plattform-Ökonomie (AirBnB für Übernachtungsmöglichkeiten, Uber und Lyft für Taxifahrten, aber auch Plattformen für generische, selbstständige Dienstleistungen wie TaskRabbit oder Amazons MTurk) einerseits vormals geschlossene Märkte geöffnet, andererseits auch zu einer Verbreitung von prekären Beschäftigungsverhältnissen und der Unterminierung von etablierten Formen der Arbeitsmarktregulierung beigetragen (Eichhorst et al. 2017).

In ähnlicher Weise hat die fortschreitende Automatisierung und Robotisierung der Arbeitswelt zunächst Beschäftigungspotenziale rationalisiert und eliminiert. Durch die zu erwartende fortschreitende Entwicklung von Künstlicher Intelligenz und „Machine Learning“ werden weitere, auch anspruchsvollere Tätigkeiten automatisierbar: Selbst-lernende Software-Algorithmen können zunehmend Routine-Tätigkeiten in sogenannten „White-Collar-Berufen“ übernehmen (z. B. Buchhaltung, Steuerberatung oder Prüfung von Rechtsfragen, vgl. Autor et al. 2003). Aus einer pessimistischen Perspektive betrachtet könnte radikaler technologischer Wandel somit zum Wegfall einer hohen Zahl von Arbeitsplätzen führen. Die optimistische Gegenperspektive hingegen besteht darin, dass der Wegfall von Routine-Tätigkeiten in Fertigungs- und einigen Dienstleistungsberufen insgesamt zu einer Verbesserung der Beschäftigungsbedingungen beitragen könnte, wenn tendenziell anspruchsvollere und qualitativ hochwertige Beschäftigungsmöglichkeiten übrig bleiben. Welche dieser beiden Perspektiven die zutreffendere ist, hängt maßgeblich davon ab, ob es gelingt, diejenigen, deren Arbeitsplatz durch technologisch bedingte Rationalisierung wegfällt, durch Weiterbildung und aktive Arbeitsmarktpolitik in die Lage zu versetzen, auch anderen Tätigkeiten nachzugehen.

Die aktuelle Forschung zu den Auswirkungen der digitalen Revolution auf den Arbeitsmarkt hat noch keine abschließende Antwort zu der Frage gefunden, wie umfassend die Veränderungen bereits sind oder in naher Zukunft sein werden. Die Forschung steht hierbei vor dem grundlegenden Problem, dass die gegenwärtigen Auswirkungen des mit der Digitalisierung einhergehenden technologischen Wandels auf den Arbeitsmarkt noch begrenzt sind, aufgrund der oben angesprochenen, sich selbst verstärkenden Dynamik aber in naher Zukunft durchaus dramatischere Dimensionen annehmen könnten. Daher kann die einschlägige Forschung in zwei Schwerpunkte unterteilt werden.

Zum einen sind dies Studien, die die Auswirkungen von technologischem Wandel und Internationalisierung (Globalisierung) auf Arbeitsmarkt-Outcomes wie Beschäftigung und Ungleichheit mit bereits erhobenen Daten retrospektiv für die Vergangenheit untersuchen. Aufbauend auf den grundlegenden Arbeiten von Autor et al. (2003) untersucht diese Forschungsrichtung, inwiefern technologischer Wandel zu einer Polarisierung von Beschäftigungsmöglichkeiten – und damit langfristig auch von Löhnen – beigetragen hat. Viele Studien (vgl. zum Beispiel Goos et al. 2014 für ein größeres Sample von OECD-Staaten) bestätigen die These von der zunehmenden Polarisierung von Arbeitsmarktstrukturen: Im Kern zeigen diese Arbeiten, dass technologischer Wandel nicht einfach zu einer Zunahme von Ungleichheit führt. Stattdessen kommt es zu einem „Aushöhlungsprozess“ der Mittelschichten: Nachdem einfache, Routine-basierte Tätigkeiten bereits in voran-

gehenden Wellen technologischer Rationalisierung weggefallen sind, seien nun anspruchsvollere Routine-Tätigkeiten in typischen Mittelklasse-Berufen am stärksten von technologischen Veränderungen betroffen. Relativ geschützt vor Veränderungen seien hoch anspruchsvolle, kreative und soziale Tätigkeiten am oberen Ende der Einkommens- und Bildungsskala sowie einfache, nicht-routinierbare Tätigkeiten am unteren Ende dieser Skalen, vor allen personenbezogene Dienstleistungen. Wenn es somit den Angehörigen der Mittelschicht nicht gelingt, anspruchsvolle Berufe am oberen Ende der Einkommens- und Bildungsskala zu erreichen, droht der relative Absturz in die unteren Einkommensschichten. Auch wenn die Evidenz für den Zusammenhang zwischen technologischem Wandel und Arbeitsmarktpolarisierung zunehmend robuster wird, laufen die Veränderungsprozesse, die in diesen Studien beschrieben werden, eher graduell ab und sind schwerlich mit den dramatischen Prognosen der Zukunftspessimisten in Einklang zu bringen, zumal viele OECD-Länder gegenwärtig historisch niedrige Arbeitslosenraten aufweisen.

Daher befasst sich eine zweite Gruppe von Studien mit den *zukünftigen* Auswirkungen von technologischem Wandel. Besonders einflussreich in diesem Zusammenhang ist die Studie von Frey und Osborne (2017), die bereits einige Jahre zuvor als Arbeitspapier veröffentlicht wurde und für ein großes Medienecho sorgte. Die zentrale methodische und empirische Herausforderung für Studien dieser Art ist, dass aus offensichtlichen Gründen noch keine realen Arbeitsmarktdaten vorliegen. Frey und Osborne (2017) begegnen dieser Herausforderung, indem sie eine Gruppe von Technologie-Experten zu ihren Einschätzungen hinsichtlich des Automatisierungspotenzials verschiedener, ausgewählter Tätigkeiten und Berufe befragen und diese Daten verwenden, um mit Hilfe von statistischen Methoden eine Einschätzung hinsichtlich des Automatisierungspotenzials aller Berufe abgeben zu können. Laut ihrer Schätzung sind 47 Prozent aller Beschäftigungsverhältnisse in den USA in Berufen einem hohen Automatisierungsrisiko (über 70-prozentige Wahrscheinlichkeit der Automatisierung in den nächsten Jahren) ausgesetzt. Nach den Schätzungen von Frey und Osborne (2017) sind besonders auch Mittelklasse-Berufe mit stark ausgeprägtem Routine-Charakter von der Automatisierung betroffen (z. B. Berufe in den Bereichen Buchhaltung, Dateneingabe, Verwaltung und Bankdienstleistungen), während Berufe in den sozialen, persönlichen und kreativen Dienstleistungsbereichen einem geringen Automatisierungsrisiko ausgesetzt sind.

Die Studie von Frey und Osborne (2017) ist vielfach kritisiert worden und erkennt auch selbst einige Einschränkungen ihrer Methodik an. So sagt die Studie nichts darüber aus, inwiefern der Wegfall von Beschäftigung durch Digitalisierung und Automatisierung durch die Entstehung neuer Beschäftigungsformen kompensiert werden kann. Voraussagen hinsichtlich neuer Berufsfelder und Beschäftigungsformen sind naturgemäß noch schwieriger als Aussagen hinsichtlich des Automatisierungspotenzials bestehender Berufe. Des Weiteren ist technologischer Wandel keine rein exogene Größe, sondern kann durch politisches Handeln beschleunigt (z. B. durch öffentliche Investitionen in Forschung und Entwicklung) oder ausgebremst werden. Schließlich kann die Tatsache, dass Frey und Osborne (2017) Technologie-Experten befragten, dazu beigetragen haben, dass Automatisierungspotenziale systematisch überschätzt werden.

Eine weitere, eher methodische Kritik bezieht sich darauf, dass Frey und Osborne (2017) Automatisierungspotenziale auf Grundlage ganzer Berufe abschätzen und nicht einzelne Tätigkeiten („tasks“) betrachten. Eine konsequent „task-zentrierte“ Perspektive (Autor et al. 2003) hingegen zeigt, dass zwar einzelne Tätigkeiten ein hohes Automatisierungspotenzial aufweisen, dies aber nur bedingt einen Beruf (als „Bündel“ unterschiedlicher Tätigkeiten) als Ganzes betreffen muss. Die Automatisierung einzelner Tätigkeiten innerhalb eines Berufes würde dann zu einer Verschiebung der relativen Bedeutung dieser Tätigkeiten führen, aber nicht zwangsläufig den Beruf insgesamt eliminieren.

Studien, die eine konsequent „task-zentrierte“ Perspektive einnehmen, kommen zu deutlich niedrigeren Zahlen hinsichtlich der zu erwartenden Veränderungen auf dem Arbeitsmarkt. Bonin et al. (2015) übertragen den Ansatz von Frey und Osborne (2017) auf Deutschland und kommen bei gleicher Methodik auf eine ähnlich hohe Zahl (42 Prozent der Beschäftigungsverhältnisse in Berufen mit einer hohen Automatisierungswahrscheinlichkeit in den nächsten Jahren). Wenn man nun allerdings von einer Berufe- auf eine „task“-zentrierte Perspektive wechselt, schätzen Bonin et al. (2015), dass nur etwa 9 Prozent der Beschäftigungsverhältnisse einem hohen Automatisierungsrisiko ausgesetzt sind (12 Prozent für den Fall USA). Arntz et al. (2016) führen eine Analyse für ein größeres Sample von OECD-Staaten durch und kommen zu ähnlichen Zahlen: Im Durchschnitt von 21 OECD-Staaten seien 9 Prozent der Beschäftigungsverhältnisse einem hohen Automatisierungsrisiko ausgesetzt mit einer Spannweite von 6 Prozent in Korea bis hin zu 12 Prozent in Österreich.

Zusammenfassend kann somit festgehalten werden, dass bisher noch kein Konsens in der Literatur hinsichtlich der gegenwärtigen und in naher Zukunft zu erwartenden Auswirkungen der Digitalisierung und Automatisierung auf Arbeitsmärkte existiert. Es ist auch nicht zu erwarten, dass ein solcher Konsens kurzfristig erreichbar ist. Die unterschiedlichen Studien, die hier kurz vorgestellt wurden, nehmen unterschiedliche Analyseperspektiven ein, und die damit einhergehenden methodologischen Entscheidungen sind durchaus nachvollziehbar und haben ihre jeweilige Berechtigung. Trotz des fehlenden Konsenses hinsichtlich der Größe des Effekts (von „dramatisch“ bis „signifikant“) verbindet die hier vorgestellten Studien jedoch die Einsicht, dass technologischer Wandel sowohl in der Vergangenheit als auch in der Gegenwart in nicht-trivialer Weise Arbeitsmarktstrukturen und -prozesse beeinflusst.

### **Praktische Anwendungen und Implikationen für die Bildungs- und Sozialpolitik**

Eine weitere Gemeinsamkeit der im vorherigen Abschnitt vorgestellten Studien besteht darin, dass sie sich mit den direkten Auswirkungen von Digitalisierung und Automatisierung auf den Arbeitsmarkt befassen, nicht aber mit den sozial- und bildungspolitischen Folgen dieser Entwicklungen. Bislang gibt es nur eine Handvoll von Arbeiten, die sich diesem Thema widmen. Thewissen und Rueda (2019) beispielsweise untersuchen unter Verwendung der in der oben skizzierten ökonomischen Literatur entwickelten Maße und Indikatoren, inwiefern das individuelle Automatisierungsrisiko eines Berufs mit Unterstützung für staatliche Umver-

teilungsmaßnahmen einhergeht und finden einen positiven Zusammenhang. Eichhorst et al. (2017) beschäftigen sich mit den Auswirkungen der Prekarisierung von Beschäftigungsverhältnissen in der „Gig“- bzw. Plattform-Ökonomie auf Arbeitsmarktregulation.

Auch wenn detaillierte wissenschaftliche Untersuchungen zu den bildungs- und sozialpolitischen Reaktionen noch weitestgehend ausstehen, gibt es durchaus bereits Debatten über die relativen Vor- und Nachteile unterschiedlicher Policy-Lösungen. Eine erste und besonders naheliegende Policy-Empfehlung besteht darin, öffentliche und private Investitionen in Bildung auszuweiten und insbesondere berufliche Weiterbildung, lebenslanges Lernen und aktive Arbeitsmarktpolitik zu fördern (Colin and Palier 2015). Da hoch qualifizierte Berufe und Tätigkeiten vor den Auswirkungen der Digitalisierung und Automatisierung besser geschützt sind als Routinebasierte, einfache Tätigkeiten, könnten Investitionen in Bildung sowohl auf individueller als auch auf gesellschaftlicher Ebene einen effektiven Schutz gegen Rationalisierungsmaßnahmen darstellen.

Die Diskussion der Rolle der Bildungspolitik im Prozess der Digitalisierung hat unterschiedliche Ebenen. Zum einen geht es um die Verbesserung des Zugangs zu weiterführenden Bildungsmöglichkeiten für Berufstätige. Der Ausbau von finanzieller Unterstützung für individuelle Bildungsmaßnahmen, beispielsweise über Bildungsgutscheine oder Bildungskonten (wie im Mai 2017 von der ehemaligen Bundesarbeitsministerin Andrea Nahles vorgeschlagen), könnte Beschäftigte bei der Erschließung neuer Beschäftigungsoptionen unterstützen. Diese Maßnahmen könnten durch gesetzliche oder tarifvertragliche Regelungen zur Freistellung von Arbeitnehmer\*innen für kurzfristige und längere Weiterbildungsmaßnahmen („Sabbatical“ und „Recht auf Weiterbildung“) flankiert werden. So gibt es in Österreich schon seit längerem das Instrument der „Bildungskarenz“, das Arbeitnehmer\*innen erlaubt, mit finanzieller Absicherung durch die Arbeitslosenversicherung eine Weiterbildungsmaßnahme von bis zu einem Jahr umzusetzen.

Maßnahmen, die auf den Ausbau von Weiterbildung und lebenslangem Lernen abzielen, stellen eine naheliegende Antwort auf die Herausforderung der Digitalisierung dar, haben allerdings auch inhärente Grenzen. So hängt die Wirksamkeit von Weiterbildungsmaßnahmen letztlich davon ab, dass tatsächlich genügend neue Beschäftigungsoptionen in neuen Wirtschaftsbereichen entstehen, um rein quantitativ den Wegfall traditioneller Beschäftigung zu kompensieren. Um eine Zunahme von Arbeitsmarktstratifizierung zu vermeiden, müssten die neuen Beschäftigungsmöglichkeiten auch qualitativ gleich- oder höherwertiger sein. Und schließlich ist keineswegs garantiert, dass diejenigen, deren Arbeitsplatz der Rationalisierung zum Opfer fällt, die notwendigen grundlegenden kognitiven und sozialen Voraussetzungen mitbringen, um erfolgreich eine Weiterbildung zu absolvieren. Wenn Tätigkeiten und Berufe im Zeitalter der Digitalisierung immer anspruchsvoller werden, könnte es sein, dass ein gewisser und wachsender Teil der Arbeitnehmerschaft trotz Weiterbildung nicht in der Lage ist, diese Tätigkeiten auszuüben.

Auch aus diesem Grund – und dies ist die zweite Ebene der bildungspolitischen Diskussion – werden zunehmend grundlegende Reformen der Bildungssysteme selbst gefördert. Ein Aspekt in dieser Debatte ist der Einsatz von technologie-

basierten Lehr- und Lernmitteln, wobei es weiterhin empirisch umstritten ist, ob digitale Lehr- und Lernmethoden den traditionellen tatsächlich überlegen sind (Falck et al. 2018). Ein zweiter Aspekt betrifft die Reform von Lehrplänen und Lehrinhalten. In diesem Zusammenhang betont die Politik vor allen Dingen die Notwendigkeit der gezielten Förderung der sogenannten MINT-Fächer (Mathematik, Informatik, Naturwissenschaft und Technik). Der offensichtliche Zusammenhang zum Thema Digitalisierung besteht darin, dass erwartet wird, dass neue Beschäftigungspotenziale vor allen Dingen in den neuen Wirtschaftssektoren der digitalen Ökonomie entstehen. Daher – so die Erwartung – stellt eine frühzeitige Vorbereitung und Ausbildung der jüngeren Generationen durch den Ausbau der MINT-Fächer in Schulen und der Ausbildung eine besonders effektive Strategie zur Sicherung des Fachkräftennachwuchses dar. Auch wenn gegenwärtig ein Fachkräftemangel in Technik-basierten Berufen zu konstatieren ist, ist langfristig allerdings nur bedingt vorhersehbar, in welchen Bereichen der Ökonomie die größten Wachstumspotenziale bestehen. So zeichnet sich ebenfalls jetzt bereits ein Fachkräftemangel in den sozialen Dienstleistungs- und Pflegeberufen ab, die laut den oben zitierten Studien ebenfalls recht weitgehend vor Digitalisierung und Automatisierung geschützt sind, da sie auf sozialen und interpersonalen Fähigkeiten aufbauen. Gleichermaßen gilt für Tätigkeiten in der Kreativwirtschaft. Insofern ist abzuwarten, ob der Diskurs um die Neuausrichtung von Lehrplänen und Lehrinhalten mittelfristig auch stärker auf die Vermittlung von sozialen, kulturellen und kreativen Fertigkeiten hin ausgerichtet wird oder ob die Digitalisierungs-Diskussion einseitig die Förderung von MINT-Fächern privilegiert.

In den sozialpolitischen Diskussionen zu den Auswirkungen von Digitalisierung stehen arbeitsmarktpolitische Fragen im Vordergrund. Neben den oben bereits angesprochenen Vorschlägen zum Ausbau von Weiterbildung und lebenslangem Lernen geht es hierbei vor allen Dingen um die aktive Arbeitsmarktpolitik und – in weitergehenden Vorschlägen – die Einführung eines bedingungslosen Grundeinkommens. Unter den Begriff der aktiven Arbeitsmarktpolitik kann ein breites Maßnahmenbündel gefasst werden, das neben Weiterbildungsmaßnahmen auch die Subventionen von öffentlichen Beschäftigungsmaßnahmen umfasst. Auch Kombinationen unterschiedliche Instrumente sind denkbar, etwa wenn ein Grundeinkommen nur für einen begrenzten Zeitraum gewährt wird und diese Zeit für Weiterbildungsmaßnahmen genutzt werden kann („Bildungskarenz“). In eine ähnliche Richtung geht die Idee eines „Partizipation income“, die der Ökonom Tony Atkinson (Atkinson 2015) vorgeschlagen hat. Atkinsons Idee besteht darin, dass der Staat eine Art Grundeinkommen auszahlt, diese Auszahlung aber davon abhängig macht, dass die Nutznießer sich in irgendeiner Form – sei es durch soziales Engagement im Non-Profit-Sektor, Weiterbildung, regulärer oder subventionierter Beschäftigung – an der Gesellschaft beteiligen.

Im Gegensatz dazu lehnen weitergehende Vorschläge zur Einführung eines bedingungslosen Grundeinkommens (BGE) die Verknüpfung der Auszahlung des Grundeinkommens an Bedingungen grundsätzlich ab. Die Debatte zum BGE ist zu vielschichtig und komplex, um sie hier ausführlich darzustellen. Politisch interessant

ist allerdings die Tatsache, dass das BGE von sehr unterschiedlichen politischen Akteuren unterstützt wird: Konservative und Libertäre erhoffen sich vom BGE eine Überwindung der Abhängigkeit vom traditionellen Sozialstaat, da alle bestehenden Sozialleistungen durch ein universales Grundeinkommen ersetzt werden könnten. Linke wiederum verbinden mit der Einführung eines BGE das Ende der Kommodifizierung der Arbeitskraft. Letztlich unterscheiden sich die Konzepte vom BGE grundlegend darin, wie großzügig das BGE ausgestaltet werden soll, und ob es mit einer Abschaffung bestehender Sozialleistungen einhergehen soll oder ob viele der etablierten sozialstaatlichen Leistungen weiterhin bestehen bleiben. Die Debatte um die Einführung eines BGE hat im Kontext der Digitalisierungs-Diskussion neuen Auftrieb erhalten, da ein BGE Sorgen um Massenarbeitslosigkeit und prekäre Beschäftigung in der digitalen Ökonomie lindern würde. Kritiker des BGE befürchten, dass es zu einem allgemeinen Rückgang der Erwerbsbeteiligung und der Beschäftigungsfähigkeit der Arbeitnehmerschaft beitragen könnte und davon bestimmte, bereits jetzt benachteiligte Bevölkerungsgruppen wie Frauen und Migranten besonders betroffen wären (Colin und Palier 2015).

### Ausblick: Künftige Entwicklung

Dieses kurze Kapitel konnte nur einen skizzenhaften Einblick in die Diskussion zu den bildungs- und sozialpolitischen Folgewirkungen der Digitalisierung und Automatisierung geben. Ohne Zweifel besteht weiterhin großer Forschungsbedarf, insbesondere hinsichtlich der Policy-Reaktionen auf die sich abzeichnenden strukturellen Verschiebungen auf den Arbeitsmärkten. Ob die digitale Revolution langfristig Ungleichheits-verstärkende Auswirkungen oder durch die Schaffung von neuen Beschäftigungsmöglichkeiten und Beteiligungsformen eine egalisierende Wirkung hat, hängt maßgeblich von politischen Faktoren und Entscheidungen ab. Bildungs- und Sozialpolitik werden hier eine zentrale Rolle spielen, aber welche Policy-Lösungen sich letztlich durchsetzen werden, ist heute nur in Grundrisse erkennbar.

---

## Literatur

- Arntz, Melanie, Terry Gregory, und Ulrich Zierahn. 2016. The risk of automation for Jobs in OECD Countries. A comparative analysis. (OECD social, employment and migration Working Papers 189). Paris: OECD Publishing.
- Atkinson, Anthony B. 2015. *Inequality. What can be done?* Cambridge, MA: Harvard University Press.
- Autor, David H., Frank Levy, und Richard J. Murnane. 2003. The skill content of recent technological change. An empirical exploration. *The Quarterly Journal of Economics* 118(4): 1279–1333.
- Bonin, Holger, Terry Gregory, und Ulrich Zierahn. 2015. *Übertragung der Studie von Frey/Osborne (2013) auf Deutschland, Kurzexpertise Nr. 57.* Mannheim: Zentrum für Europäische Wirtschaftsforschung.
- Colin, Nicolas, und Bruno Palier. 2015. The next safety net social policy for a digital age. *Foreign Affairs* 94(4): 29–33.

- Eichhorst, Werner, Holger Hinte, Ulf Rinne, und Verena Tobsch. 2017. How big is the gig? Assessing the preliminary evidence on the effects of digitalization on the labor market. *Management Revue* 28(3): 298–318.
- Falck, Oliver, Constantin Mang, und Ludger Woessmann. 2018. Virtually no effect? Different uses of classroom computers and their effect on student achievement. *Oxford Bulletin of Economics and Statistics* 80(1): 1–38.
- Frey, Carl Benedikt, und Osborne, Michael A. 2017. The future of employment. How susceptible are jobs to computerisation? *Technological Forecasting and Social Change* 114(Issue C): 254–280.
- Goos, Maarten, Alan Manning, und Anna Salomons. 2014. Explaining Job polarization: Routine-based technological change and offshoring. *American Economic Review* 104(8): 2509–2526.
- Thewissen, Stefan, und David Rueda. 2019. Automation and the welfare State. Technological change as a determinant of redistribution preferences. *Comparative Political Studies* 52(2): 171–208.



---

# Digitalisierung von Schule, Schulverwaltung und Schulaufsicht

Sigrid Hartong, Andreas Breiter, Juliane Jarke und Annina Förschler

## Inhalt

1 Klärung der Begriffe .....	486
2 Konzeptionelle Grundlagen .....	488
3 Praktische Anwendungsfelder .....	488
4 Umsetzungsstand und Auswirkungen .....	489
5 Perspektiven für Staat und Verwaltung .....	492
Literatur .....	493

---

## Zusammenfassung

Im Bildungsbereich haben Prozesse der *Datafizierung* und *Digitalisierung* zu einem nachhaltigen Wandel von Staat und Verwaltung geführt, der sich in der zunehmenden Bedeutung komplexer Informationssysteme und zentralisierter Infrastrukturen des Datenmanagements sowie in der wachsenden Nutzung von Daten für Zwecke des Bildungsmonitorings zeigt. Trotz dieses allgemeinen Trends finden sich gerade im deutschen bildungsföderalen Kontext ohne originäre Zuständigkeit des Bundes gravierende Unterschiede zwischen den Bundesländern. Gleichzeitig mangelt es nach wie vor an Transparenz, Partizipationsmöglichkeiten sowie Kompetenzen im Umgang mit Daten (*Data Literacy*).

---

S. Hartong (✉) · A. Förschler

Fakultät für Geistes- und Sozialwissenschaften, Helmut Schmidt Universität, Hamburg,  
Deutschland

E-Mail: [hartongs@hsu-hh.de](mailto:hartongs@hsu-hh.de); [foerschler.annina@hsu-hh.de](mailto:foerschler.annina@hsu-hh.de)

A. Breiter

Universität Bremen und Institut für Informationsmanagement Bremen, Bremen, Deutschland  
E-Mail: [abreiter@ifib.de](mailto:abreiter@ifib.de)

J. Jarke

ifib: Institut für Informationsmanagement Bremen GmbH, Universität Bremen, Bremen,  
Deutschland  
E-Mail: [jjarke@ifib.de](mailto:jjarke@ifib.de)

## Schlüsselwörter

Schulverwaltung · Schulaufsicht · Datenbasierte Schulsteuerung · Schulinformationssysteme · Datafizierung · Critical Data Studies · Educational Governance · Data Literacy

## 1 Klärung der Begriffe

Folgende ausgewählte Kernbegriffe lassen sich für die Digitalisierung im Themenbereich Schule, Schulverwaltung und -aufsicht als besonders bedeutsam identifizieren:

**Datafizierung:** Wenngleich Daten (etwa Statistiken oder Schulnoten) schon immer Teil von Schule und Schulverwaltung gewesen sind, so wurden sie in Deutschland unter dem Schlagwort *datenbasierte Schulsteuerung* seit Ende der 1990er-Jahre zu einem bildungspolitischen Mantra, bei dem die systematische(re) Definition, Erhebung, Verarbeitung und Visualisierung von insbesondere digitalen Bildungsdaten ins Zentrum gerückt wurde. Mit ihrem Konstanzer Beschluss aus dem Jahr 1997 stärkte die Kultusministerkonferenz (KMK) diese *empirische Wende* mit einem stärkeren Fokus auf outputorientierte Bildungssteuerung und damit auf Datenerhebung und -nutzung. Diese betraf Verwaltungs- und Leistungsdaten gleichermaßen, wobei es in Deutschland bis zur Teilnahme an den internationalen Schulleistungsuntersuchungen *Programme for International Student Assessment* (PISA) und *Trends in International Mathematics and Science Study* (TIMSS) weder national noch international Leistungsdatenerhebungen gegeben hatte, die nun wiederum im Eilverfahren implementiert wurden. Im Fokus der staatlichen Schulverwaltung stehen seitdem eine im nationalen und internationalen Vergleich verortete Unterrichts- und Schulentwicklung sowie eine datenbasierte Qualitätssicherung. Hierfür sind die digitale Datenverarbeitung und damit Prozesse der *Quantifizierung* im Sinne einer Überführung qualitativ-komplexer Phänomene in vergleichbare Zahlenwerte zentral. Gleichzeitig ist auch die Veränderung der Beschaffenheit algorithmischer Verfahrensvorschriften sowohl bei Produktions- als auch bei Verarbeitungsprozessen von Daten eine wichtige Komponente von Datafizierung, etwa wenn Prozesse zunehmend automatisiert ablaufen und immer größere Datenmengen – *Big Data* – verarbeiten.

**Digitalisierung:** Ursprünglich wurde der Begriff genutzt, um den technischen Prozess der Konvertierung analoger Informationen in diskrete, digitale Dateneinheiten zu beschreiben. Mittlerweile wird Digitalisierung zunehmend als Phänomen verstanden, das sich durch tief greifende und vielfältige gesellschaftliche Transformationsprozesse auszeichnet und dabei die wachsende Automatisierung, Vernetzung oder den Einfluss künstlicher Intelligenz gleichermaßen umfasst. Im Bereich Schule, Schulverwaltung und Schulaufsicht lässt sich beispielsweise eine wachsende Digitalisierung von Kernprozessen wie SchülerInnenverwaltung, Stunden-/Vertretungsplanung, Kurs- und Notenverwaltung, Klassenbuchführung, Ressourcenmanagement oder Leistungsdatenverwaltung feststellen, bei der die grundlegende Verschiebung und

digitale Verdichtung von Sichtbarkeit (etwa die Integration von Leistungs- mit Verhaltens- oder Anwesenheitsdaten einzelner SchülerInnen) mitunter tief greifende Veränderungen in den Rollen und Beziehungen von schulischen Akteuren impliziert. Mit der Digitalisierung verstärkt sich gleichzeitig die Datafizierung des Schulsystems noch einmal gravierend, indem bei fast allen Bildungsprozessen digitale Daten gesammelt werden, die gleichermaßen Entscheidungs- und Meinungsbildungsprozesse der Schulpolitik, der Schulaufsicht, der Schulträger und Schulleitungen, der Lehrkräfte, der SchülerInnen und ihrer Eltern sowie der Öffentlichkeit beeinflussen.

*E-Government:* Die dargelegten Entwicklungen indizieren eine sukzessive Umstellung auf sogenanntes E-Government, wie es auch zunehmend in anderen gesellschaftlichen Bereichen angestrebt wird. Gleichzeitig stellt sich die erfolgreiche Implementation eines solchen, oftmals mit *Standardisierung* und *Zentralisierung* einhergehenden Steuerungsmodells im deutschen Bildungssektor als besonders herausfordernd dar, der vielmehr durch eine gesetzliche Trennung in innere (Zuständigkeit der Bundesländer) und äußere (Zuständigkeit der Kommunen) Schulangelegenheiten gekennzeichnet ist (siehe Abschn. 4). Zu den äußeren Schulangelegenheiten gehören dabei beispielsweise Errichtung und infrastrukturelle Unterhaltung der Schulgebäude und -ausstattung; zu den inneren Schulangelegenheiten hingegen beispielsweise die Verantwortung für das Lehrpersonal oder die Lehrplanentwicklung.

Der Begriff des E-Governments wird hier abgegrenzt vom sogenannten *E-Learning* beziehungsweise von Digitalisierungsphänomenen, die insbesondere pädagogischen Fragestellungen betreffen. In diesem Sinne nehmen die im Folgenden dargestellten Befunde zwar die Schul- und Unterrichtsebene insofern in den Blick, dass beispielsweise über die Nutzung digitaler Unterrichtsmedien, Lernmanagementsysteme und dergleichen schneller und direkter Daten für Schulverwaltungs- und Schulaufsichtszwecke produziert werden. Über die pädagogischen Implikationen soll und kann hierbei jedoch noch keine Aussage getroffen werden (siehe dazu Hartong 2019).

*Dateninfrastrukturen:* Dateninfrastrukturen bilden auch im Bildungswesen das Rückgrat der Datenverarbeitung und sind als eine Kombination aus Akteuren, Technologien und Policies zu verstehen beziehungsweise als Arrangements von materiellen/technischen, semiotischen und sozialen Relationen und Praktiken (vgl. Star und Ruhleder 1996; Sellar 2015). Technologisch basieren sie zumeist auf vernetzten Datenbanksystemen, die von unterschiedlichen Akteuren geplant und organisiert werden und in denen Normen, Werte und Strategien verdinglicht sind. Sie sind eingebettet in und Teil von Informationssystemen.

*Schulinformationssysteme:* Im Bereich der Digitalisierung von Schule, Schulverwaltung und Schulaufsicht spielen Schulinformationssysteme eine zentrale Rolle (vgl. Breiter et al. 2008). Sie werden sowohl innerhalb der Verwaltungsebene von Einzelschulen, als auch innerhalb von übergeordneten Behörden der staatlichen Schulaufsicht und -verwaltung eingesetzt und dienen meist als Datenschnittstelle zwischen verschiedenen Organisationseinheiten. In Deutschland befindet sich eine Vielzahl unterschiedlicher Schulinformationssysteme in der Entwicklung und im Einsatz.

## 2 Konzeptionelle Grundlagen

Sowohl national als auch international befassen sich die Sozial- und Erziehungswissenschaften seit Längerem mit der wachsenden Bedeutung sozialer Vermessungspraktiken, Datafizierung und der Rolle von Algorithmen, die in zunehmendem Maße auch den Bildungskontext und dabei sämtliche Ebenen des Schulsystems betreffen. Hierbei wird die Transformation einer wachsenden Expansion und Intensivierung von Dateninfrastrukturen als durchaus ambivalent beurteilt, nämlich zwischen größerer Transparenz und neuen (effektiveren) Steuerungsmöglichkeiten der Schulverwaltung auf der einen und größerer Kontrolle und Überwachung der Schulakteure auf der anderen Seite.

Als eine besondere Forschungsperspektive im deutschsprachigen Raum, die insbesondere auf die Komplexität von (sich wandelnden) Interdependenzstrukturen zwischen Akteuren unterschiedlicher Ebenen des Schulsystems (auch) durch Datafizierung abzielt, kann das Konzept der *Educational Governance* bezeichnet werden (Überblick bei Altrichter et al. 2007 oder bei Maag Merki et al. 2014). Diese Art Forschung hat Daten bislang vor allem unter der Fragestellung thematisiert, wie diese effektiver bzw. effizienter produziert, gesammelt, aufbereitet, vermittelt und ebenenübergreifend genutzt werden können, und dabei einen gewissen *what works*-Fokus eingenommen. Wenngleich also Daten(infrastrukturen) und die Frage ihrer Nutzung für Bildungspolitik, Forschung und Schule zunehmend diskutiert und empirisch untersucht werden, so steht die gezielte Grundlagenforschung zu digitalisierten Formierungen dieser Daten im deutschsprachigen Raum noch am Anfang. Hierbei geht es beispielsweise auch darum, wie in die Produktion und Verwendung von Daten bereits Vorstellungen von *guter Bildung*, aber auch bestimmte Rollen- (-beziehungen) oder Wahrnehmungen eingeschrieben werden. Derartige Perspektiven auf Datafizierung als wirkmächtige Praktiken sind bislang eher im anglo-amerikanischen Raum entwickelt worden, etwa unter dem Schlagwort *Critical Data Studies* (Überblick bei Iliadis und Russo 2016). Die Frage, wie Daten nicht nur soziale Wirklichkeit beschreiben, sondern auch selektive Wirklichkeit erschaffen oder verändern, wird hierbei zunehmend in den Fokus gerückt (vgl. Williamson 2017). So führt beispielsweise die Festlegung bestimmter Indikatoren zur datenbasierten Evaluation schulischer Qualität dazu, dass diese Indikatoren zunehmend ins Zentrum der Wahrnehmung rücken und damit die Komplexität von *guter Schule* tendenziell auf ein gutes Abschneiden bei diesen Indikatoren reduziert wird. Mit anderen Worten konstituieren Dateninfrastrukturen immer auch Reflexionspotenziale (etwa induzierte Selbst- und Fremdbeschreibungen), Einflusschancen, Ontologien, Sichtbarkeiten oder Machtdynamiken sowie spezifische Möglichkeitsräume der Problemlösung und Handlungskoordination.

## 3 Praktische Anwendungsfelder

Bei der Betrachtung der staatlichen Bildungsverwaltung muss zwischen den Aktivitäten der Bundesländer und der Kommunen sowie gemeinsamen Prozessen auf Bundesebene – in der Regel koordiniert über die Kultusministerkonferenz (KMK)

– unterschieden werden. Die Kommunen haben gemäß ihrer Zuständigkeit für äußere Schulangelegenheiten primär ein Interesse an Daten, die für die Bereitstellung und Instandhaltung der schulischen Infrastruktur notwendig sind. SchülerInnenzahlen und ihre Zuordnung zu Klassen sind wiederum relevant, weil sie die Basis für den kommunalen Schulentwicklungsplan darstellen, der turnusgemäß erstellt wird. Aus Sicht der Länder und der Aufsichtsbehörden sind aufgrund ihrer Zuständigkeit für innere Schulangelegenheiten die pädagogischen Kennzahlen, darunter Daten aus Schulleistungsmessungen oder Leistungstests sowie Daten über Beschäftigung, Unterrichtsversorgung und so weiter von Bedeutung. Hinzu kommt als dritte Akteurin die Schule selbst, die Informationssysteme für Notenverwaltung, Anwesenheit, Stundenplan, Vertretungsunterricht, Raumbuchung, Elternadressen und dergleichen benötigt und über Lernplattformen die Kommunikation zwischen Lehrkräften und ihren SchülerInnen organisiert. Schulen nutzen Mediendienste, die wiederum von Kommunen oder dem Land zur Verfügung gestellt werden, sie sind verknüpft mit Verzeichnisdiensten, in denen die Rollen und Rechte der NutzerInnen zentral vorgehalten werden. Auf Ebene der Länder und des Bundes lassen sich schließlich durch Statistikgesetze geregelte Schul-Controlling-Systeme identifizieren, für die Datenlieferungen erforderlich sind und mit denen Datenanalysen beispielsweise für Bildungsberichte oder im Rahmen internationaler Vergleichsstudien erfolgen. Insgesamt handelt es sich also um komplexe Schulinformationssysteme, die je nach Ausbaustand vertikal und/oder horizontal integriert sind. Hierbei lassen sich Systeme der Makro-, Meso- und Mikroebene unterscheiden, wobei diese Ebenen nicht deckungsgleich sind mit den politischen Ebenen (etwa Bund, Land, Kommune). Vielmehr werden die Systeme in den Bundesländern jeweils unterschiedlich eingesetzt beziehungsweise zugeordnet (Abb. 1).

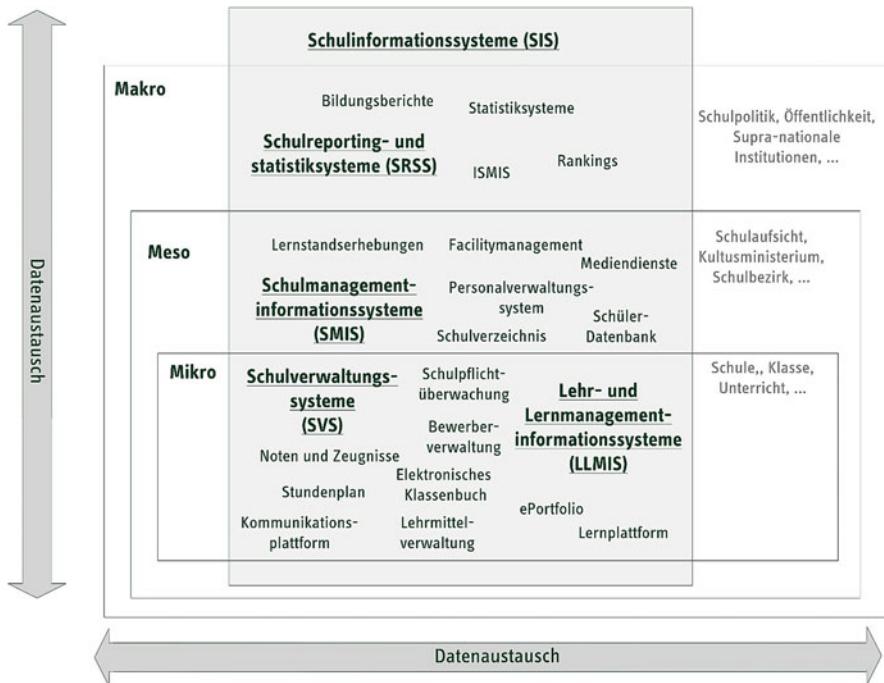
---

## 4 Umsetzungsstand und Auswirkungen

Für die wachsende Datafizierung und Digitalisierung von Schule, Schulverwaltung und Schulaufsicht sind in Deutschland seit Anfang des 21. Jahrhunderts die folgenden Entwicklungen und Beschlüsse zentral:

*Statistischer Minimalkatalog:* Im Jahr 2000 verabschiedete die KMK den sogenannten Statistischen Minimalkatalog. Dieser beinhaltet Vorgaben zur einheitlichen Erhebung spezifischer Merkmale durch die staatliche Schulverwaltung, um eine Vergleichbarkeit der erhobenen schulstatistischen Daten für nationale und internationale Statistiken in den Bundesländern zu forcieren. Die Länder bekundeten im Zuge dieses KMK-Beschlusses die Absicht, die im Minimalkatalog festgelegten Merkmale (Angaben zu Schulen, Klassen, SchülerInnen und Lehrkräften) jährlich zu erheben und an die KMK zu übermitteln (vgl. [www.kmk.org/dokumentation-statistik.html](http://www.kmk.org/dokumentation-statistik.html)).

*Kerndatensatz:* Mit der Verabschiedung des Kerndatensatzes durch die KMK wurden im Jahr 2003 die Anforderungen des Statistischen Minimalkatalogs um weitere Merkmale (wie beispielsweise Migrationshintergrund) ergänzt. Des Weiteren ist darin die Umstellung auf die Erhebung von Individualdaten anstelle von



**Abb. 1** Typische Funktionen digitaler Schulverwaltung über die Nutzung von Schulinformationssystemen. (Quelle: Breiter und Lange 2019)

aggregierten Daten vorgesehen. Begründet wurde dieser weitreichende Beschluss mit gestiegenen Ansprüchen an moderne länderübergreifende Bildungsstatistik, mit größerer Auswertungsflexibilität bei der Nutzung anonymisierter Einzeldaten im Vergleich zu aggregierten Daten sowie mit bisher nicht erfüllbaren internationalen Datenanforderungen, also Informationslücken bezüglich nationaler und internationaler Fragestellungen.

Mit diesen beiden Beschlüssen der KMK wurden die Länder zum ersten Mal in der bundesdeutschen Geschichte dazu aufgefordert, eine definierte Zahl an national standardisierten, zum Teil individualisierten Daten zu erheben und zurückzumelden. Jedoch ist die Umsetzung des Kerndatensatzes für die Bundesländer (bisher) nicht verpflichtend. Ursprünglich sollte die Umstellung auf Individualdaten bis 2006 in allen Ländern stattgefunden haben – bis heute ist der Kerndatensatz nicht flächendeckend oder in gleichem Umfang in den Bundesländern implementiert. Dies resultiert unter anderem aus technischen, finanziellen oder personellen Gründen, datenschutzrechtlichen Bedenken, den föderalen Strukturen sowie unterschiedlichen Softwareprogrammen in den Ländern. Dennoch sollten die langfristigen Wirkungen des Kerndatensatzes nicht unterschätzt werden.

*Strategie Nationales Bildungsmonitoring:* Zentral für die neue Form der an Ergebnissen orientierten Steuerung des Bildungswesens ist vor allem die 2006 verabschiedete und 2016 zuletzt aktualisierte Gesamtstrategie der KMK zum Bil-

dungsmonitoring. In dieser sind Instrumente und Testverfahren zusammengefasst, die der neuen Steuerungsphilosophie im Sinne evidenzbasierter Bildungspolitik entsprechen. Sie setzen sich zusammen aus der regelmäßigen Teilnahme an internationalen Schulleistungsstudien, der Entwicklung von Bildungsstandards seit 2003, deren Überprüfung in testbasierten Vergleichsarbeiten (VERA) auf Länderebene sowie einer Mehrebenen-Bildungsberichterstattung in Zusammenarbeit mit dem Bund. Trotz dieses massiven Ausbaus verpflichtender Datenerhebungen und -berichterstattung werden in Deutschland individuelle Testdaten bislang umfassend geschützt und es besteht die politische Absicht, Konsequenzen auf Basis disaggregierter Leistungsdaten (im Sinne von High-Stakes-Praktiken) auch weiterhin systematisch zu verhindern.

*Implementierung und Wandel des Datentransfers zwischen Schulen, Schulverwaltung und Schulaufsicht:* In dieser Gemengelage lassen sich auf der Ebene der Länder zwei grundsätzliche Ansätze zur Implementierung oder Transformation von Schulinformationssystemen (hier selektiv dargestellt für die allgemeinbildenden Schulen) unterscheiden: *Zentrale* versus *dezentrale* Lösungen. Während die eine Gruppe in einem aufwendigen Prozess die Bedarfe aller Schulen und Aufsichtsbehörden erfasst, modelliert und dann in einem betrieblichen Informationssystem implementiert bzw. ein solches bei einem externen Anbieter einkauft, überlässt die zweite Gruppe die Datenerfassung und Speicherung den Schulen und fordert regelmäßig Datenberichte an, um die zentrale Statistik zu bedienen. Insgesamt lässt sich beobachten, dass die erste Gruppe, welche zentrale Lösungen entwickelt, in den letzten Jahren kontinuierlich gewachsen ist und sich dieser Trend fortzusetzen scheint, wobei einige Bundesländer jedoch eine Art Zwischenweg gehen, bei dem die Nutzung der zentralen Lösung für die Schulen explizit freiwillig ist. Die zentrale Einführung einer Schulverwaltungssoftware verspielte die Vorteile einer Standardisierung jedoch oftmals dann, wenn die Funktionen nicht den schulischen Bedarfen entsprachen und parallele Systeme aufgebaut wurden (Tab. 1).

*Die Etablierung eigenständiger Monitoringinstitute zum Ausbau und zur Koordination von Dateninfrastrukturen:* Neben der Transformation von Schulinformationssystemen lässt sich über die Länder hinweg ein systematischer Ausbau institutioneller Strukturen für die Durchführung und Auswertung von Bildungsmonitoring beziehungsweise für die datenbasierte schulische Qualitätssicherung erkennen. In wenigen Bundesländern wurden hierfür eigenständige Landesinstitute geschaffen (etwa das *Institut für Bildungsmonitoring und Qualitätsentwicklung* in Hamburg), in anderen Bundesländern wurden entsprechende Strukturen innerhalb der Landesbehörde oder dem Ministerium realisiert. Innerhalb dieser Institute oder Strukturen finden sich mittlerweile eigene Dateninfrastrukturen, die gleichzeitig durch die institutionelle Tätigkeit weiter ausdifferenziert oder aber verdichtet werden, indem beispielsweise zentralisierte Datenbanken geschaffen oder Datenauswertungen verknüpft werden. Landesspezifisch unterschiedlich ist dann wiederum das Verhältnis der Dateninfrastrukturen zwischen diesen Institutionen und den zum Beispiel statistischen Datensammlungen und -auswertungen der (anderen Strukturen innerhalb der) Behörden oder Ministerien, was beispielsweise Datentransfer und -zugriff betrifft.

**Tab. 1** Schulinformationssysteme der Bundesländer im Vergleich. Stand Juni 2018.

Zentrale Lösung, obligatorisch für alle allgemeinbildenden Schulen	Zentrale Lösung (nicht obligatorisch, daher neben alternativen Anbietern)	Dezentrale Lösung, teilweise jedoch zentrale Lösung geplant
Bayern (edoo.sys)	Baden-Württemberg (edoo.sys)	Mecklenburg-Vorpommern
Berlin (LUSD, Kooperation mit Hessen, Implementation bis Ende 2018)	Niedersachsen (DaNis)	Schleswig-Holstein (Kooperation mit Hamburg geplant)
Brandenburg (weBBSchule)	Nordrhein-Westfalen (SchILD)	Saarland
Bremen (Eigenentwicklung)		Sachsen-Anhalt (Ausschreibung erfolgt: Softwareentwicklung ab Februar 2019 geplant)
Hessen (LUSD)		Thüringen
Sachsen (SaxSVS)		Rheinland-Pfalz (Modellschulen mit edoo.sys, jedoch neue Ausschreibung laufend)
Hamburg (DiVis)		

*Probleme beim Umstellen auf E-Government:* Zentral für ein funktionierendes E-Government im deutschen Bildungssektor wäre eine stärkere Harmonisierung zwischen den deutschen Bundesländern in Sachen Nutzung und Ausweitung von digitalen Dateninfrastrukturen. Gerade diese stellt sich wegen der föderalen Kompetenzverteilung sowie der Trennung in äußere und innere Schulangelegenheiten als besonders schwierig dar. In anderen Verwaltungsbereichen (der Kernverwaltung) ist dies anders, da hier etwa über die Aktivitäten des *IT-Planungsrates* harmonisierte E-Government-Initiativen vorangebracht und durch Regelungen sowohl auf Bundes- und Länderebene als auch zwischen Bund und Ländern gefestigt wurden, die bislang eher getrennt agierten. Hierzu wurde sogar eigens ein neuer Artikel in das Grundgesetz eingefügt (Artikel 91c GG), der eine enge Kooperation zwischen Bund und Ländern in der Verwaltungsorganisation ermöglicht beziehungsweise fordert. Im Gegensatz hierzu stehen die jeweiligen Bildungsverwaltungen der Länder (innere Schulangelegenheiten) sowie der Kommunen (äußere Schulangelegenheiten) also weiterhin vor der Herausforderung, jeweils eigene E-Government-Lösungen zu entwickeln oder aber den teuren Prozess so lange wie möglich heraus zu zögern – beide Varianten lassen sich finden.

## 5 Perspektiven für Staat und Verwaltung

In Zukunft wird die Erwartung der Gesellschaft und vor allem der Eltern an Bildungsinstitutionen und damit auch an eine offene Kommunikation schulischer Daten weiter steigen. Vor allem Eltern werden zunehmend einfordern, im Sinne der

Transparenz- beziehungsweise Informationsfreiheitsgesetze der Länder auf Schulinformationssysteme zugreifen zu können, wie es bereits heute nicht nur in angelsächsischen Ländern (USA, Großbritannien oder Australien) zu weiten Teilen selbstverständlich ist. Gleichermaßen wird die datenbasierte Schulsteuerung in allen Bundesländern an Dynamik gewinnen – Anzeichen hierfür ist die besagte Gründung von Instituten für Bildungsqualität und Monitoring, die wiederum auf betriebliche Informationssysteme und Dateninfrastrukturen angewiesen sind bzw. systematisch deren Ausbau vorantreiben. Was dies für die technische und organisatorische Umsetzung dieser Systeme und Dateninfrastrukturen über die Ländergrenzen hinweg bedeutet, kann derzeit noch nicht abgeschätzt werden. Offen ist außerdem, wie sich durch die Verfügbarkeit von Daten aller Art die Vorstellungen von und die Erwartungen an Schule, Lehrkräfte und Schulaufsicht verändern. Diesbezüglich wird eine Bewertung von Schulen mit Hilfe von Datenvergleichs-Plattformen an Bedeutung gewinnen. Hier sind Großbritannien, die USA und Kanada aber auch Australien oder die Niederlande bereits weiter fortgeschritten und damit auch die Bedeutung von Rankings; erste Anzeichen sind aber auch im deutschen Kontext zu erkennen (siehe z. B. die Plattformen [www.jedeschule.de](http://www.jedeschule.de) oder [www.schulen-vergleich.de](http://www.schulen-vergleich.de)). Je stärker die Vermessung sämtlicher Leistungen einer Schule auf Basis verschiedener Metriken dabei voranschreitet, desto wichtiger werden Daten, ihre Qualität und damit auch deren Verarbeitung in qualitätsgesicherten Informationssystemen. Dies bedeutet auch, dass die Anforderungen an die Datenkompetenz (*Data Literacy*, vgl. Mandinach und Gummer 2013) aller Akteure im Schulsystem steigen werden, welche nicht nur ein Bewusstsein für die Produktions- und Selektionsprozesse von (digitalen) Daten und Informationssystemen umfassen, sondern ebenso einen produktiven und selbstbestimmten Umgang mit den selbigen ermöglichen muss. Ziel muss mit anderen Worten sein, nicht nur eine Partizipation in, sondern auch eine kritische Auseinandersetzung mit Datafizierung und Digitalisierung zu ermöglichen.

---

## Literatur

- Altrichter, Herbert, Brüsemeister Thomas, und Jochen Wissinger, Hrsg. 2007. *Educational Governance. Handlungskoordination und Steuerung im Bildungssystem*. Wiesbaden: Springer.
- Breiter, Andreas, und Angelina Lange. 2019. Die digitale Schulverwaltung. In *Handbuch Digitale Verwaltung*, Hrsg. Sabine Smentek, Roland Jabkowski und Henning Lühr. Wiesbaden: KSV Kommunal- und Schul-Verlag.
- Breiter, Andreas, Angelina Lange, und Emese Stauke, Hrsg. 2008. *School Information Systems and Data-based Decision-Making. Schulinformationssysteme und datengestützte Entscheidungsprozesse*. Frankfurt a. M.: Peter Lang.
- Hartong, Sigrid. 2019. Bildung 4.0? Kritische Überlegungen zur Digitalisierung von Bildung als erziehungswissenschaftliches Forschungsfeld. *Zeitschrift für Pädagogik* 65(3): 424–444.
- Iliadis, Andrew, und Federica Russo. 2016. Critical data studies. An introduction. *Big Data & Society* 3(2): 1–7.
- Maag Merki, Katharina, Roman Langer, und Herbert Altrichter, Hrsg. 2014. *Educational Governance als Forschungsperspektive. Strategien. Methoden. Ansätze*. Wiesbaden: Springer.
- Mandinach, Ellen B., und Edith S. Gummer. 2013. A systemic view of implementing data literacy in educator preparation. *Educational Researcher* 42(1): 30–37.

- 
- Sellar, Sam. 2015. Data infrastructure. A review of expanding accountability systems and large-scale assessments in education. *Discourse: Studies in the Cultural Politics of Education* 36(5): 765–777.
- Star, Susan L., und Karen Ruhleder. 1996. Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information Systems Research* 7(1): 111–134.
- Williamson, Ben. 2017. *Big data in education. The digital future of learning, policy and practice*. Los Angeles: Sage.



---

# Digitalisierung im Gesundheitssektor

Moritz E. Behm und Tanja Klenk

## Inhalt

1 Einleitung .....	496
2 Begriffsklärung .....	497
3 Theorie: Institutioneller Rahmen und Akteurskonstellationen .....	498
4 Praktische Anwendungsfelder .....	500
5 Umsetzungsstand und Auswirkungen .....	502
6 Perspektiven für Staat und Verwaltung .....	505
Literatur .....	506

---

## Zusammenfassung

Deutschland liegt bei der Digitalisierung des Gesundheitssektors weit hinter vergleichbar entwickelten Sozialstaaten zurück. Die Verantwortung für die Digitalisierung des Gesundheitssektors liegt maßgeblich bei den Leistungserbringern und Krankenkassen, die aufgrund ihrer Selbstverwaltungsrechte hier eine besondere Autonomie genießen. Zwischen Leistungserbringern, Krankenkassen und Patienten bestehen starke Interessenkonflikte, die durch die Ökonomisierung des Gesundheitssektors in den vergangenen Jahren weiter an Schärfe gewonnen haben. Die institutionelle Ausgestaltung des Selbstverwaltungsregimes gibt jedoch nur wenige Anreize, diese Interessenkonflikte zu lösen. Insbesondere Verteilungsfragen (z. B. die Finanzierung von Investitionen und die Vergütung von digitalen Gesundheitsangeboten) und Koordinationsfragen (z. B. die Sicherstellung von Interoperabilität) können nur bedingt im Rahmen von Selbstverwaltung gelöst werden und bedürfen staatlich-hierarchischer Intervention.

---

M. E. Behm (✉) · T. Klenk

Fakultät für Wirtschafts- und Sozialwissenschaften, Helmut-Schmidt-Universität, Hamburg, Deutschland

E-Mail: [mail@moritzbehm.de](mailto:mail@moritzbehm.de); [tanja.klenk@hsu-hh.de](mailto:tanja.klenk@hsu-hh.de)

## Schlüsselwörter

eHealth · Telemedizin · Telematikinfrastruktur · Elektronische Gesundheitskarte · Elektronische Patientenakte

### 1 Einleitung

Der technologische Wandel verändert den Gesundheitssektor nachhaltig. Die Digitalisierung eröffnet neue Diagnosetechniken und Behandlungswege, macht den Zugang zu Leistungen unabhängiger von räumlichen und zeitlichen Restriktionen, erleichtert die Verfügbarkeit von medizinischem Wissen – für Ärzte sowie für Patienten – und verändert dadurch Kommunikations- und Entscheidungsprozesse. Neben der Transformation der Arzt-Patienten-Beziehung sind aber auch alle Fragen der politischen Steuerung und der Administration von Gesundheitsleistungen in Veränderung begriffen, so zum Beispiel die Interaktionen von Patienten und Ärzten mit Krankenkassen als Leistungsförderern, das Management von Gesundheitseinrichtungen und die Planung von Leistungsangeboten. Die Digitalisierung betrifft zudem auch die der Heilung vorgelagerten Prozesse der Prävention, der Forschung und der Ausbildung des Personals sowie epidemiologische Fragen der Volksgesundheit, die vom Heilungsprozess einzelner Patienten unabhängig sind.

Digitalisierung birgt das Versprechen, Lösungen für die Herausforderungen der Gesundheitsversorgung der analogen Welt zu bringen. Zu nennen sind insbesondere die wohlbekannten Probleme der medizinischen Über-, Unter- und Fehlversorgung. So gibt es beispielsweise die Hoffnung, dass durch digitale Kommunikation und Fernbehandlung Versorgungssengpässe in ländlichen Regionen behoben werden können. Eine vernetzte Erhebung und Bereitstellung von Patienten- und Behandlungsinformationen wiederum kann Probleme der Fehlversorgung minimieren, da Diagnosen, Medikationspläne etc. schnell zugänglich sind. Die neue Transparenz der Daten kann helfen, Überversorgung zu vermeiden. Schlussendlich kann Digitalisierung zum *Empowerment* von Patienten beitragen: Neue Informations- und Kommunikationstechnologien vereinfachen den Zugang zu Wissen, digitale *Tools* wiederum ermöglichen neue Formen der Selbststeuerung und der partizipativen Entscheidungsfindung (vgl. Matusiewicz und Behm 2017, S. 74 f.).

Den Versprechen stehen allerdings Risiken und Herausforderungen gegenüber. Die zentrale Herausforderung der Digitalisierung des Gesundheitswesens besteht – wie auch in vielen anderen Politikfeldern – in der Finanzierung der technischen Infrastruktur. Daneben gibt es aber auch eine Reihe von sektorspezifischen Risiken. Wie können z. B. Patienten verlässliche Gesundheitsinformationen mit medizinischem Mehrwert von rein kommerziellen Angeboten ohne Mehrwert oder mit gar schädlicher Wirkung unterscheiden? Die Herkunft von Gesundheitsinformationen ist selten transparent und noch gibt es keine allgemeingültigen Zertifizierungsverfahren. Risiken für den Einzelnen ergeben sich auch aus der Speicherung personenbezogener Gesundheitsdaten, wenn ein leichterer Zugang zu Daten unzulässige individuelle Diskriminierung (etwa im Kontext von Arbeitsverhältnissen oder im

Versicherungsverhältnis mit Krankenkassen) möglich macht. Risiken für die Gesellschaft bestehen, wenn Krankenhäuser als kritische Infrastrukturen Gegenstand von Cyberattacken werden.

Im Moment realisieren sich für die Patienten und Nutzer von Gesundheitsleistungen in Deutschland allerdings weder die Versprechen der Digitalisierung, noch sind in Anbetracht des Ausbaustandes unkontrollierbare Risiken zu fürchten. Deutschland liegt beim Ausbau der technischen Infrastruktur und der Etablierung von digitalen Versorgungsangeboten deutlich hinter vergleichbar entwickelten Sozialstaaten zurück. Eine Ursache für den zögerlichen und schleppenden Digitalisierungsprozess wird in den besonderen Akteurskonstellationen dieses Sektors gesehen. Leistungserbringer und Krankenkassen sind aufgrund des Selbstverwaltungsprinzips maßgeblich für die Digitalisierung des Gesundheitssektors verantwortlich. Zwischen Leistungserbringern, Krankenkassen und Patienten (deren Interessen nur bedingt im Selbstverwaltungsregime repräsentiert sind) bestehen jedoch starke Interessenkonflikte, die durch die Ökonomisierung des Gesundheitssektors in den vergangenen Jahren weiter an Schärfe gewonnen haben. Aufgrund der Interessenblockaden sind allenfalls inkrementelle Veränderungsprozesse durchsetzbar (vgl. Klenk 2018, S. 19).

---

## 2 Begriffsklärung

Die Diskussion über die Digitalisierung im Gesundheitssektor wird durch eine Reihe uneinheitlich und nicht trennscharf verwendeter Begriffe geprägt. Zu nennen sind insbesondere die Begriffe Telematik und *Telemedizin*, *eHealth* (= electronic health), *mHealth* (= mobile health), *digital health* und *health 2.0*. (Gesundheits-)Telematik ist der älteste der Begriffe, ein Kunstwort, das sich aus den Begriffen Gesundheitswesen, Telekommunikation und Informatik zusammensetzt. Es findet sich heute noch versteckt im Firmennamen der Gematik, der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, die zu Beginn der 2000er-Jahre von den Spitzenorganisationen der Selbstverwaltung gegründet wurde und die Digitalisierung im deutschen Gesundheitswesen maßgeblich vorantreiben sollte. Insgesamt hat sich jedoch auch in Deutschland der in der internationalen Debatte gebräuchlichere Begriff *eHealth* durchgesetzt, der auch von der Weltgesundheitsorganisation (WHO 2005) verwendet wird.

Die Definitionen der genannten Begriffe variieren sehr stark. Der disziplinäre Hintergrund von Autoren oder ihre politische Zielsetzung prägen die Verwendung der Begriffe. Es lässt sich eine enge Begriffsverwendung mit einem starken Technikbezug von einer weiten Begriffsverwendung unterscheiden, die multi-disziplinäre und multi-akteursorientierte Perspektiven einnehmen und neben technischen Fragen auch die Dimension von Normen, Werten und Einstellungen von Akteuren berücksichtigen. Ein enges Verständnis von Digitalisierung im Gesundheitswesen meint den Einsatz von Informations- und Kommunikationstechnologien mit dem Ziel, räumliche und zeitliche Restriktionen zu überwinden. Differenziertere Begriffsverwendungen heben hervor, dass es unterschiedliche Akteure bzw. *Stakeholder* der

Digitalisierung des Gesundheitswesens mit jeweils unterschiedlichen Interessen gibt. So hält die Definition der Europäischen Union fest: „... eHealth refers to the use of modern information and communication technologies to meet the needs of citizens, patients, health care professionals, health care providers as well as policy makers“ (*EU Ministerial Declaration of eHealth 2003* (European Commission 2004)). Die WHO-Definition wiederum betont die vielfältigen Einsatzfelder der Digitalisierung, die nicht nur die direkte Interaktion zwischen Patient und Arzt (bzw. Pflegekraft) betreffen, sondern die Gesamtheit der Prozesse von der Forschung über die Prävention, die Diagnostik und Behandlung hin zu Fragen des Managements von Gesundheitseinrichtungen und der politischen Steuerung des Gesundheitswesens. In diesem Kontext verweist *eHealth*, also die Gesamtheit von digitalen Gesundheitsanwendungen, eben nicht nur auf technologische Möglichkeiten, sondern vor allem auf Denkweisen und Einstellungen, insbesondere auf die (Selbst-) Verpflichtung, mit Hilfe von neuen Informations- und Kommunikationstechnologien die Gesundheitsversorgung lokal, national und global in ihrer Effizienz und Effektivität zu verbessern.

---

### **3      Theorie: Institutioneller Rahmen und Akteurskonstellationen**

Die Digitalisierung des Gesundheitswesens – wie auch die Steuerung des Gesundheitswesens insgesamt – findet im Rahmen des Selbstverwaltungsprinzips statt. Die Gesundheitsministerien von Bund und Ländern haben im Vergleich zu anderen Politikfeldern hier nur eingeschränkte Aufgaben und Kompetenzen; stattdessen haben Ärzte und Krankenhäuser als Leistungsanbieter sowie die gesetzlichen Krankenkassen als Leistungsfinanzierer das historisch gewachsene Recht, ihre Angelegenheiten in eigener Verantwortung zu regeln. Der Staat schafft hierfür die institutionellen Voraussetzungen in Form von Selbstverwaltungskörperschaften mit Pflichtmitgliedschaft (die gesetzlichen Krankenkassen für Versicherte als Leistungsfinanzierer einerseits, Kassenärztliche Vereinigungen, Krankenhausgesellschaften und Ärztekammern für Ärzte/Krankenhäuser als Leistungsanbieter anderseits) und definiert Verhandlungsarenen, in denen Akteure ihre Interessenkonflikte austragen. Hierzu gehört insbesondere die sogenannte Gemeinsame Selbstverwaltung von Leistungsfinanzierern und Leistungsanbietern mit dem gemeinsamen Bundesauschuss als oberstes Verhandlungsgremium.

Die institutionelle Ausgestaltung des Selbstverwaltungsregimes begünstigt die Interessen der Leistungsfinanzierer und -anbieter; Patienten, deren Interessen eigentlich im Zentrum des Geschehens stehen sollten, haben im Selbstverwaltungsregime nur eingeschränkte Vertretungs- und Beteiligungsrechte. Welche Rolle Patienten im Prozess der Digitalisierung einnehmen, wird kontrovers diskutiert. Patienten sind eine höchst heterogene und daher in Bezug auf ihre Organisationsfähigkeit „schwache“ Gruppe, die auf advokatorische Interessenvertretung durch Patienten- oder Wohlfahrtsverbände angewiesen ist. Von der Digitalisierung versprechen sich einige ein *Empowerment* der Patienten, die nun selbst auf Daten und medizinisches Wissen

zugreifen und damit die Informationsasymmetrie zwischen Arzt und Patient in Teilen ausgleichen können. In der öffentlichen Diskussion sind aber vor allem auch die Risiken der Digitalisierung präsent. Kritisch diskutiert werden beispielsweise Fragen der sozialen (Un-)Gleichheit. Die Digitalisierung enthält insbesondere auch das Ziel, die Versorgung in ländlichen, schwach besiedelten Räumen zu verbessern – just in diesen Bereichen sind aber die notwendigen digitalen Kompetenzen und die *ehealth-literacy* (Fähigkeiten und Kenntnissen, die wesentlich für die Anwendung von technologiebasierten Gesundheitsangeboten sind) bei Patienten und Bürgern am wenigsten gegeben.

Seit Mitte der 1990er-Jahre wird die Steuerung des Gesundheitssektors durch Selbstverwaltung sukzessive mit Elementen von Markt und Wettbewerb ergänzt. Ausdruck davon sind der Privatisierungsdruck im Krankenhaussektor und der Wettbewerb von Krankenhäusern und Krankenversicherungen um Patienten und Versicherte. Aufgrund der komplexen Akteurskonstellationen zählt der Gesundheitssektor zu den Feldern, die in hohem Maße durch Reformblockaden und Status-quo-Politik gekennzeichnet sind. Auch im Kontext der Digitalisierung bringt der Steuerungsmix aus Selbstverwaltung, Markt und Wettbewerb diverse Herausforderungen mit sich. Konflikte zwischen den Selbstverwaltungsakteuren ergeben sich zum einen aus ungeklärten Fragen der Finanzierung bzw. der Vergütung von digitalen Versorgungsangeboten. Digitale Anwendungen sind gegenwärtig nur vereinzelt im Leistungskatalog der gesetzlichen und privaten Krankenversicherungen (GKV/PKV) enthalten. Die Mehrheit der GKV-Versicherten, die wiederum 90 % der deutschen Bevölkerung darstellen, hat jedoch keinen regulären Zugang zu digitalen Versorgungsangeboten. Stattdessen etabliert sich zunehmend ein „zweiter Gesundheitsmarkt“ mit digitalen Versorgungsangeboten für sehr spezifische Zielgruppen mit meist privater Finanzierung.

Eine zweite Konfliktlinie ergibt sich aus dem Spannungsverhältnis zwischen dem Wunsch nach Transparenz einerseits und dem Schutz personenbezogener Daten andererseits. Die Verwendung der Daten im Dreiecksverhältnis zwischen Patient, Krankenversicherung und Leistungserbringern ist sehr intransparent. Der Wettbewerb zwischen den Krankenkassen und die starren Grenzen zwischen ambulantem und stationärem Sektor, zwischen Prävention, Rehabilitation und Pflege haben die Herausbildung nicht-kompatiblen Datensilos zur Folge, auf die jeweils unterschiedliche Akteure Zugriffsrechte haben.

Ein Beispiel *par excellence* für die Implementationsprobleme im Gesundheitswesen stellt die Einführung der elektronischen Gesundheitskarte (eGK) dar, die eindrücklich demonstriert, wie ungeklärte Fragen der Finanzierung und des Datenschutzes zu Blockaden führen. Die Einführung der eGK und verschiedener auf ihr basierender Anwendungen (z. B. die elektronische Patientenakte und das elektronische Rezept) wurde bereits 2004 mit dem Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz [GMG]) beschlossen. Das Gesetz, dem seinerseits eine über zehnjährige Diskussionszeit über die (Begrenzung der) technischen Möglichkeiten der eGK, über Datenschutz und Finanzierung vorausging, sah vor, dass die gesetzlichen Krankenkassen ihre Versicherten bis 2006 mit einer eGK ausstatten. Die Selbstverwaltungsakteure haben zu diesem Zweck die Gematik mbH gegründet, die die elektronische Gesundheitskarte und ihre Infrastruktur definieren, testen und betreiben sollte.

Mehrere Anläufe zur Einführung scheiterten jedoch. Erst seit 2013 ist die Mehrzahl der GKV-Versicherten in Besitz einer eGK, deren Funktionalität aber erheblich eingeschränkt ist. Auf ihr sind die Versichertenstammdaten gespeichert; für die GKV-Versicherten ist sie der Berechtigungsnachweis für die Inanspruchnahme ärztlicher Leistungen. Weitergehende Funktionen wie die Speicherung und der Austausch von medizinischen Informationen (z. B. Diagnosen, Medikationspläne etc.) werden bislang allenfalls in Rahmen von Pilotprojekten erprobt, sodass das *eHealth*-Gesetz, das am 01.01.2016 in Kraft getreten ist, erneut die Aufforderung an die Selbstverwaltungsakteure enthält, die weitergehenden Funktionen der Karte auszubauen. Die in dieses Reformprojekt investierten Versichertengelder und der bisher erzielte Nutzen der technischen Neuerung stehen in keinem Verhältnis zueinander.

In zunehmendem Maße wird die Digitalisierung des Gesundheitssektors von (Wirtschafts-)Akteuren bestimmt, die nicht zu den klassischen Mitspielern zählen und sich von neuen technologischen Standards Wettbewerbsvorteile versprechen. Deutlich wird dies insbesondere bei den digitalen Angeboten des „zweiten“ Gesundheitsmarktes, auf dem rein privat finanzierte Produkte und Dienstleistungen rund um die Gesundheit gehandelt werden. Die dort vertriebenen gesundheitsbezogenen *Wearables* und *Apps* werden in aller Regel von Innovatoren aus dem privatwirtschaftlichen Umfeld entwickelt (und eben nicht von Akteuren der Selbstverwaltung im Gesundheitswesen). Aber auch die Selbstverwaltungsakteure versuchen ihre Wettbewerbsposition mit Industriepartnerschaften zu verbessern. So setzen beispielsweise die Techniker Krankenkasse (TK) oder die Allgemeine Ortskrankenkasse (AOK) Nordost nicht allein auf die *Telematikinfrastruktur*, sondern haben je individuelle Beziehungen zu einzelnen Industriepartnern aufgebaut, um die elektronische Patientenakte in Kombination mit der elektronischen Gesundheitskarte marktfähig zu machen. Auf Seiten der Leistungsanbieter hat die Kassenärztliche Vereinigung in Baden-Württemberg das Modelprojekt „*doctdirect*“ zur Erprobung der *Online-Fernbehandlung* initiiert (vgl. KVBW 2019). Auch in Bayern, Nordrhein-Westfalen und Niedersachsen gibt es ähnliche Digitalisierungsprojekte. Diese Initiativen haben zwar durchaus einen innovativen Charakter, aber sie bleiben aufgrund ihres Geltungsbereichs nur „Silo-Lösungen“.

Die Beispiele zeigen, dass der institutionelle Steuerungsmix im Gesundheitswesen zu nicht-intendierten Folgeproblemen bei der Digitalisierung des Gesundheitswesens führt: Im Vergleich mit anderen Staaten findet sie in Deutschland zeitverzögert und mit gedrosseltem Tempo statt. Zudem haben sich durch die Einführung von Markt und Wettbewerb die Interessenkonflikte zwischen den Akteuren weiter verschärft. Konzertierte Aktionen sind nur schwer realisierbar; stattdessen werden Insellösungen geschaffen, die ihrerseits wieder zu Interoperabilitätsproblemen führen.

---

## 4 Praktische Anwendungsfelder

Der eigentlich disruptive Vorgang für die Veränderung in der Arzt-Patienten-Beziehung liegt in der Erfindung des *Smartphones*, das sich zunehmend zum medizinischen Allzweckwerkzeug des 21. Jahrhunderts entwickelt, mit dem die Diagnose

mehr und mehr von der Hand des Arztes in die des Patienten gelegt wird. Befördert wird diese Entwicklung durch gesellschaftliche Trends wie Achtsamkeit und „Quantified Self“, die in den Alltag integrierte, kontinuierliche, gesundheitsbezogene Selbstvermessung des Körpers. So befinden sich bereits Anamnesewerkzeuge wie die Applikation „Ada“ auf dem Markt (Ada 2018), die es Patienten ermöglicht, in einem standardisierten Prozess ihre Symptome einzugeben und die, nach einem Abgleich mit der hinterlegten Datenbank auf der Basis von Künstlicher Intelligenz, eine Auskunft über mögliche Diagnosen gibt. Die Differenzialdiagnose wird objektiviert, indem sie ausweist, auf wie viele Patienten mit den gleichen Symptomen eine entsprechende Diagnose zutraf.

Für Ärzte wiederum gewinnt bei den exponentiell steigenden Datenmengen der Einsatz von modernen *Medical Decision Support Systems* (MDSS) an Bedeutung (vgl. Woosley et al. 2016, S. 161 f.). Das sind Informationssysteme, die Ärzte bei klinischen Entscheidungen unterstützen. Durch Verfahren wie „Data Mining“ (die systematische Anwendung statistischer Methoden auf große Datenmengen) sowie „Machine Learning“ (das „Lernen“ aus einer Vielzahl von Beispielen durch künstliche Systeme) unterstützen solche Systeme Ärzte dabei, aus großen Datenmengen die relevanten Informationen herauszufiltern und auf dieser Grundlage eine evidenzbasierte Entscheidung zu treffen.

Zur Anwendung kommen diese technischen Systeme in den Bereichen Diagnose, Therapie und Medikation. Im Rahmen der Medikation können beispielsweise *Electronic Medical Records* (EMR) mit Datenbanken zu Risikofaktoren und Risikoklassen von Medikamenten verknüpft werden. Das MDSS überprüft automatisch die relevanten Informationen und kann bei einer potenziellen Fehlverschreibung eine Meldung ausgeben und Alternativen vorschlagen. Neben evidenzbasierter Medizin verspricht die Verknüpfung von EMRs mit einem MDSS eine Erhöhung der Behandlungssicherheit sowie eine verbesserte Diagnostik. Für die medizinische Behandlung können zeitnah relevante Informationen zu Verfügung gestellt und auf diese Art und Weise Behandlungsfehler reduziert und die Behandlungsqualität verbessert werden.

Mit Blick auf das Arzt-Patienten-Verhältnis ist zudem das Thema Telemedizin zu diskutieren. Der Begriff umfasst verschiedene Versorgungskonzepte, bei denen medizinische Leistungen via Informations- und Kommunikationstechnologien über räumliche Distanzen hinweg erbracht werden. Diese Leistungen können die Bereiche Diagnostik, Therapie, ärztliche Entscheidungsberatung, Monitoring sowie Rehabilitation umfassen. Die am weitesten entwickelten Formen der Telemedizin sind die Videosprechstunde sowie das Telemonitoring, also eine dauerhafte Überwachung der zentralen Gesundheitsparameter von Risikopatienten über das Internet, um zeitkritische Interventionen frühzeitig zu ermöglichen.

In Deutschland war es Ärzten lange verwehrt, Patienten ausschließlich via Telekommunikationsmedien zu behandeln. Gemeinhin wird dies als „Fernbehandlungsverbot“ bezeichnet. Von zentraler Bedeutung ist allerdings der Zusatz ‚ausschließlich‘, denn nach der Rechtslage war nach einem physischen Arztbesuch eine Weiterbehandlung per Videokonsultation oder Telefon durchaus möglich. Da telemedizinische Behandlungen aber lange Zeit nicht im Leistungskatalog der GKV

enthalten und daher für Ärzte nicht abrechenbar waren, gab es ein faktisches Fernbehandlungsverbot. Langsam und schrittweise werden nun aber Leistungskatalog und Vergütungssätze angepasst. Beim 121. Deutschen Ärztetages im Mai 2018 wurde zudem mit großer Mehrheit für die Anpassung der Musterberufsordnung (MBO-Ä) gestimmt, sodass nunmehr auch in Deutschland erlaubt ist, was z. B. in der Schweiz längst Standard ist, nämlich der medizinische Erstkontakt via Fernbehandlung.

Im Vergleich zur Schweiz gibt es aber Einschränkungen: Eine Bescheinigung der Arbeitsunfähigkeit per Video oder Telefon bei unbekannten Patienten lehnten die Delegierten auf dem Bundesärzttetag ab, ebenso Verordnung von Arzneimitteln ausschließlich im Rahmen von Fernbehandlungen. Beispiele in Nachbarländern zeigen jedoch, dass auch Krankschreibungen und Rezepte für Medikamente vielversprechende „Features“ sein können, um auf der einen Seite Effizienzreserven in der medizinischen Versorgung zu mobilisieren und auf der anderen Seite der gewünschten *Patient Experience* einer sich in allen Bereichen digitalisierenden Gesellschaft gerecht zu werden.

Mit Blick auf den Austausch von Daten und Informationen zwischen Patienten, Ärzten und Krankenkassen ist schließlich die elektronische Gesundheitskarte von Relevanz. Die Einführung der elektronischen Gesundheitskarte erfolgte in mehreren Stufen seit 2011. Bislang wird die Karte jedoch vornehmlich zur Speicherung der Versichertenstammdaten genutzt. Viele weitere Anwendungsfelder, die zur Verbesserung der Behandlungsqualität beitragen können, wie z. B. die Speicherung von Arztbriefen, Notfalldaten oder Medikationsdaten in einer elektronischen Patientenakte, sind denkbar, kommen in Deutschland aber (anders als in vergleichbaren Sozialstaaten) bislang nicht zum Einsatz.

---

## 5 Umsetzungsstand und Auswirkungen

Der rechtliche Rahmen für die Digitalisierung des Gesundheitswesens wird gegenwärtig vor allem durch das „eHealth“-Gesetz der Großen Koalition (2013–2017) bestimmt. Die Kernpunkte des Gesetzes sind der digitale Medikationsplan für bestimmte Versichertengruppen, die Förderung des elektronischen Arztbriefes, die Vergütung von telemedizinischen Arztkonsilen (Austausch zwischen Ärzten zur Beurteilung), die Förderung von Videosprechstunden, die Speicherung der Notfalldaten auf der elektronischen Gesundheitskarte und die verpflichtende Prüfung der Versichertenstammdaten dieser Karte sowie die elektronische Patientenakte. Der Umsetzungsstand des *eHealth*-Gesetzes stellt sich wie folgt dar (vgl. BMG 2018):

- Ab dem 1. Januar 2019 sollte für alle Versicherten ein Anspruch auf eine elektronische Patientenakte (ePA) bestehen, in die wichtige medizinische Dokumente wie Arztbriefe, Medikationsplan, Notfalldaten, Impfausweis etc. abgelegt werden können und diese direkt beim Patienten liegen. Die bundesweite Installation neuer Telematikinfrastrukturen, die als technische Voraussetzungen für die Einführung von elektronischen Patientenakten gelten, hängt dem ursprünglichen

Zeitplan hinterher. Im November 2018 hat der Bundestag die Frist für die Anbindung der einzelnen Gesundheitseinrichtungen an die Telematikinfrastruktur (TI) verlängert. Für Praxen, die nachweisen konnten, dass sie bis zum 31. März 2019 die notwendigen Komponenten für den Anschluss an die TI verbindlich bestellt haben, wurde der Honorarabzug bis zum 30. Juni 2019 ausgesetzt (vgl. Kassenärztliche Vereinigung 2019).

- Seit Anfang 2017 wird in der Testregion Nord (Schleswig-Holstein, Nordrhein-Westfalen und Rheinland-Pfalz) mit 500 Ärzten eine Erprobung des Versichererstammdatenmanagements durchgeführt. Der ursprünglich gesetzlich vorgesehene Zeitplan, wonach ab 1. Juli 2018 Ärzte und Psychotherapeuten zur Prüfung der Stammdaten der Versicherten auf der elektronischen Gesundheitskarte gesetzlich verpflichtet sein sollten, wurde jedoch nicht eingehalten. Nach wie vor werden zudem Patienten mit Karten der ersten Generation in den Praxen vorstellig, die gar nicht mehr gültig sind, weil sie für die neuen digitalen Anwendungsfelder des *eHealth*-Gesetzes technisch nicht tauglich sind.
- Laut Gesetz sollten die Versicherten ab dem 1. Januar 2018 die Möglichkeit haben, notfallrelevante Informationen (Diagnosen, Medikation, Allergien, Unverträglichkeiten etc.) auf ihrer elektronischen Gesundheitskarte eintragen zu lassen. Bereits seit dem 1. Oktober 2016 haben Patienten Anspruch auf einen Medikationsplan – in Papierform –, sofern sie mindestens drei gleichzeitig verordnete Medikamente bekommen haben. Apotheken müssen auf Wunsch Aktualisierungen des Plans vornehmen. Ab 2018 sollte der Medikationsplan auch auf der elektronischen Gesundheitskarte zugreifbar sein und ab 2019 sollten alle Vertragsärzte und Apotheken in der Lage sein, einen mittels der eGK gespeicherten Medikationsplan zu aktualisieren. Dieser ursprüngliche Zeitplan konnte nicht eingehalten werden.
- Am 15. Mai 2019 präsentierte das Bundesgesundheitsministerium (BMG) als nächsten Schritt einen Referentenentwurf für ein „Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation“ – kurz das „Digitale Versorgung Gesetz“ (DVG). Der neue Entwurf beinhaltet verschiedene Regelungen zur TI-Anbindung, zur Zulassung von digitalen Gesundheitsanwendungen (Apps) und zur Bewerbung von Videosprechstunden. Erstmals wird auch eine Frist zur TI-Anbindung für Apotheken genannt: Bis zum 31. März 2020 müssen Apotheken an die Datenautobahn angeschlossen sein, um den elektronischen Medikationsplan künftig aktualisieren zu können.
- Seit dem 1. Januar 2017 wird der elektronische Versand von Arztbriefen mit 0,55 € vergütet, sofern der Arztbrief mittels eines eArztausweises elektronisch signiert wird.
- Seit dem 1. April 2017 können Vertragsärzte ihren Bestandspatienten Videosprechstunden anbieten; im EBM Katalog wurde ein entsprechender Kostensatz eingeführt. Bislang wird diese Möglichkeit jedoch nur selten genutzt.

Die Aufzählung zeigt, dass ein Großteil des Lastenheftes, welches im Rahmen des *eHealth*-Gesetzes von 2016 verabschiedet wurde, aus mannigfaltigen Gründen bisher keine oder nur partielle Umsetzung gefunden hat.

Um die Digitalisierung des deutschen Gesundheitssystems dennoch weiter voranzutreiben, hat das Bundesgesundheitsministerium die offenen Aspekte zum Teil in neueren Gesetzgebungsverfahren wieder eingebracht. So sieht neben dem Entwurf für das DVG beispielsweise das am 1. Mai 2019 in Kraft getretene Terminservice- und Versorgungsgesetz (TSVG), das im Kern den Ausbau von Terminservicestellen betrifft, aber auch als „eHealth-Reparatur-Gesetz“ bekannt ist, folgende Regelungen vor:

- Ebenso wie in anderen Branchen üblich, sollen Terminservicestellen für das Terminmanagement digitale Assistenten nutzen; zukünftig sollen Patienten mit den Terminservicestellen Termine also nicht mehr nur telefonisch, sondern auch *online* und per *App* vereinbaren können.
- In infrastrukturell schwächeren Gebieten, bzw. dort wo eine Unterversorgung droht, müssen die Kassenärztlichen Vereinigungen zukünftig Versorgungsalternativen anbieten, welche auch von den Kassenärztlichen Vereinigungen eigens betriebene Praxen oder Fernbehandlung sein können.
- Krankenkassen sind verpflichtet, die elektronische Patientenakte bis spätestens 2021 für all ihre Versicherten anzubieten (es kommt also im Vergleich zum ursprünglichen Zeitplan des *eHealth*-Gesetzes um eine weitere Verzögerung von zwei Jahren); in Zukunft sollen alle Versicherten auch über ihre mobilen Endgeräte Zugriff auf ihre Akten erhalten. Auch Arbeitsunfähigkeitsbescheinigungen sollen ab 2021 digital übermittelt werden. Krankenkassen erhalten zudem die Erlaubnis, bei strukturierten Programmen für chronisch Kranke digitale Anwendungen zu nutzen.
- Schlussendlich sieht das Gesetz auch vor, die Entscheidungsverfahren in der Gematik zur verbessern; mit dem Ziel, Entscheidungsprozesse zu beschleunigen, plant das Bundesministerium für Gesundheit, 51 Prozent der Geschäftsanteile der Gematik zu übernehmen.

Die Korrekturen am *eHealth*-Gesetz erscheinen als dringend notwendig, um eine nachhaltige Digitalisierung des Gesundheitssystems voranzutreiben. Aufgrund der fehlenden Umsetzung der gesetzlichen Vorgaben ist festzustellen, dass immer mehr private Anbieter das Feld besetzen und eigene Lösungen anbieten. So existieren als Alternative zur elektronischen Patientenakte bereits mobile Lösungen, wie die *Apps* „Lifetime“ oder „Vivy“. Hier trägt der Patient seine medizinischen Dokumente auf seinem *Smartphone* immer griffbereit bei sich, das Gerät ersetzt gewissermaßen die elektronische Patientenakte sowie Gesundheitskarte, denn auch Notfalldaten, Versichertenstammdaten und sonstige relevante Informationen lassen sich darüber an die jeweilige Praxis übermitteln. Private Firmen, die diese *Apps* entwickelt haben, kooperieren bereits mit einer nennenswerten Anzahl an gesetzlichen Krankenkassen. Auch bei Videosprechstunden gibt es private Lösungen. Seit Januar 2018 bietet die deutsche privaten Krankenversicherung *Ottonova* für alle Versicherten die Vergütung von telemedizinischen Arztkonsultationen über den Schweizer Anbieter „*eedoctors*“ an. Diese privaten Akteure bieten einerseits innovative Lösungen an, die

den Erwartungen einer digitalen Gesellschaft entsprechen, andererseits können sich neue Probleme ergeben, wenn innovative digitale Gesundheitsanwendungen die Interoperabilität zu existierenden Strukturen unberücksichtigt lassen.

---

## 6 Perspektiven für Staat und Verwaltung

Die oben beschriebenen praktischen Anwendungsfelder für digitale Gesundheitsleistungen beschreiben für das deutsche Gesundheitssystem vielfach einen potenziellen Möglichkeitsraum; von einer nachhaltigen Implementation und weitverbreiteten Nutzung kann in den meisten Feldern noch keine Rede sein.

Eine dynamische digitale Transformation findet lediglich im zweiten Gesundheitsmarkt statt, indem Digitalisierungsstrategien jedoch vor allem von den Interessen privater Akteure abhängen und es bislang keine hinreichenden politischen Instrumente zur Regulierung von Qualität, Preis und Zugang zu Leistungen gibt. Der digitale Transformationsprozess schafft zudem neue soziale Spaltungslien bzw. vertieft und verfestigt bestehende soziale Ungleichheitsstrukturen. Ob Patienten Zugang zu digitalen Gesundheitsleistungen haben, hängt gegenwärtig häufig vom Zufall (z. B. dem Wohnort), von privaten (Finanz-)Ressourcen und vorhandenen digitalen Kompetenzen ab.

Zudem wird sich sukzessive die Anzahl von gewichtigen Spielern in der Gesundheitswirtschaft erhöhen, da Unternehmen wie Google, Amazon, Facebook und Apple durch ihre Kompetenz im Datenmanagement sowie ihrem breitem Zugang zur Bevölkerung, ihrer Bekanntheit und Akzeptanz auf signifikante Potenziale im Bereich der Umsetzung von innovativen Versorgungskonzepten zurückgreifen können und so den ursprünglich gestaltenden Institutionen den Rang des „first movers“ ablaufen.

Die schleppende Digitalisierung des deutschen Gesundheitswesens deutet darauf hin, dass bei der Vielzahl der Akteure und den unterschiedlichen Interessenslagen ohne eine stärkere zentrale Steuerung (wie sie im Terminservice- und Versorgungsgesetz jüngst schon in Ansätzen deutlich geworden sind) größere Durchbrüche kaum zu erwarten sind. Trotz erheblicher Investitionen in die Infrastruktur ist die elektronische Gesundheitskarte heute kaum mehr als ein erweiterter Mitgliedsausweis für die jeweilige Krankenkasse, von allgemein etablierten elektronischen Patientenakten sind wir noch weit entfernt. Wenn technische Angebote Akzeptanz finden sollen, dann müssen sie für Versicherte und Patienten einen spürbaren Mehrwert bringen. Das gilt nicht nur für die medizinische Versorgung, sondern auch für einen erleichterten Umgang mit Gesundheitsverwaltung und Leistungsanbietern. Die Menschen haben im digitalen Zeitalter nicht nur bestimmte Erwartungen, wie Dienstleistungen erbracht werden sollten; sie wollen auch ihre Erfahrungen im Gesundheitssystem einbringen. Den etablierten Akteuren droht also nicht nur eine neue Konkurrenz durch Firmen, die sich auf die Nutzung von Daten spezialisiert haben, sondern auch eine zunehmende Kritik von Seiten der Bürger.

## Literatur

- Ada. 2018. *Your personal health guide*. <https://ada.com/>.
- BMG – Bundesministerium für Gesundheit. 2018. eHealth Gesetz. <https://www.bundesgesundheitsministerium.de/service/begriffe-von-a-z/e/e-health-gesetz.html>. Zugriffen am 31.07.2018.
- European Commission. 2004. *eHealth. Ministerial declaration*. Brussels, 22.05.2003. [http://ec.europa.eu/information\\_society/doc/qualif/health/COM\\_2004\\_0356\\_F\\_EN\\_ACTE.pdf](http://ec.europa.eu/information_society/doc/qualif/health/COM_2004_0356_F_EN_ACTE.pdf). Zugriffen am 01.08.2019.
- Klenk, Tanja. 2018. Interessenlagen und Interessenpolitik im Gesundheitssektor. In *Ärzteverbände und ihre Mitglieder*, Hrsg. Tim Spier und Christoph Strünck, 19–46. Wiesbaden: Springer VS.
- KVBW – Kassenärztliche Vereinigung Baden-Württemberg. 2019. *doc2direct. Das telemedizinische Modell-Projekt der KVBW*. <https://www.kvbawue.de/praxis/neue-versorgungsmodelle/doc2direct/>.
- Matusiewicz, David, und Moritz E. Behm. 2017. Zehn Thesen zur digitalen Transformation im Gesundheitswesen. Eine Branche zwischen etabliertem Stillstand und disruptiven Sprüngen. In *Gesundheitswesen Aktuell 2017. Beiträge und Analysen*, Hrsg. Uwe Repschläger, Claudia Schulte und Nicole Osterkamp, 66–86. Schwäbisch Gmünd: Barmer GEK.
- WHO. 2005. *WHO eHealth resolution*. 58th World Health Assembly, Resolution 28. Geneva: World Health Organization. <http://www.who.int/healthacademy/news/en/>. Zugriffen am 05.08.2019.
- Woosley, Raymond L., John Whyte, Ali Mohamadi, und Klaus Romero. 2016. Medical decision support systems and therapeutics: The role of autopilots. *Clinical Pharmacology and Therapeutics* 99(2): 161–164.



---

# Smart Cities

Felix Butzlaff

## Inhalt

1 Einleitung .....	508
2 Begriff: Smart Cities zwischen Stadtmarketing und Management-Versprechen .....	509
3 Konzeptionelle Grundlagen .....	511
4 Verbreitung und Wirkungen .....	513
5 Perspektiven für Staat, Stadt und Verwaltung .....	514
Literatur .....	515

---

## Zusammenfassung

Smart Cities sollen mit digitalen Netzwerk- und Kommunikationstechnologien einerseits die Arbeit von Stadtplanung und – regierung ökonomisch wettbewerbsfähig und effizient gestalten und andererseits die Lebensqualität der BürgerInnen und die Responsivität von Politik und Verwaltung erhöhen wie auch eine ökologisch nachhaltigere Stadt verwirklichen. Komplexe Gesellschaften sollen durch das Versprechen digitaler Technologien besser steuerbar bleiben und eine direktere Einbindung der BürgerInnen ermöglichen. Gleichzeitig drohen durch die Technologie- und eine Wachstumsfixierung der bisherigen Umsetzungen soziale und ökologische Ziele zu Feigenblättern degradiert zu werden.

---

## Schlüsselwörter

Smart City · Demokratie · Transparenz · Überwachung · Nachhaltigkeit

---

F. Butzlaff (✉)

Institut für Gesellschaftswandel und Nachhaltigkeit (IGN), Vienna University of Economics and Business, Wien, Österreich

E-Mail: [felix.butzlaff@wu.ac.at](mailto:felix.butzlaff@wu.ac.at)

## 1 Einleitung

Der Begriff der *Smart City* als einer digitalen Vernetzungs- und Koordinierungsstrategie für Großstädte ist seit den ausgehenden 1990er-Jahren zunächst in Singapur und anderen ostasiatischen Metropolregionen entwickelt worden. Eine Smart City soll, so der Anspruch, mittels Nutzung digitaler Netzwerk- und Kommunikationstechnologien die Arbeit von Stadtplanung und -regierung einerseits ökonomisch wettbewerbsfähig und effizient gestalten, andererseits die Lebensqualität der BürgerInnen und die Responsivität der Politik und Verwaltung ihnen gegenüber erhöhen und drittens ökologische Nachhaltigkeit im urbanen Raum verwirklichen helfen. Immer komplexer werdende Gesellschaften und Problemlagen sollen durch das Versprechen digitaler Technologien, Daten zu sammeln, Akteure zu vernetzen, Präferenzen abzubilden und Interessen abzustimmen, steuerbar bleiben und gleichzeitig eine direktere Einbindung der BürgerInnen ermöglichen.

Das Leitbild einer Smart City hat seit der Jahrtausendwende und besonders seit 2010 in Europa an Verbreitung und Überzeugungskraft gewonnen. Die Europäische Union hat es zum Ankerbegriff für die Forschungsförderung und Entwicklungsstrategie gemacht (Cocchia 2014). Kaum eine Metropolregion kommt mehr ohne den Anspruch aus, smart zu sein, smart zu regieren und smart den Wohlstand und das Wohlsein seiner BürgerInnen zu gestalten (Martin et al. 2018). Nicht zuletzt beinhaltet das Konzept der Smartness auch das Versprechen, durch intelligente und technologiebasierte Steuerung gegenüber den als restriktiv wahrgenommenen Imperativen vergangener gesellschaftlicher Krisendiagnosen, etwa der *Nachhaltigkeit*, zukünftige Krisen ohne eine Einschränkung des individuellen Lebensstils meistern zu können.

Smart Cities verbinden im Hinblick auf die Stadtplanung also einerseits einen technologischen Optimismus mit einer Demokratisierung der Technologie. Letzteres nimmt auch dezidiert Bezug auf eine Legitimitätskrise der repräsentativen Demokratie, wie sie sich etwa in immer geringer werdenden Beteiligungsralten bei Wahlen, Abstimmungen oder den Mitgliedschaften politischer Großorganisationen abzeichnet. Neue digitale Beteiligungstechnologien im Rahmen von Smart Cities sollen hier Abhilfe schaffen und die BürgerInnen zur direkten Partizipation und demokratischen Selbstermächtigung aktivieren: Mittels Internetportalen, digitalen Abstimmungsprozessen sowie crowd-sourcing-Lösungen sollen vermutete Hemmschwellen demokratischer Teilhabe abgebaut werden und neue Formen demokratischer Partizipation verwirklicht werden.

Andererseits ist die *Demokratisierung* der Technologie im Rahmen von Smart Cities lediglich ein Pfeiler ihres Selbstverständnisses – andere sind Wettbewerbsfähigkeit und die Steigerung von Wohlstand und Lebensqualität. Während wissenschaftliche BeobachterInnen dem einen dabei eine zutiefst neoliberalen Entwicklungsvorstellung zuschreiben – die Verquickung von öffentlicher Hand und privaten Gewinninteressen sowie die starke Konzentration auf managerial approaches, d. h. eine post-politische Auffassung, dass es zu jedem Problem technische Lösungen gebe (Novy 2015) –, streichen KritikerInnen die Kehrseite einer umfassenden Datensammlung heraus: zunehmende Einsichtnahme und Wissensaggre-

gation zum Verhalten und den Präferenzen der BürgerInnen bergen auch das Risiko von *Überwachung*, Homogenisierungsdruck und Zensur (Riesenecker-Caba 2016; Martin et al. 2018). Denn Technologien als solche sind nie neutral, sondern in ihren Wirkungen abhängig davon, wer sie nutzt und in welcher Weise. Zudem wird durch Smart Cities ein zentraler Faktor zeitgenössischer Legitimitätsdefizite eher noch zugespitzt: die Abhängigkeit des demokratischen Einflusses von persönlichen, sozialen, finanziellen und technischen Ressourcen, welche Menschen zu ihrer Verfügung haben, wächst in Smart Cities noch an und vertieft diese zuletzt diagnostizierte gesellschaftliche Spaltung in diejenigen, welche von Modernisierungsprozessen profitieren und jene, die dazu nicht imstande sind (Rosol et al. 2018).

---

## **2 Begriff: Smart Cities zwischen Stadtmarketing und Management-Versprechen**

Der Begriff Smart City ist keine wissenschaftliche Analysekategorie, sondern Selbstzuschreibung, politisches Programm und städtisches Entwicklungsziel in einem, ein Leitbild, das von Beratungsfirmen und Unternehmen sowie von Parteipolitik und Stadtverwaltungen gleichermaßen propagiert wird. Ein beinahe inflatorischer Gebrauch macht es schwer, präzise zu definieren, anhand welcher Kriterien man eigentlich von einer Smart City reden kann. Die Heterogenität der beteiligten Akteure bringt nicht nur unterschiedliche Perspektiven, sondern auch abweichende Prioritäten mit sich. Für Stadtverwaltungen sind das oftmals gänzlich andere als für Politiker, die für das Amt des Bürgermeisters kandidieren, eine Tourismus-Behörde oder einen IT-Konzern.

Mit den oft synonym verwendeten Begriffen der Intelligent City, Digital City, Knowledge City oder Sustainable City gibt es ähnlich unscharfe konkurrierende Konstrukte, die deutlich machen, dass es sich bei der Zuschreibung „smart“ (oder einem der Synonyme) immer auch um legitimierende Strategien im Wettbewerb der Standorte handelt, wie sie im Stadtmarketing und im Ringen um Attraktivität, Investitionen und Arbeitsplätze gang und gäbe sind (Cocchia 2014). Jede Großstadt beschäftigt mittlerweile ganze Abteilungen von Marketing- und Strategie-ExpertInnen, um ihr Image zu pflegen und Alleinstellungsmerkmale herauszustellen und ihr den Nimbus von *Lebensqualität*, Innovation und Zukunftsfähigkeit auf den Leib zu schreiben. Städte sind in diesem Sinne Spielfeld eines weltweiten Wettbewerbs um Ansehen, Fachkräfte und Wirtschaftskraft geworden.

Der Topos smart spielt hier seit den 1990er-Jahren eine zentrale Rolle. Ausgangspunkt ist zunächst einmal der Gedanke, Technologie und speziell Mittel der vernetzten Informations- und Kommunikationstechnologien zur gezielten Verbesserung von Lebensqualität im öffentlichen und privaten Raum von Städten einzusetzen (Batty et al. 2012). Hierbei soll das Zukunfts- und Innovationsversprechen von Technik zur Effizienzsteigerung und Erfassung von Bedarf und Nachfrage genutzt werden. Digitalisierung soll, so die Idee, in

immer weitere Bereiche von Städteplanung und -verwaltung Einzug erhalten, damit die BürgerInnen einerseits rascher und müheloser mit ihrer Stadtverwaltung Kontakt aufnehmen, Feedback geben, Kritik üben etc., andererseits schneller und reibungsloser informiert werden können. Drittens sollen urbane Allokationsprobleme, etwa im Verkehrs- oder Energiebereich, möglichst ressourcenschonend und nachhaltig gelöst werden können. Zentraler Gedanke ist dabei weiterhin, dass möglichst viele Gruppen und Akteure umfassend an diesem technikbasierten Koordinierungsprozess beteiligt werden: BürgerInnen, Stadtpolitik, Verwaltung, Unternehmen, Wissenschaft, Interessensverbände und Medien sollen Zugang und Gehör finden.

Städte sind allerdings nicht nur die Träger technologiefixierter Zukunftsversprechen eines wirtschaftlichen Wachstums oder steigender Lebensqualität, sondern auch Ort und Kristallisierungspunkt zentraler Krisenerscheinungen der Moderne, vor allem im Hinblick auf Ökologie, Ressourcennutzung und Klimawandel einerseits und zunehmenden gesellschaftlichen Heterogenitäten, der Auflösungen von Milieus und einheitlichen Lebenslagen andererseits (Novy 2015; Viitanen und Kingston 2014). Diese Krisenlagen zeitigen nicht nur in Städten überaus mächtige Auswirkungen, sondern auch ihre Ursachen lassen sich hier – über das demografisch und ökonomisch beschleunigte Wachstum von Metropolen – zu einem Großteil verorten. Das Konzept Smart City möchte diese Bereiche – Zukunfts- und Wachstumsversprechen, effizientere Krisenbewältigung und eine direktere Einbindung der BürgerInnen; Wachstum, Ökologie und Demokratie – miteinander verbinden und mittels Digitalisierung und Technologie zusammenführen.

Technologische Lösungen, die dabei entstehen – miteinander kommunizierende Sensoren in öffentlichen wie privaten Bereichen, die fortwährend Daten bereitstellen, BürgerInnen, die selbst ihre Bedürfnisse und Wissen einspeisen, Konzerne, die ihre Produkte „mit“ den BürgerInnen entwickeln, Verwaltungen, welche zielgenauer entscheiden, Algorithmen, welche Daten, Bedürfnisse und Angebote aufbereiten – sind, so das Versprechen, besser in der Lage, Krisen zu bewältigen, ohne dass dies bedeutet, dass Menschen in ihrer Lebensqualität eingeschränkt werden. Für die BürgerInnen bedeutet dies, so die Annahme, ein Demokratiever sprechen: dass sie stärker und passgenauer beteiligt werden, da ihr Leben in größerem Maße (über Datensammlung und Partizipationsmöglichkeiten) in die Entscheidungsfindung einfließt. Für die Bewältigung von Krisen bedeutet dies ein Effizienz- und Nachhaltigkeitsversprechen: dass mehr Wissen, Hintergrunddaten, Synergiepotenziale und Lösungsansätze gemeinsam analysiert werden können, ohne dass die BürgerInnen Einbußen in ihrem Lebenswandel hinnehmen müssen. Für die Wirtschaft bedeutet dies ein Innovationsversprechen: dass ihnen einerseits ein viel größerer Zugang zur Stadt und deren BewohnerInnen als Testlabor und Datenreservoir eingeräumt wird – und sie andererseits in der Stadt einen Markt für ihre Produkte erschließen. Für die Politik bedeutet dies, die Postulate Demokratie, Nachhaltigkeit, Effizienz und Innovation in der Überschrift Smart City zusammen führen zu können. Anders als unter anderen Überschriften – wie etwa Nachhaltigkeit – schwingt dabei allerdings nicht die Gefahr einer Beschränkung von individueller Selbstverwirklichung und den damit verknüpften Konsum- und Lebensstilen mit.

### 3 Konzeptionelle Grundlagen

Auch wenn annähernd zwei Drittel der bis 2012 zum Thema Smart City veröffentlichten Literatur einen theoretischen und definitorischen Charakter besitzen, hat dies bislang nicht zu einer konzeptuellen Klarheit des Begriffs geführt: Fast sämtliche Forschungsarbeiten betonen unisono das Nebulöse und Undefinierte des Begriffs – und damit auch aller Folgefragen zu Selbstverständnis, Umsetzung und Erfolgsmessung (Cocchia 2014). Eine damit einhergehende Schwierigkeit ist auch, dass sich die Forschungsliteratur zu Smart Cities dieser Unbestimmtheit selbst kaum entziehen kann und oftmals wenig konkret bleiben muss. Viele konkurrierende Konzeptualisierungen stehen nebeneinander – die meisten allerdings stellen die technologischen und digitalen Vernetzungsaspekte ins Zentrum (Batty et al. 2012) und unterscheiden sich darin, ob überhaupt und inwiefern daneben Lebensqualität allgemein, die Qualität öffentlicher Dienstleistungen, Demokratieentwicklung oder aber Ressourcenverbrauch und Nachhaltigkeit eine Priorität eingeräumt wird. Zwei grundsätzliche Forschungsrichtungen können dabei unterschieden werden.

In vielen vergleichenden Projekten ist die Entwicklung von Smart Cities zum Gegenstand empirischer Untersuchungen gemacht worden, vor allem auch durch Forschungsförderungen der Europäischen Union. Ziel ist es dabei zumeist nicht, die sozialwissenschaftlichen oder philosophischen Grundlagen der Auswirkungen von Digitalisierung auf die städtischen Verwaltungen und Institutionen zu analysieren, sondern Best-Practice-Beispiele zu sammeln und sowie über die Bündelung von Parametern einer Smart City Indikatoren für Städtevergleiche zu gewinnen (Giffinger et al. 2007). Es geht primär darum, Instrumente zum Städtewettbewerb bzw. für eine Einschätzung bereitzustellen, wie stark die Smart-City-Werdung bereits vorangeschritten ist. Dabei sollen aber auch Felder definiert werden, in denen noch Nachholbedarf besteht oder aber ein Alleinstellungsmerkmal zu beobachten ist. Die Perspektive richtet sich häufig auf städtische „Leuchttürme“, was heißt, dass die meisten Forschungsprojekte entweder selbst eine explorative Praxis evaluieren oder aber verschiedene Aktivitäten nach ihrem innovativen Charakter reihen (Bac-carne et al. 2014). Das Prinzip des Rankings jedenfalls nimmt in vielen Studien zur Smart City einen zentralen Raum ein. Ob und wo genau eigentlich eine Steigerung der Lebensqualität stattfindet und nach welchen Kriterien diese zu beurteilen ist, wird kaum zum Gegenstand gemacht. Dies hat auch damit zu tun, dass ein Großteil der Forschung zu Smart Cities entweder unter Beteiligung oder auf Initiative von Industrie- und Technologiekonzernen stattfindet (Riesenecker-Caba 2016), deren Perspektive naturgemäß eine wenig sozialwissenschaftliche ist (Ausnahmen bilden etwa Martin et al. 2018; Bauriedl und Strüver 2018; Deakin 2014).

Das Zusammengehen in Public-Private-Partnerships und die Orientierung an Leuchtturmprojekten sind denn auch zwei wesentliche Merkmale des Forschungsstandes, der sich im weiteren auf den Vergleich technologischer Entwicklungspfade und Wachstumspotenziale konzentriert (Giffinger et al. 2007; Batty et al. 2012). Dabei werden zumeist Eckpfeiler und Bausteine einer jeweils umfassenden Smart-City-Strategie definiert (den Kern bilden oft die Felder Ökonomie, Governance, Mobilität, BürgerInnen, Ökologie etc.), welche dann auf ihren Vernetzungs- und

Digitalisierungsstand hin untersucht werden (Riesenecker-Caba 2016). Der Vergleich (und damit der Wettbewerb), wie weit eine Stadt schon auf dem Weg zur Smartness vorangeschritten ist, und die Entwicklung und Begründung weiterer Digitalisierungs- wie Technologieprojekte in Verbindung mit den beteiligten Industriepartnern steht dabei im Vordergrund.

In einem weiteren Strang der Forschung wird diese Fixierung auf die technologische Entwicklung einerseits sowie die implizite Übernahme wettbewerbszentrierter und neoliberaler Stadtentwicklungserspektiven andererseits bei gleichzeitiger Vernachlässigung ökologischer wie sozialer Entwicklungsziele aus der Perspektive der *Stadtsoziologie* und *Demokratieforschung* kritisiert (March 2018; Glasmeier und Christopherson 2015; Vanolo 2014; Deakin 2014; Hollands 2008). Mit Verweis auf arabische und asiatische Smart-City-Strategien werden die Gefahren einer umfassenden Überwachung und Kontrolle der BürgerInnen herausgehoben, die durch die Digitalisierung erst ermöglicht werden (Eichenmüller und Michel 2018). Diese Ambivalenz zeichnet Smart Cities aus: Dieselben Mittel und Technologien, welche den Kern der Versprechen von Innovation, Wachstum, Nachhaltigkeit und Demokratie ausmachen, mögen ebenso für Kontrolle, Überwachung und Manipulation der Stadtbewohner stehen. Sensoren, die Bewegungsprofile, Verkehrsströme oder Gesichter im öffentlichen wie privaten Raum aufzeichnen, die Energie- und Datenverbrauch messen sowie den Bedarf an Informations- wie Konsumgütern ableiten, eignen sich nicht nur, um Verteilungsprobleme effizient zu managen, sondern eben auch, um Informationen über BürgerInnen zu sammeln oder Oppositionsbewegungen zu bekämpfen.

Der zweite Kritikpfeiler an der „smarten“ Stadt ist das technikfixierte und wachstumszentrierte Verständnis von Lebensqualität, das von den Geschäftsinteressen großer Konzerne befeuert wird (Martin et al. 2018). Ökologie, Ressourcenschonung, Engagement und Partizipation blieben lediglich, so das Argument, beschönigende Begleitmusik, ohne die grundlegenden Prämissen von Wachstum und Wirtschaftskraft infrage zu stellen. Das Versprechen, Wachstum, Demokratie und Nachhaltigkeit zu maximieren, ohne dass Menschen sich in ihrem Lebensstil oder Konsum einschränken müssen, führe in der Praxis dazu, dass sozialer Ausgleich und Ökologie als Leitprinzipien permanent zurückstünden (Martin et al. 2018; Viitanen und Kingston 2014).

Das Unbehagen an der „smarten“ Stadt erschöpft sich nicht in der Kritik an einer immer enger werdenden Verknüpfung von Verwaltung und Privatwirtschaft, sondern zielt auch auf die Verschiebung der Perspektive vom Bürger zum Konsumenten, die damit einhergeht, dass Stadt und Verwaltung zwar Beteiligung und Offenheit anbieten, in erster Linie allerdings vorbestimmte und user-freundliche Konsumententscheidungen ermöglichen (Bauriedl und Strüver 2018). Ein technokratischer Überlegenheitsgestus, welcher die BürgerInnen zu Empfängern einer optimierten Vorauswahl von Optionen macht, droht damit auch die dem Konzept Smart City innewohnenden Emanzipations- und Freiheitsversprechen hinter neoliberalen Wachstums- und Wettbewerbsprimaten zurück zu stellen (Martin et al. 2018; Novy 2015). Damit einher geht eine weit fortgeschrittene Individualisierung von digitalisierten Partizipationsformen über Open-Data-Plattformen und digitale Abstimm-

mungsinstrumente, die eine kollektive Organisation politischer Macht erschweren – mit erwartbaren Konsequenzen für eine Vertiefung bereits existierender sozialer Schieflagen bei der Frage, wer in einer Stadt eigentlich politisch aktiv wird und wessen Bedürfnisse Gehör finden. Dies greift Diagnosen aus der Demokratieforschung auf, welche die Individualisierung demokratischer Partizipation sowie die Fokussierung auf eine demokratische Legitimation durch Policy-Output (anstelle einer Input-orientierten Legitimation mittels partizipativer Formate) herausgestellt haben (Streeck 2012; Buchstein und Jörke 2003).

Ein gewichtiges Problem dabei ist, dass Technologie und Digitalisierung zum Nukleus einer Verbesserung von Lebensqualität gemacht werden, ohne aber im Weiteren zu definieren, was genau eigentlich der Wert ist, der gesteigert werden soll. Der Wert von Smartness für die beteiligten BürgerInnen wird in solchen Konzepten rasch und oftmals kurzsichtig mit Wachstum und Innovation durch Digitalisierung übersetzt (Viitanen und Kingston 2014). So kommt es zu einem Widerspruch zwischen einem effizienten Datensammeln und einem Beteiligungs-Empowerment, bei dem die Selbstorganisation der BürgerInnen zum Ziel stadtpolitischen Handelns wird. Folgerichtig betonen Martin et al. (2018) und March (2018), dass die Potenziale, via einer Smart-City-Strategie eine nachhaltige Steigerung der urbanen Lebensqualität zu sichern, entscheidend davon abhängen, in welcher Form a) etablierte gewinn- und wachstums-zentrierte Perspektiven auch in den Stadtverwaltungen infrage gestellt und durch offenere, stärker soziale und ökologische Entwicklungsziele ersetzt werden sowie b) digitale Partizipationsformen nicht auf BürgerInnen als Konsumenten hin ausgerichtet werden, sondern eine soziale Unterschiede ausgleichende Ermutigung und Ermächtigung ermöglichen sollen, bei denen digitale Formate nicht Ziel an sich, sondern dienendes Mittel zum Zweck sind.

---

## 4 Verbreitung und Wirkungen

2014 waren bereits 90 % aller EU-Großstädte mit über einer halben Millionen Einwohner dabei, in verschiedenem Umfang Smart-City-Strategien umzusetzen; bei den EU-Großstädten mit über 100.000 Einwohnern waren es immerhin schon 51 %. Aber auch außerhalb Europas, wo ein Großteil entsprechender Projekte verortet werden kann, geht diese Entwicklung mit Riesenschritten voran: In Indien sollen bis 2022 über einhundert Städte zu digital vernetzten und gesteuerten Smart Cities werden, zum Teil gar als komplette Neubauten (Eichenmüller und Michel 2018; Novy 2015), knapp dreihundert in China. Die öffentlichen Investitionen jedenfalls, die getätigt werden, um Städte digital und smart werden zu lassen, erscheinen gewaltig: Schätzungen zufolge wird der globale Smart-City-Markt im Jahre 2022 etwa 1,56 Billionen US-Dollar wert sein (Martin et al. 2018). Es ist nicht zu übersehen, dass der Topos smart als Legitimität stiftende Entwicklungsparole genutzt wird, die eine geplante, geordnete und zukunftssichere Prosperität garantieren soll. Gleichwohl zeigen Beispiele aus autoritär regierten Ländern, wie stark sich digitale Technologien zu einer immer effizienteren Überwachung und Kontrolle von

BürgerInnen einsetzen lassen – und wie sehr Technologiekonzerne auch diese Entwicklungen als ein lukratives Geschäftsfeld betrachten.

Umsetzungen von Smart-City-Strategien gibt es dabei in ebenso großer Heterogenität wie der Reichtum konzeptueller Definitionen andeutet. Es gibt umfassende, top-down geplante und orchestrierte Umsetzungsstrategien ebenso wie solche, die zunächst un gekoppelt wachsen, eher bottom-up orientierte Ansätze von einzelnen Unternehmen, Abteilungen der Administration oder gar Bürgerinitiativen, welche moderne Technologien und die Digitalisierung zur Verbesserung der Lebensqualität nutzen wollen, die dann aufgegriffen und in ein mehr oder weniger stringentes Gesamtkonzept eingefügt werden. Dazu gehört mitunter auch, dass durch Industrieverbände in Partnerschaft mit staatlichen Institutionen Anreize – beispielsweise durch Wettbewerbe und Förderungsausschreibungen – gesetzt werden, um Städten und Stadtverwaltungen Digitalisierungsreformen und Vernetzungen attraktiv zu machen. In Deutschland etwa hat der Branchenverband Bitkom in Verbund mit dem Deutschen Städte- und Gemeindebund den Wettbewerb „Digitale Stadt“ ins Leben gerufen, um hier Öffentlichkeitsarbeit zu leisten und eine zunehmende Vernetzung anzuschieben. Auch hier geht es darum, dass Städte Modellcharakter und Leuchtturmqualität beweisen sollten, und sich mittels eines Konzepts zur digitalen Vernetzung darum bewerben konnten, von einer beträchtlichen Zahl an Technologieunternehmen mit digitalen Dienstleistungen und Netzwerktechnologien ausgestattet zu werden.

Diese Betonung von Synergien geschieht nicht zufällig: Nicht nur Stadtregierungen und Administrations übernehmen das Konzept einer Smart City, sondern es sind vor allem große Technologieunternehmen, die in der Verbindung von Architektur und Städtebau, Digitalisierung und Datenanalyse sowie Verwaltung und Ressourcenschonung einen Markt mit überaus großen Wachstumspotentialen entdecken (Glasmeier und Christopherson 2015). Dass an den meisten derzeitigen Smart-City-Projekten auch eine Vielzahl an Firmen beteiligt ist, die Pilotprojekte mitentwickeln oder Daten über das Verhalten von BürgerInnen sammeln und aufbereiten, kann insofern nicht überraschen. Denn nicht nur der Verkauf von vernetzten Haushaltskomponenten wie Fernseher, Steckdosen, Lampen oder Rasenmäher oder der entsprechenden Software erscheint dabei besonders lohnend, sondern auch und im Besonderen die Aussicht darauf, langfristig und engmaschig Daten, Bewegungs- und Nachfrageprofile der BürgerInnen sammeln zu können und sich darüber auch zu einem unverzichtbaren Partner der Politik zu machen.

---

## 5 Perspektiven für Staat, Stadt und Verwaltung

Für Stadtverwaltungen, Lokalpolitik und Gesetzgeber gilt es in diesem Fall besonders aufmerksam zu sein, um eine digitale Automatisierung von Entscheidungen nicht zu einem depolitisierenden Bumerang werden zu lassen, der am Ende den Spielraum der Demokratie immer enger werden lässt. Bisherige komparative Evaluierungen von Smart-City-Strategien zeichnen jedenfalls ein Bild, welches deutlich mehr Schatten als Licht zeigt, was die gleichzeitige Verwirklichung von Demokratie,

Nachhaltigkeit und Prosperität anbelangt (Martin et al. 2018; Viitanen und Kingston 2014). Denn die Ambivalenz von Smart Cities, auf der einen Seite mittels Digitalisierung und Vernetzung Innovation, Wachstum, Nachhaltigkeit und Demokratie zu versprechen, mag auf der anderen Seite rasch in eine größere Kontrolle und Überwachung der StadtbewohnerInnen münden. Insofern gilt es für BürgerInnen sowie für politische Akteure, einerseits sehr genau hinzuschauen, auf welcher Grundlage und mit welchem Ziel Vernetzung und Digitalisierung ins Auge gefasst werden – und auf der anderen Seite nicht in Gefahr zu geraten, neue gesellschaftliche Spaltungen gerade durch Digitalisierungsprozesse entstehen zu lassen. Dieselben Potenziale, welche durch Transparenz und Offenheit mehr Partizipationsmöglichkeiten und Demokratisierung für einige sicherstellen sollen, mögen für andere soziale Gruppen einen weiteren Ausschluss bedeuten.

Insofern werden die Aussichten, mittels einer Smart-City-Strategie eine nachhaltige Steigerung der urbanen Lebensqualität zu erreichen, auch davon abhängen, inwieweit sich Stadtverwaltungen und Administrationen in der Tat auf die Lebensqualität der BürgerInnen als zentralen Messwert einlassen und die verlockende Hochglanzfassade einer technologie-, wachstums- und gewinnorientierten Modernisierung hinterfragen. BürgerInnen nicht als Konsumenten zu verstehen, sondern als handelnde Akteure, von denen viele zu einem demokratischen Einnischen aktiv befähigt werden müssen, mag dabei ein Schlüsselprozess sein. Die Digitalisierung und Vernetzung können dabei helfen. Ein Selbstzweck aber, so unterstreicht der Stand der Forschung eindrucksvoll, sind sie keineswegs.

---

## Literatur

- Baccarne, Bastiaan, Peter Merchant, und Dimitri Schuurman. 2014. Empowered cities? An analysis of the structure and generated value of the smart city Ghent. In *Smart city: How to create public and economic value with high technology in urban space*, Hrsg. Renata Paola Dameri und Camille Rosenthal-Sabroux, 157–182. Cham: Springer.
- Batty, Michael, Kay W. Axhausen, Fosca Giannotti, Alexei Pozdnoukhov, Armando Bazzani, Mónica Wachowicz, Georgios Ouzounis, und Yuval Portugali. 2012. Smart cities of the future. *The European Physical Journal Special Topics* 214(1): 481–518. <https://doi.org/10.1140/epjst/e2012-01703-3>.
- Bauriedl, Sybille, und Anke Strüver, Hrsg. 2018. Raumproduktion in der digitalisierten Stadt. In *Smart City. Kritische Perspektiven auf die Digitalisierung in Städten*, 11–30. Bielefeld: transcript.
- Buchstein, Hubertus, und Dirk Jörke. 2003. Das Unbehagen an der Demokratietheorie. *Leviathan* 31(4): 470–495. <https://doi.org/10.1007/s11578-003-0027-8>.
- Coccia, Annalisa. 2014. Smart and digital City. A systematic literature review. In *Smart city: How to create public and economic value with high technology in urban space*, Hrsg. Renata Paola Dameri und Camille Rosenthal-Sabroux, 13–43. Cham: Springer.
- Deakin, Mark. 2014. Smart cities. The state-of-the-art and governance challenge. *Triple Helix* 1(7): 1–16. <https://doi.org/10.1186/s40604-014-0007-9>.
- Eichenmüller, Christian, und Boris Michel. 2018. Smart Cities in Indien. Fortschreibung einer Geschichte modernistischer Stadtplanung. In *Smart City. Kritische Perspektiven auf die Digitalisierung in Städten*, Hrsg. Sybille Bauriedl und Anke Strüver, 99–108. Bielefeld: transcript.
- Giffinger, Rudolf, Christian Fertner, Hans Kramar, Robert Kalasek, Natasa Pichler-Milanovic, und Evert Meijers. 2007. Smart cities. Ranking of European medium-sized cities. Wien: Forschungs-

- bereich Stadt- und Regionalforschung/Technische Universität Wien. [http://www.smart-cities.eu/download/smart\\_cities\\_final\\_report.pdf](http://www.smart-cities.eu/download/smart_cities_final_report.pdf). Zugegriffen am 06.11.2019.
- Glasmeier, Amy, und Susan Christopherson. 2015. Thinking about smart cities. *Cambridge Journal of Regions, Economy and Society* 8(1): 3–12. <https://doi.org/10.1093/cjres/rsu034>.
- Hollands, Robert G. 2008. Will the real smart city please stand up? *City* 12(3): 303–320. <https://doi.org/10.1080/13604810802479126>.
- March, Hug. 2018. The smart city and other ICT-led techno-imaginaries. Any room for dialogue with degrowth? *Journal of Cleaner Production* 197(1): 1694–1703. <https://doi.org/10.1016/j.jclepro.2016.09.154>.
- Martin, Chris J., James Evans, und Andrew Karvonen. 2018. Smart and sustainable? Five tensions in the visions and practices of the smart-sustainable city in Europe and North America. *Technological Forecasting and Social Change* 133:269–278. <https://doi.org/10.1016/j.techfore.2018.01.005>.
- Novy, Johannes. 2015. Smart Citys. Wunsch oder Alptraum? *Politische Ökologie* 142:46–52.
- Riesenecker-Caba, Thomas. 2016. „Smart Cities“. Eine technologische und datenschutzrechtliche Einschätzung. Wien: Kammer für Arbeiter und Angestellte für Wien. [https://wien.arbeiterkammer.at/service/studien/stadtpunkte/Stadtpunkte\\_21.pdf](https://wien.arbeiterkammer.at/service/studien/stadtpunkte/Stadtpunkte_21.pdf). Zugegriffen am 06.11.2019.
- Rosol, Marit, Gwendolyn Blue, und Victoria Fast. 2018. „Smart“, aber ungerecht? Die Smart-City-Kritik mit Nancy Fraser denken. In *Smart City. Kritische Perspektiven auf die Digitalisierung in Städten*, Hrsg. Sybille Bauriedl und Anke Strüver, 87–98. Bielefeld: transcript.
- Streeck, Wolfgang. 2012. Citizens as customers. Considerations on the new politics of consumption. *New Left Review* 76:27–47.
- Vanolo, Alberto. 2014. Smart mentality. The smart city as disciplinary strategy. *Urban Studies* 51(5): 883–898. <https://doi.org/10.1177/0042098013494427>.
- Viitanen, Jenni, und Richard Kingston. 2014. Smart cities and green growth. Outsourcing democratic and environmental resilience to the global technology sector. *Environment and Planning A: Economy and Space* 46(4): 803–819. <https://doi.org/10.1068/a46242>.



---

# Digitale Polizeiarbeit

Constantin Houy, Oliver Gutermuth, Sharam Dadashnia und  
Peter Loos

## Inhalt

1 Einleitung .....	518
2 Klärung des Begriffs .....	518
3 Theoretische und konzeptionelle Grundlagen .....	520
4 Ausgewählte praktische Anwendungen .....	522
5 Umsetzungsstand und Auswirkungen .....	522
6 Künftige Entwicklungen .....	524
Literatur .....	525

---

## Zusammenfassung

Aus der fortschreitenden Digitalisierung alltäglicher Aktivitäten ergeben sich erhebliche Potenziale, aber auch Herausforderungen für die Polizeiarbeit. Einerseits können elektronische Hilfsmittel die Erfüllung der Aufgaben erheblich erleichtern, andererseits rüsten auch Kriminelle technologisch beständig auf. Die Bekämpfung der Kriminalität dürfte auch im digitalen Zeitalter einem Wettlauf zwischen Hase und Igel ähneln, da die Polizei auf einige Instrumente verzichten muss, die technologisch verfügbar sind, während Straftäter sich jede neue Methode aneignen können und dies auch tatsächlich tun. Besonders umstritten sind u. a. Techniken zur automatisierten Bild- und Videoanalyse sowie die sogenannte vorhersagende Polizeiarbeit, welche zwar die Einsatzplanung unterstützen, aber auch zur Diskriminierung von Personen führen kann.

---

C. Houy (✉) · O. Gutermuth · P. Loos

Institut für Wirtschaftsinformatik (IWi), DFKI GmbH und Universität des Saarlandes, Saarbrücken, Deutschland

E-Mail: [Constantin.Houy@dfki.de](mailto:Constantin.Houy@dfki.de); [Oliver.Gutermuth@dfki.de](mailto:Oliver.Gutermuth@dfki.de); [Peter.Loos@dfki.de](mailto:Peter.Loos@dfki.de)

S. Dadashnia

Scheer GmbH, Saarbrücken, Deutschland

E-Mail: [Sharam.Dadashnia@scheer-group.com](mailto:Sharam.Dadashnia@scheer-group.com)

## Schlüsselwörter

Künstliche Intelligenz · Predictive Policing · Mobile Policing · Internetkriminalität · Darknet

---

## 1 Einleitung

Staat und Verwaltung sehen sich im digitalen Zeitalter mit der Herausforderung konfrontiert, die Potenziale und Chancen, welche sich aus der Digitalisierung ergeben, für ihre speziellen Belange zu erschließen. Für die Arbeit der Polizei – als Exekutivorgan des Staates – hat die fortschreitende Digitalisierung des öffentlichen, aber auch des privaten Bereiches, vielseitige Implikationen. Einerseits stehen der Polizei durch die zunehmende Verfügbarkeit leistungsfähiger Informations- und Kommunikationssysteme sowie gängiger Anwendungskonzepte aus den Bereichen Informationsmanagement, *Künstliche Intelligenz* und maschinelles Lernen zunehmend Werkzeuge zur Verfügung, ihre Aufgaben – wie die Kriminalitätsbekämpfung und -prävention, Gefahrenabwehr oder Aufklärungs- und Informationsarbeit – erfolgreich und effizient zu erledigen. Andererseits ermöglichen das *Internet* und die zunehmende Digitalisierung auch neue Formen der Kriminalität (Münch 2017). Beispiele sind das sogenannte *Phishing* zur Erlangung von Bankdaten, aber auch der Drogen- oder Waffenhandel im sogenannten *Darknet*. Durch die Digitalisierung ergeben sich für die Polizei somit neue Herausforderungen, aber auch neue Chancen (Rüdiger und Bayerl 2018).

---

## 2 Klärung des Begriffs

*Digitalisierung* ist kein eindeutig belegter Terminus. Grundsätzlich beschreibt dieses Schlagwort zunächst einen Transformationsprozess bezüglich analoger Daten – im Sinne von Befunden, Werten oder Angaben, die durch Beobachtung oder Messung erhoben werden können –, welche in eine digitale, d. h. mit Informations- und Rechnertechnik verarbeitbare Repräsentationsform überführt werden. Aktuell wird der Begriff allerdings eher im Sinne einer gesellschaftlichen Umbruchphase bzw. eines Transformationsprozesses verwendet („*digitale Revolution*“), in dem sämtliche Lebensbereiche (Wirtschaft, Arbeit, Politik und Gesellschaft, Privatleben) von den Möglichkeiten und den Herausforderungen der digitalen Rechnertechnik und des Internets beeinflusst und durch deren Präsenz geprägt werden.

Innerhalb Deutschlands existieren verschiedene Polizeien. Der Bundespolizei (früher: Bundesgrenzschutz) obliegen die Überwachung der Grenzen und des grenzüberschreitenden Verkehrs (insbesondere auch bei der Bahn), die Sicherung des Luftverkehrs, der Schutz von Verfassungsorganen und andere Aufgaben. Das Bundeskriminalamt (BKA) koordiniert gemeinsam mit den Landeskriminalämtern die Verbrechensbekämpfung in Deutschland und es ermittelt in Fällen, in denen ein

Auslandsbezug besteht. Es fungiert auch als zentrale Stelle für ein übergreifendes Informationsmanagement. Des Weiteren ist es Aufgabe des BKA, Mitglieder der Verfassungsorgane des Bundes zu schützen, und es repräsentiert darüber hinaus die Bundesrepublik Deutschland bei *Interpol*, der internationalen Organisation der Kriminalpolizeien, bzw. beim europäischen Pendant *Europol*. Die Bereitschaftspolizeien des Bundes und der Länder sind für länderübergreifende Großeinsätze zuständig.

Auf Landesebene sind grundsätzlich zu unterscheiden:

- a.) die *Schutzpolizei*, die für die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung, die Kriminalprävention, die Erfassung gesetzeswidriger Handlungen oder auch die Ahndung von Ordnungsdelikten zuständig ist, sowie
- b.) die *Kriminalpolizei*, die sich vor allem um die Verhütung und Verfolgung von Straftaten, insbesondere um schwerwiegende Straftaten, wie zum Beispiel Kapitalverbrechen (Raub, Erpressung, Tötung, etc.) kümmert und für Delikte im Bereich der Wirtschaftskriminalität, aber auch für die Suche nach Vermissten zuständig ist.

Bei allen Aufgaben von Schutzpolizei und Kriminalpolizei können digitale Instrumente nützlich sein (Siller 2017):

- *Verkehrsdienst* (Unfallaufnahme, Verkehrskontrollen, Schulwegsicherung, etc.),
- *sicherheitspolizeiliche Aufgaben* (Streifendienst zur Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit, Streitschlichtung und Schutz vor Gewalt in der Familie, Hilfeleistung, Betreuung von Veranstaltungen, z. B. Sportveranstaltungen oder Kundgebungen),
- *Kriminaldienst* (Aufnahme von Strafrechtsdelikten wie zum Beispiel von Diebstählen, Sachbeschädigung, Körperverletzung, Tatortarbeit mit Spurenabsicherung, Erstellen von Spurenabsicherungsberichten, Fahndung, etc.),
- Prävention von Straftaten (vor allem Einbruch und Diebstahl sowie Internetkriminalität, etc.),
- Konfliktlösung und Beziehungsarbeit (z. B. innerhalb einzelner Wohnviertel, im Kontakt mit Jugendlichen, etc.).

Unter *digitaler Polizeiarbeit* ist somit die informationstechnische bzw. internetbasierte Unterstützung sämtlicher polizeilicher Aufgaben auf Bundes- und Landesebene sowie der damit verbundenen Arbeits-, Informations-, Kommunikations- und Interaktionsprozesse zu verstehen. In diesem Kontext ist es auch nötig, wichtige Arbeitsmittel, wie Formulare oder Fallakten, in digitaler Form zu nutzen, um die polizeiliche Informationslogistik zu verbessern. Der elektronische Informationsaustausch der Polizeien von Bund und Ländern, aber auch über die Grenzen hinaus, ist im digitalen Zeitalter unverzichtbar. Gerade in der internationalen Polizeiarbeit bestehen bei der digitalen Kommunikation, Koordination und Kooperation noch erhebliche Entwicklungs- und Ausbaupotenziale.

### 3 Theoretische und konzeptionelle Grundlagen

Digitale Polizeiarbeit ist ein intensiv diskutiertes, nicht selten hochgradig strittiges Thema mit vielen Facetten. Im Rahmen der Betrachtung der Effizienz und Effektivität von Aktivitäten spielen allgemeine betriebswirtschaftliche Theorien bzw. organisationstheoretische Ansätze zur Beurteilung verschiedener Aspekte der digitalen Polizeiarbeit eine Rolle. Von Bedeutung hierbei sind u. a. Erkenntnisse der *Transaktionskostentheorie*, des *Ressourcenorientierten Ansatzes* oder auch der *Motivationstheorie*, welche relevante organisatorische Rahmenbedingungen oder persönliches menschliches Handeln und seine Auswirkungen bei der Nutzung von IT in der Polizeiarbeit beschreiben, erklären oder auch prognostizieren können. Des Weiteren sind im konkreten Gegenstandsbereich der Polizeiarbeit verschiedene theoretische Ansätze von Bedeutung, wie zum Beispiel die sogenannte *Broken-Window-Theorie*, die einen Zusammenhang zwischen dem Verfall von Gebäuden in bestimmten Gebieten einer Stadt und der dort festzustellenden Kriminalitätsrate beschreibt. Im unten noch näher beschriebenen Anwendungsfeld der *vorhersagenden Polizeiarbeit (Predictive Policing)* spielt u. a. auch der sogenannte *Routine-Activity-Ansatz* (Cohen und Felson 1979) eine Rolle, der das Zustandekommen einer Straftat mit der Gegebenheit von drei Faktoren erklärt: a.) Es existiert ein geeignetes Ziel einer Straftat. b.) Es besteht ein Mangel an Schutz, der die Straftat verhindern könnte. c.) Es existiert ein motivierter Täter. Eine weitere relevante theoretische Grundannahme, die in der vorhersagenden Polizeiarbeit eine Rolle spielt, bietet das häufig zu beobachtende *Near-Repeat-Victimisation*-Phänomen, wonach bestimmte Straftaten (z. B. Wohnungseinbrüche) in einem Gebiet in absehbarer Zeit ähnliche Folgetaten wahrscheinlich werden lässt. Es existieren auch hier weitere theoretische Modelle und empirisch breit gestützte Zusammenhänge zur Beschreibung, Erklärung und ggf. Prognose von beobachtbaren Sachverhalten.

Konzeptionell lässt sich das Feld der digitalen Polizeiarbeit anhand folgender Aspekte fassen und beschreiben (Rüdiger und Bayerl 2018): (a.) *Kommunikation und Interaktion mit den Bürgerinnen und Bürgern*, (b.) *Kriminalitätsprävention und -bekämpfung*, (c.) *organisatorische Aspekte* und (d.) *rechtliche Fragen*.

(a.) *Kommunikation und Interaktion mit den Bürgerinnen und Bürgern*: Ein Bereich, welcher insbesondere aufgrund der zunehmenden Nutzung *sozialer Medien (Social Media)*, wie *Facebook* oder *Twitter*, in Deutschland für die Polizeiarbeit immer mehr an Bedeutung gewinnt, ist die digitale Kommunikation und Interaktion mit Bürgern über Kanäle, die ihnen im Alltag vertraut sind (*Facebook*, *Messenger-Dienste* etc.). Die Nutzung dieser Kanäle kann nicht nur die polizeiliche Außenwirkung positiv beeinflussen, sondern auch in akuten Krisensituationen zur raschen Verbreitung von Informationen und damit womöglich zu geringeren Schäden beitragen. Die Kommunikation der Polizei mit den Bürgerinnen und Bürgern über *Twitter* und *Facebook* während des Münchner Amoklaufs im Sommer 2016 hat z. B. zu einem positiven Medienecho

geführt. Negative Reaktionen, Kritik und umfangreiche Diskussionen in sozialen Netzwerken gab es hingegen nach dem sogenannten „Nafri“-Tweet der Kölner Polizei, in dessen Rahmen die intern verwendete Abkürzung „Nafri“ (für „Nordafrikaner“) für die externe Kommunikation verwendet wurde. Die Nutzung moderner Arbeitsgeräte wie *Smartphones* oder *Tablets* – anstelle von Block und Bleistift – kann darüber hinaus den Eindruck einer modernen, technisch gut ausgestatteten Polizei vermitteln.

- (b.) *Kriminalitätsprävention und -bekämpfung:* Hierfür stehen inzwischen IT-Lösungen zur Verfügung, die sich Künstlicher Intelligenz bedienen. Beispiele dafür sind unter anderem Anwendungen der sogenannten *vorhersagenden Polizeiarbeit (Predictive Policing)*, intelligente Videoanalyseverfahren (u. a. die biometriebasierte forensische Personensuche) (Eigenseer et al. 2018) oder auch Ansätze zur Bekämpfung und Aufdeckung von *Cybercrime* bzw. Computerkriminalität (Sowa und Silberbach 2018) bzw. zur Erhöhung der *Cybersicherheit*. Die Daten, die dafür genutzt werden, können aus den Informationssystemen von Polizeibehörden, aber auch aus externen Quellen stammen. Im Rahmen von „Internet-Streifen“ in sozialen Medien können Beleidigungen, Hasscommentare oder das Verbreiten von Gerüchten aufgespürt und verfolgt werden. Die Polizei kann aber auch versuchen, Personen zu identifizieren, die Straftaten ankündigen oder im Internet Kontakte zu Kriminellen unterhalten. *Messenger*-Dienste wie *WhatsApp* können in verschiedenen Ermittlungsphasen von Bedeutung sein, etwa bei der Sicherung von Beweisen.
- (c.) *Organisatorische Aspekte:* Neben der technischen Infrastruktur und zeitgemäßer *Hardware* und *Software* müssen für eine erfolgreiche digitale Polizeiarbeit IT-Kompetenzen vorhanden sein. Da inzwischen die Generation der sogenannten *Digital Natives* in die Polizeiarbeit hineinwächst, kann von einer zunehmenden IT-Affinität innerhalb des Personals ausgegangen werden. Umgekehrt entsteht dadurch allerdings auch eine gewisse Erwartungshaltung gegenüber erfahreneren Beamtinnen und Beamten, die IT-Infrastruktur und digitale Services ebenso selbstverständlich einzusetzen. Bei IT-Spezialisten konkurrieren die Polizeien allerdings, wie die öffentliche Verwaltung insgesamt, mit privaten Arbeitgebern, die meist eine bessere Vergütung bieten können. Eine nahtlose Integration digitaler Instrumente in die polizeilichen Arbeitsprozesse setzt zudem voraus, diese vorab zu optimieren. Nur dann können deren Potenziale wirklich ausgeschöpft werden. Dazu könnte auch eine Anpassung von Vorschriften gehören.
- (d.) *Rechtliche Fragen:* Wenn die Polizei Daten aus sozialen Netzwerken zur Erfüllung ihrer Aufgaben nutzen möchte, dann bedarf es dafür einer Ermächtigungsgrundlage. Das gilt für alle ihre Eingriffe in Rechte der Bürgerinnen und Bürger. Ab wann solche Maßnahmen, etwa der Einsatz von „Staatstrojanern“ auf privaten Rechnern, tatsächlich gerechtfertigt sind, ist Gegenstand intensiver Diskussionen (Krischok 2018; siehe auch Kap. ► „Der Staat als Hacker“ in diesem Handbuch).

## 4 Ausgewählte praktische Anwendungen

Die praktischen Möglichkeiten digitaler Polizeiarbeit sind sehr vielfältig. Im folgenden Abschnitt werden zwei ausgewählte Anwendungskonzepte illustriert.

*Vorhersagende Polizeiarbeit (Predictive Policing):* Bei der Verhinderung von Straftaten und der Bekämpfung von Verbrechen spielt die „vorhersagende Polizeiarbeit“ (*Predictive Policing*) eine besondere Rolle (Bode et al. 2017). Basierend auf statistischen Daten früherer Vorfälle werden Prognosen erstellt, mit welcher Wahrscheinlichkeit an welchen Orten erneut ähnliche Vorfälle auftreten könnten. Solche Modelle, die auf einem ständigen Evaluieren, Bewerten und Rückmelden von Erkenntnissen basieren, können die Planung von Streifen oder präventive Maßnahmen erheblich erleichtern. Vorhersagende Polizeiarbeit stützt sich auf verschiedene sozialwissenschaftliche Theorien bzw. Thesen, wie die oben bereits eingeführte *Broken-Window-Theorie*, den *Routine-Activity-Ansatz*, oder das *Near-Repeat-Victimisation*-Phänomen. Die Steigerung der Polizeipräsenz in relevanten Gegenden kann kriminellem Verhalten entgegenwirken. Während in der Frühphase der Entwicklung von *Predictive-Policing*-Ansätzen und im Rahmen von *Proof-of-Concept*-Projekten erwähnenswerte Erfolge verzeichnet werden konnten, wird die Methode inzwischen aus verschiedenen Gründen häufiger in Frage gestellt. Kritisch gesehen wird, dass statistische Analysen Menschen aufgrund bestimmter äußerlicher Merkmale diskriminieren können, was der Unschuldsvermutung widersprechen würde, die vor Gericht als zentrales Grundprinzip eines rechtsstaatlichen Strafverfahrens gilt.

*Mobile digitale Polizeiarbeit (Mobile Policing):* Mit diesem Begriff wird der Einsatz mobiler Geräte im Außeneinsatz beschrieben, mit denen Polizeibeamte unabhängig von stationären Systemen kommunizieren, Informationen abrufen bzw. prozessrelevante Daten aufnehmen und an die zentralen Anwendungssysteme der Polizei weiterleiten können (Dadashnia et al. 2017). Anwendungssoftware auf mobilen Endgeräten kann zudem die Nachbereitung von Vorfällen in der Dienststelle unterstützen und doppelte Eingaben vermeiden helfen. In einem *Proof-of-Concept*-Projekt (*VU-App*) erprobte die saarländische Polizei beispielsweise die elektronische Aufnahme und Bearbeitung von Verkehrsunfällen direkt vor Ort. Ähnliche Lösungen sind auch in anderen Bundesländern und in Österreich im Einsatz. Durch den Einsatz mobiler IT lassen sich nicht nur redundante Arbeitsvorgänge, sondern auch Erfassungsfehler und Medienbrüche vermeiden, während die Datenqualität und eine schnelle Verfügbarkeit der Informationen gesteigert werden können. Des Weiteren kann die Polizei dadurch ihre „Präsenz auf der Straße“ erhöhen, weil die Beamtinnen und Beamten weniger verwaltende Tätigkeiten auf der Dienststelle verrichten müssen.

## 5 Umsetzungsstand und Auswirkungen

Während die Datenverarbeitung in der Polizeiarbeit in Deutschland eine lange Historie hat, die bereits weit vor der breiten Nutzung des Internet begann, z. B. im Kontext der unter Horst Herold in den 1970er-Jahren im Bundeskriminalamt einge-

führten Rasterfahndung, hat sich die digitale Polizeiarbeit im oben definierten Sinne in den vergangenen Jahren weiter verbreitet. Dies gilt insbesondere im Kontext mobiler Polizeiarbeit. In einigen Bundesländern werden zunehmend mobile Endgeräte zur Aufnahme von Verkehrsunfällen oder Strafanzeigen eingesetzt, so z. B. in Rheinland-Pfalz. Dort begann nach erfolgreichem Pilotprojekt im Herbst des Jahres 2018 die schrittweise Einführung mobiler Endgeräte mit dem Ziel einer flächendeckenden Verfügbarkeit mobiler Apps für die Polizeiarbeit (Ministerium des Innern und für Sport des Landes Rheinland-Pfalz 2018). In Deutschland kann Rheinland-Pfalz diesbezüglich als einer der Vorreiter bezeichnet werden, da in anderen Bundesländern noch keine mobilen polizeilichen Fachanwendungen in größerem Ausmaß im Einsatz sind. Wie groß die Kosteneinsparungen durch mobile Technologien, die sich in den durchgeführten *Proof-of-Concept-* oder *Pilotprojekten* andeuteten, tatsächlich sind, wird sich in den kommenden Jahren zeigen. Es ist allerdings zu erwarten, dass sich mit zunehmender Verbreitung und Akzeptanz mobiler Anwendungssoftware bei der Polizei auch entsprechende Einsparungen durch mehr Routine bei der Benutzung und eine bessere Prozessorganisation ergeben werden.

Auch hinsichtlich der digitalen Polizeiarbeit im Internet ist eine Zunahme der öffentlich dokumentierten sowie der nichtöffentlichen Aktivitäten zu verzeichnen bzw. anzunehmen. Während in den Medien aktuell immer wieder von entsprechenden Fahndungserfolgen der Polizei berichtet wird, ist allerdings davon auszugehen, dass sich Kriminelle und die Polizei im Internet ein „Katz-und-Maus-Spiel“ liefern, das durch die stetige Weiterentwicklung der technischen Möglichkeiten geprägt ist. Das Bundeskriminalamt geht in aktuellen Kriminalstatistiken nicht nur von einer großen Anzahl unbekannter und nicht zur Anzeige gebrachter Fälle aus (Bundeskriminalamt 2017), sondern verzeichnet auch eine stetig wachsende Anzahl von Straftaten im Internet (Bundeskriminalamt 2018). Eine in ihrer Intensität und in ihrem Umfang zunehmende digitale Polizeiarbeit erscheint somit notwendig, um im Rahmen dieses „Wettrennens“ überhaupt Anschluss an die Aktivitäten Krimineller im Internet halten zu können.

Gegenüber den Ansätzen der vorhersagenden Polizeiarbeit bestanden in den letzten Jahren zwar große Hoffnungen, allerdings ist der polizeiliche Alltag noch weit von einer Umsetzung der gegebenen Möglichkeiten entfernt (Diehl und Kartheuser 2018). Während einige Bundesländer entsprechende Anwendungen aktuell im Rahmen von Pilotprojekten testen bzw. den Einsatz prüfen, werden in Deutschland Techniken der vorhersagenden Polizeiarbeit im Alltag zur Planung präventiver Streifen nur in wenigen Bundesländern genutzt (gemäß der Recherche von Diehl und Kartheuser (2018) bisher in Hessen und Bayern). Andere Bundesländer hegen aktuell keine Pläne zum Einsatz von *Predictive Policing*. Im Gegensatz zur größeren Nutzung solcher Techniken in den USA sind in Deutschland die Vorbehalte in der Bevölkerung und auch bei Kriminalisten gegenüber der vorhersagenden Polizeiarbeit mit Hinweisen auf die Bürger- und Freiheitsrechte, die herrschenden Datenschutzbestimmungen und die allgemein geltende Unschuldsvermutung im Rahmen von Gerichtsverfahren erheblich größer. Kritiker warnen in diesem Kontext insbesondere auch vor den Möglichkeiten und Gefahren des sogenannten *Profiling* – dem Sammeln und Auswerten personenbezogener Daten mit dem Ziel der Erstellung

und Nutzung von Personenprofilen in unterschiedlichen Kontexten. Besonders umstritten sind in diesem Zusammenhang Ideen zur Erstellung personenbezogener Bewertungssysteme (*Scoring*), welche z. B. in Form des sogenannten *Citizen Score* aktuell in China an Bedeutung gewinnen und weiter umgesetzt werden sollen. Solche Systeme können u. a. für eine automatisierte Entscheidungsunterstützung im Rahmen der Strafverfolgung dienen (Krempe 2018). Während solche Ansätze für die Polizeiarbeit in anderen Teilen der Erde durchaus angewandt bzw. erprobt werden, wird deren Vereinbarkeit mit den gesetzlichen Rahmenbedingungen in der Bundesrepublik Deutschland weiterhin intensiv diskutiert und ein weitreichender Konsens dazu ist in nächster Zeit nicht zu erwarten.

---

## 6 Künftige Entwicklungen

Die Nutzung von IT und elektronischen Geräten als digitale Hilfsmittel ist aus der Polizeiarbeit nicht mehr wegzudenken. Die Kommunikation sowie die Interaktion der Polizei mit den Bürgerinnen und Bürgern über digitale Medien dürfen weiter zunehmen. Welche Formen der direkten (beidseitigen) Kontakt aufnahme sich durchsetzen können, bleibt abzuwarten. Die Nutzung von elektronischen Nachrichten zur Verbreitung aktueller Informationen und von Handlungsempfehlungen in Notsituationen oder bei Großveranstaltungen hat sich in der Vergangenheit in verschiedenen Situationen bereits als hilfreich dargestellt. Im Rahmen der Kommunikation und Interaktion der Polizei mit Bürgern über das Internet sind allerdings geeignete Mechanismen zur Sicherstellung der Identität von Bedeutung, um missbräuchliche Nutzung (anonymisiert bzw. unter falscher Identität, z. B. zur Denunziation von Personen) zu verhindern.

Techniken und Konzepte zur Auswertung großer Datenmengen (Stichwort: *Big Data Analytics*) dürfen zukünftig in der Präventionsarbeit und bei der Kriminalitätsbekämpfung eine größere Rolle spielen. Die 2017 gegründete *Zentrale Stelle für Informationstechnik im Sicherheitsbereich* (ZITIS) in München soll die technischen Instrumente entwickeln, welche die Polizei zur Erfüllung ihrer Aufgaben braucht. Gleichwohl werden die Erprobung und Nutzung von IT- und KI-gestützten Ansätzen im Rahmen der Polizeiarbeit aktuell kontrovers diskutiert.

Die Digitalisierung bietet erhebliche Potenziale und Chancen für die Polizeiarbeit der Zukunft. Es bestehen insbesondere organisationale Effizienzpotenziale durch den Einsatz digitaler und mobiler Anwendungssysteme, welche explizit die polizeilichen Arbeitsprozesse beschleunigen und das damit verbundene Informationsmanagement verbessern können. Es kann davon ausgegangen werden, dass mit wachsendem Kostendruck in der öffentlichen Verwaltung trotz der erheblichen notwendigen Investitionen ein zunehmendes Ausschöpfen solcher Effizienzpotenziale vonseiten der Landesregierungen angestrebt wird. Inwiefern das Konzept *Bring-Your-Own-Device* (BYOD) eine Rolle spielen kann, bleibt abzuwarten. In diesem Zusammenhang sind allerdings insbesondere datenschutzrelevante Aspekte zu betrachten und geeignete technische Lösungen für eine geräteunabhängige und sichere Arbeitsumgebung zu entwickeln und zur Verfügung zu stellen.

Die Balance zwischen Freiheit und Sicherheit, also die Frage, wie intensiv und extensiv die Polizei digitale Werkzeuge nutzen und Daten analysieren darf, dürfte auf der Tagesordnung bleiben. Während Kriminelle vermutlich sämtliche verfügbaren Möglichkeiten hinsichtlich Anonymität im Netz und Verschlüsselung nutzen, die das digitale Zeitalter bereithält, darf die Polizei in einem Rechtsstaat nicht alles machen, was technisch denkbar wäre. In den nächsten Jahren wird insofern ein erheblicher Arbeitsaufwand zur Herbeiführung juristischer und politischer Klärungen zu leisten sein, um die Frage zu beantworten, wie sich die Polizei zukünftig aufzustellen muss und welche modernen Instrumente sie künftig zur Erledigung ihrer Aufgaben einsetzen soll.

---

## Literatur

- Bode, Felix, Florian Stoffel, und Daniel Keim. 2017. Variabilität und Validität von Qualitätsmetriken im Bereich von Predictive Policing. [https://kops.uni-konstanz.de/bitstream/handle/123456789/38312/Bode\\_0-402496.pdf?sequence=3&isAllowed=y](https://kops.uni-konstanz.de/bitstream/handle/123456789/38312/Bode_0-402496.pdf?sequence=3&isAllowed=y). Zugegriffen am 01.03.2019.
- Bundeskriminalamt. 2017. Internetkriminalität/Cybercrime. [https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet\\_node.html](https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html). Zugegriffen am 01.03.2019.
- Bundeskriminalamt. 2018. Cybercrime. Bundeslagebild 2017. <https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017.html>. Zugegriffen am 01.03.2019.
- Cohen, Lawrence E., und Marcus Felson. 1979. Social change and crime rate trends: A routine activity approach. *American Sociological Review* 44:588–608.
- Dadashnia, Sharam, Constantin Houy, und Peter Loos. 2017. Mobile Verkehrsunfallerfassung bei der Polizei im Saarland – Zur wissenschaftlichen Begleitforschung des Projektes VU-App. *Veröffentlichungen des Instituts für Wirtschaftsinformatik (IWI) im Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI), IWI-Heft* Nr. 204. [https://www.uni-saarland.de/fileadmin/user\\_upload/Professoren/fr13\\_ProfLoos/IWI-Hefte/IWI-Heft\\_204\\_VU-App\\_1.pdf](https://www.uni-saarland.de/fileadmin/user_upload/Professoren/fr13_ProfLoos/IWI-Hefte/IWI-Heft_204_VU-App_1.pdf). Zugegriffen am 01.03.2019.
- Diehl, Jörg, und Boris Kartheuser. 2018. Predictive Policing. Ich weiß, was du heute tun wirst. [10whhttp://www.spiegel.de/panorama/justiz/kriminalitaet-in-deutschland-polizei-setzt-auf-computer-vorhersagen-a-1188350.html](http://www.spiegel.de/panorama/justiz/kriminalitaet-in-deutschland-polizei-setzt-auf-computer-vorhersagen-a-1188350.html). Zugegriffen am 01.03.2019.
- Eigenseer, Alex Elisabeth, Stephan G. Humer, und Anna Lederer. 2018. Von der konventionellen zur intelligenten Videoüberwachung – Chancen und Risiken für Polizei und Gesellschaft. In *Digitale Polizeiarbeit. Herausforderungen und Chancen*, Hrsg. Thomas-Gabriel Rüdiger und Petra Saskia Bayerl, 147–157. Wiesbaden: Springer.
- Krempel, Stefan. 2018. Predictive Policing: Die Polizei arbeitet verstärkt wie ein Geheimdienst. <https://www.heise.de/newsticker/meldung/Predictive-Policing-Die-Polizei-arbeitet-verstaerkt-wie-ein-Geheimdienst-4008214.html>. Zugegriffen am 01.03.2019.
- Krischok, Heike. 2018. Das Internet in der polizeilichen Gefahrenabwehr. In *Digitale Polizeiarbeit. Herausforderungen und Chancen*, Hrsg. Thomas-Gabriel Rüdiger und Petra Saskia Bayerl, 237–257. Wiesbaden: Springer.
- Ministerium des Innern und für Sport des Landes Rheinland-Pfalz. 2018. Start für flächendeckendes mobiles Arbeiten bei der Polizei. <https://mdi.rlp.de/de/service/pressemitteilungen/detail/news/detail/News/start-fuer-flaechendeckendes-mobiles-arbeiten-bei-der-polizei/>. Zugegriffen am 01.03.2019.
- Münch, Holger. 2017. Polizeiarbeit in digitalen Zeiten – Wie Ermittler und IT-Spezialisten gemeinsam Kriminalität bekämpfen. Manuskript. <https://www.bka.de/SharedDocs/Reden/DE/muench/GastbeitragCebit.pdf>. Zugegriffen am 01.03.2019.
- Rüdiger, Thomas-Gabriel, und Petra Saskia Bayerl, Hrsg. 2018. *Digitale Polizeiarbeit. Herausforderungen und Chancen*. Wiesbaden: Springer.

- 
- Siller, Helmut. 2017. Operatives, strategisches und normatives Management. In *Handbuch Polizeimanagement: Polizeipolitik – Polizeiwissenschaft – Polizeipraxis*, Hrsg. Jürgen Stierle, Dieter Wehe und Helmut Siller, 682–701. Wiesbaden: Springer Gabler.
- Sowa, Aleksandra, und Fred-Mario Silberbach. 2018. Cyber Security Intelligence – Kollaborative Ansätze gegen Cyber- und Computerkriminalität. In *Digitale Polizeiarbeit. Herausforderungen und Chancen*, Hrsg. Thomas-Gabriel Rüdiger und Petra Saskia Bayerl, 109–128. Wiesbaden: Springer.



---

# Der Staat als Hacker

Martin Schallbruch

## Inhalt

1 Begriffsklärung/Problemstellung .....	528
2 Theoretische Grundlagen .....	530
3 Praktische Anwendungsfelder und gesetzliche Grundlagen .....	531
4 Umsetzungsstand und Umsetzungsschwierigkeiten .....	533
5 Perspektiven .....	536
Literatur .....	537

---

## Zusammenfassung

Staatliches Hacking ist im Instrumentarium der deutschen Sicherheitsbehörden angekommen – mit gesetzlichen Befugnissen für Polizeien und einige Nachrichtendienste, mit der Entwicklung entsprechender Technologien („Bundestrojaner“) und ersten Einsatz erfahrungen. Gleichzeitig ist staatliches Hacking mit erheblichen Risiken für die Betroffenen und die Gesellschaft insgesamt verbunden. Staatliches Hacking wird zunehmen und sich verstetigen. Es wird dauerhaft ein zentrales Spannungsfeld zwischen der Förderung von IT-Sicherheit auf der einen und der Durchbrechung von IT-Sicherheit auf der anderen Seite darstellen.

---

## Schlüsselwörter

Verschlüsselung · Computer-Grundrecht · Online-Durchsuchung · Staatliches Hacking · Hack-Back · Schwachstellen

---

M. Schallbruch (✉)  
ESMT Berlin, Berlin, Deutschland  
E-Mail: [martin.schallbruch@esmt.org](mailto:martin.schallbruch@esmt.org)

## 1 Begriffsklärung/Problemstellung

„Hacker“ ist ein schwierig zu fassender Begriff. Er ist in der öffentlichen Meinung und in der Literatur je nach Kontext stark positiv oder stark negativ belegt. Im Allgemeinen versteht man unter Hackern Personen, die in ein Computersystem eindringen, wobei das Eindringen typischerweise über die reine unbefugte Benutzung hinausgeht: eine irgend geartete Überwindung von Sicherheitsmaßnahmen gehört im allgemeinen Verständnis zum Hacking hinzu. Hacking kann Hardwarebausteine zur Manipulation ihrer Funktionsweise oder zum Auslesen von Daten betreffen, das Hacking von Geräten, typischerweise durch Firmware-Manipulation, das Hacking von Betriebssystem- oder Anwendungssoftware von Computern einschließlich Tablets und Smartphones zwecks Übernahme der Kontrolle der Systeme oder auch das Hacking von Servern im Internet, um sie für eigene Zwecke zu nutzen.

Die Motive von Hackern können sehr unterschiedlich sein. Hacking kann zum Zwecke des Überprüfens eigener IT-Systeme, zur kommerziellen oder nichtkommerziellen Sicherheitsprüfung fremder Systeme, aus reinem Spiel- und Abenteuertrieb oder auch zu Zwecken des Ausspähens, Manipulierens oder Zerstörens fremder Systeme erfolgen. Entsprechend dieser unterschiedlichen Intentionen des Hacking differenziert auch die Rechtsordnung. § 202a StGB stellt das unbefugte Eindringen in Systeme unter Überwindung von Sicherheitsmaßnahmen unter Strafe. Ein Penetrationstest eines Unternehmensnetzwerks durch einen Hacker mit Zustimmung des Unternehmens ist nicht unbefugt und damit nicht strafbar. Bei der Strafbarkeit kommt es allerdings nicht (mehr) darauf an, dass tatsächlich Daten abgeschöpft oder Manipulationen vorgenommen werden. Schon das unbefugte Eindringen selbst ist strafbar.

Hacking durch staatliche Behörden wird in der internationalen Debatte als „Lawful Hacking“ bezeichnet und kommt in verschiedenen Bereichen staatlicher Aufgabenwahrnehmung in Betracht. Es kann der abstrakten Gefahrenabwehr dienen, etwa durch Untersuchung von IT-Systemen auf sicherheitsgefährdende Schwachstellen durch das BSI. Es kann der konkreten Gefahrenabwehr dienen, etwa das Lahmlegen einer Website, auf der konkrete Straftaten verabredet werden. Es kann auch der Strafverfolgung dienen, etwa das „Knacken“ verschlüsselter Festplatten der Beschuldigten in einem Steuerstrafverfahren, um die Transaktionen nachvollziehen zu können. Im Zuge der vollständigen Digitalisierung unseres Alltagslebens nimmt der Bedarf staatlicher Stellen zum Eindringen in fremde IT-Systeme zu. Immer mehr Lebenssachverhalte sind nur durch Handeln und Ermitteln im digitalen Raum aufzuklären. So wie selbst die öffentliche Verwaltung ihre Aktenführung mittlerweile auf elektronische Akten umgestellt, haben auch Kriminelle ihr Handeln digitalisiert, zumal im Bereich der Schwerkriminalität.

Der Zugriff auf digitale Systeme durch Behörden wird immer schwieriger. Wegen der zunehmenden Kritikalität digitaler Daten und Anwendungen sowie der zunehmenden Zahl von Cyberangriffen kommen von Seiten der Hardware- und Softwarehersteller mehr und mehr Sicherheitsmaßnahmen gegen das Eindringen in ihre Systeme zum Einsatz. Festplatten sind standardmäßig verschlüsselt, Smartphones

mit Codes gegen das Auslesen gesichert, die Kommunikation im Internet auf allen Ebenen durch *Verschlüsselung* abgesichert. Selbst die gängigsten Massenkommunikationsmittel im digitalen Raum, etwa der Messenger-Dienst WhatsApp, haben eine standardmäßige Verschlüsselung eingeführt.

Sicherheitsbehörden und Staatsanwaltschaften weltweit beklagen die mit diesen Sicherheitsvorkehrungen verbundenen Schwierigkeiten der Staaten, auf Systeme Krimineller zuzugreifen. Damit werde die Kriminalitätsbekämpfung erheblich erschwert, weil die Straftäter mit Hilfe von Verschlüsselung und Zugriffsschutzmaßnahmen in die Unsichtbarkeit abtauchen. International hat sich hierfür der Begriff „Going Dark“ eingebürgert. Der tatsächliche Einfluss dieser unzweifelhaften Zunahme an verschlüsselter Speicherung und Kommunikation auf die Wirksamkeit staatlicher Gefahrenabwehr und Strafverfolgung ist umstritten. Während beispielsweise einerseits die Zahl der für Sicherheitsbehörden nicht auslesbaren Smartphones steigt, stehen andererseits der Polizei und den Nachrichtendiensten neue digitale Möglichkeiten zur Verfügung, etwa die Überwachung der Reisebewegungen Verdächtiger durch Tracking ihrer Smartphone-Positionen oder die Sammlung und Auswertung von Kommunikations-Metadaten.

Auch *staatliches Hacking* trägt als neue Handlungsoption zur Modernisierung des Instrumentariums der Sicherheitsbehörden bei. Das hängt auch mit dem erfolglosen Kampf der Sicherheitsbehörden gegen die Verbreitung starker Verschlüsselung zusammen. Eine mittlerweile über 20-jährige Debatte über Möglichkeiten der Einschränkung oder Abschwächung von Verschlüsselung im Interesse der nationalen Sicherheit hat praktisch keine nennenswerten Ergebnisse gebracht hat. Wegen der globalen Verbreitung von Verschlüsselungstechniken und -produkten, der Interessen der Wirtschaft an starker Verschlüsselung zum Schutz ihrer digitalen Produkte und ihres Know-How sowie der praktischen Schwierigkeiten der Umsetzung einer möglichen Kryptoregulierung sind gesetzliche Regelungen nahezu überall gescheitert. Auch nachrichtendienstliche Bemühungen um Abschwächung von Verschlüsselung – wie sie die National Security Agency (NSA) ausweislich des Snowden-Materials unternommen hat – waren allenfalls von zeitweiligem Erfolg gekrönt.

In der praktischen Anwendung staatlichen Hackings und der Debatte über seine Ausweitung spielen vor allem vier Fallkonstellationen eine Rolle. Erstens erfordert die Auswertung von digitalen Beweismitteln, von Smartphones bis zu externen Festplatten das Überwinden der Sicherheitsmaßnahmen, typischerweise einer Verschlüsselung (Forensik). Zweitens kann eine Kommunikationsüberwachung das Brechen der zum Schutz der Kommunikation verwendeten Kryptoverfahren erfordern (Kommunikations-Kryptoanalyse). Drittens gibt es Fälle, in denen durch Eindringen in das IT-System eines Verdächtigen Daten abgeschöpft werden sollen (*Online-Durchsuchung*) oder eine nicht zu entschlüsselnde Kommunikation bei Quelle oder Empfänger mitgelesen werden soll (Quellen-TKÜ). Viertens kann staatliches *Hacking* auch das Eindringen in Computersysteme zum Zwecke ihrer Manipulation bedeuten, etwa das Vernichten gestohler sensibler Daten oder das Stoppen eines laufenden Cyberangriffs, der von diesem Computer gesteuert wird (letzteres in Deutschland typischerweise als „*Hack-Back*“ bezeichnet).

## 2 Theoretische Grundlagen

Technisch betrachtet erfordert staatliches Hacking die Analyse der jeweiligen Zielsysteme, die Entwicklung von Verfahren zur Überwindung ihrer Sicherheitsmaßnahmen sowie der anschließende Zugang zu den geschützten Systemen. Dabei ist insgesamt zwischen den generellen Fähigkeiten der Sicherheitsbehörden und den konkreten Möglichkeiten im Einzel- bzw. Einsatzfall zu unterscheiden. Um überhaupt auf geschützte Systeme zugreifen zu können, müssen die Behörden über grundlegende Kenntnisse dieser Art von Systemen verfügen, also zum Beispiel darüber, welche Möglichkeiten es prinzipiell gibt, in Smartphones eines bestimmten Herstellers einzudringen, um Daten auszulesen. Hierzu gehören vor allem Kenntnisse über die Stärke der verwendeten Sicherheitsmaßnahmen, z. B. die verwendeten Kryptoverfahren, und die vorhandenen Schwachstellen in den Zielsystemen. *Schwachstellen* sind hierbei Konzeptions- oder Implementierungsfehler eines Systems, die es erlauben, von außen Sicherheitsmaßnahmen zu umgehen oder auszuschalten. Solche Schwachstellen sind teilweise öffentlich bekannt. Sie werden für viele Standardprodukte auch transparent im Internet gesammelt, um Anwendern bei ihrem Schutz zu helfen. Manche Schwachstellen sind jedoch (noch) nicht öffentlich bekannt, in einigen Fällen nicht einmal dem Hersteller des Systems bekannt (sogenannte Zero-Day-Schwachstellen). Diese sind für Hacker besonders wertvoll, weil unwahrscheinlich ist, dass das jeweilige Zielsystem, gegen diese unbekannte Schwachstelle bereits geschützt ist. Ein Eindringen ist mithin sehr erfolgversprechend.

Im konkreten Einsatzkontext sind über die generellen Fähigkeiten und Fertigkeiten der Behörden hinaus spezifische Informationen erforderlich, insbesondere zu der Art und Weise, wie das spezielle System eingesetzt wird. Sie helfen bei der Auswahl der geeigneten Werkzeuge und der Durchführung des Eindringens. Zudem muss auf taktisch-operativer Ebene das Eindringen in das System geplant und vorbereitet werden. Relevant ist natürlich die Frage, ob ein Eindringen offen oder verdeckt erfolgen muss und wie ein System am einfachsten zugänglich ist. Der Zugriff auf den PC eines Verdächtigen kann beispielsweise durch das Aufspielen einer Software im Wege des heimlichen Betretens der Wohnung, des Einschleusens eines USB-Sticks oder auch durch eine Phishing-E-Mail erfolgen, die einen Link auf eine manipulierte Website erhält. Beim Einsatz technischer Werkzeuge zum Eindringen in fremde Systeme ist zudem zu beachten, dass immer auch ein Entdeckungsrisiko damit verbunden ist; das Bekanntwerden eines Werkzeugs oder Vorgehensmodells der Sicherheitsbehörden in der Öffentlichkeit kann die jeweilige Methode im Gebrauchswert erheblich behindern, weil Kriminelle sich gegen sie wappnen können.

Rechtlich bedarf das Eindringen des Staates in geschützte IT-Systeme in Deutschland stets einer gesetzlichen Grundlage. Mit der Entscheidung des Bundesverfassungsgerichts zur Online-Durchsuchung im Jahr 2008 hat das Gericht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG das Grundrecht auf „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ hergeleitet. Dieses sogenannte *Computergrundrecht* oder IT-Sicherheitsgrundrecht schützt den Einzelnen davor, dass der Staat heimlich, also hinter dem Rücken des Berechtigten, auf

IT-Systeme zugreift, Daten ausliest oder das System manipuliert. Der Begriff des IT-Systems ist hierbei sehr weit gefasst und umfasst Computerchips ebenso wie Smartphones, PC, Server oder auch digitale Assistenzsysteme im Auto. Eingriffe in dieses Grundrecht sind nur aufgrund eines Gesetzes und unter Wahrung der Verhältnismäßigkeit möglich. Selbst wenn kein heimliches Eindringen erforderlich ist, wird eine Behörde für das staatliche Hacking eine Gesetzesgrundlage benötigen, um eine Befugnis vorweisen zu können, die eine Strafbarkeit ihres Tuns nach § 202a StGB vermeidet.

Das Bundesverfassungsgericht fordert für den Einsatz von Hacking-Methoden auf informationstechnischen Systemen der Bürger eine normenklare und verhältnismäßige gesetzliche Grundlage, die hohe Anforderungen an die Zulässigkeit der Maßnahme und die begleitenden Absicherungen stellt. Wegen der Schwere des Eingriffs setzt die Verhältnismäßigkeit der Maßnahmen eine besondere Rechtfertigung voraus, etwa die Terrorismusbekämpfung oder die Verfolgung anderer schwerer Straftaten. Wegen dieser gesetzlichen Erfordernisse und aber auch des hohen Aufwandes der praktischen Durchführung kommt Hacking in Fällen leichterer Kriminalität nicht in Betracht.

---

### **3 Praktische Anwendungsfelder und gesetzliche Grundlagen**

Hacking kann grundsätzlich eine Vielzahl staatlicher Aufgaben unterstützen. Ganz unterschiedliche Behörden benötigt für ihre Tätigkeit einen Zugriff auf digitale System, der sich im Falle starker Verschlüsselung nur durch Hacking-Methoden erreichen lässt. Dies reicht von Polizei, Steuerfahndung und Zoll über die Nachrichtendienste bis zu technischen Aufsichtsbehörden, die im Rahmen der Kontrolle von Anlagen und Produkten auch die digitale Sicherheit testen.

In verschiedenen der oben definierten Fallkonstellationen ist schon heute eine gesetzliche Grundlage vorhanden, die das staatliche Hacking erlaubt. Das Eindringen in fremde IT-Systeme, die sich schon in Obhut der Behörden befinden, etwa nach einer Hausdurchsuchung, erfolgt typischerweise nicht heimlich und ist in der Regel durch die Befugnisse gedeckt, auf deren Basis das System beschlagnahmt oder anderweitig eingezogen wurde. Zu Zwecken der IT-Sicherheitsprüfung hat das Bundesamt für Sicherheit in der Informationstechnik in § 7a BSIG eine ausdrückliche Untersuchungsbefugnis auf dem Markt angebotener IT-Produkte erhalten; auch diese Untersuchungen erfolgen jedoch nicht heimlich, auch wenn sie möglicherweise gegen den Willen des Herstellers durchgeführt werden. Eine rechtliche Grundlage gibt es auch für die Fallkonstellation, in der aufgrund einer gesetzlichen Ermächtigung, etwa aus dem Artikel 10-Gesetz oder der Strafprozessordnung, eine Überwachung laufender digitaler Kommunikation erfolgt. Die dabei aufgezeichnete Kommunikation kann – sofern praktisch möglich – entschlüsselt werden. Hierbei handelt es sich auch nicht um einen Eingriff in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, weil das „Abgreifen“ der Kommunikation auf der Über-

tragungsstrecke, beim Telekommunikationsunternehmen oder Internetanbieter erfolgt, nicht bei dem Verdächtigen selbst.

Spezielle Rechtsgrundlagen werden hingegen für den heimlichen Zugriff auf Computersysteme durch die Sicherheitsbehörden benötigt, sei es in Form einer Online-Durchsuchung oder einer Maßnahme der Quellen-TKÜ. Im Nachgang zu der erwähnten Entscheidung des Bundesverfassungsgerichts von 2008, mit dem die erste Befugnisnorm für Online-Durchsuchungen in Deutschland (des Verfassungsschutzes Nordrhein-Westfalen) zunächst für verfassungswidrig erklärt wurde, haben Bund und Länder mittlerweile verschiedene Befugnisse für Online-Durchsuchung und Quellen-TKÜ geschaffen. Auf Bundesebene erhielt zunächst das Bundeskriminalamt im Jahr 2009 mit den §§ 20k, 20l BKAG die Befugnis, die beiden Instrumente zu nutzen, allerdings allein zum Zwecke der Gefahrenabwehr im Bereich der Bekämpfung des internationalen Terrorismus. 2017 wurde diese Befugnis auch für die Zwecke der Strafverfolgung geschaffen und allen Polizeien zur Verfügung gestellt. Mit der Änderung der §§ 100a, 100b StPO dürfen sie nun mit richterlicher Genehmigung Online-Durchsuchung und Quellen-TKÜ einsetzen, sofern dies zur Verfolgung bestimmter schwerer Straftaten erforderlich ist. Der Straftatenkatalog ist umfangreich und reicht von der gewerbsmäßigen Hehlerei über schweren Rauschgifthandel bis zu Mord und Totschlag. Die Gefahrenabwehrbefugnisse des Bundeskriminalamtes (BKA) wurden nicht erweitert, allerdings haben einige Bundesländer wie Rheinland-Pfalz, Bayern, Thüringen oder Hessen in ihren Polizeigesetzen den Einsatz von Online-Durchsuchung im Rahmen polizeilicher Gefahrenabwehr erlaubt.

Ähnlich unterschiedlich ist die Situation bei den Nachrichtendiensten. Einige Verfassungsschutzgesetze der Länder (etwa Bayern und Nordrhein-Westfalen) erlauben ihren Diensten die Online-Durchsuchung. Dem Bundesamt für Verfassungsschutz fehlt eine Rechtsgrundlage. Der Bundesnachrichtendienst hat ebenfalls keine ausdrückliche Rechtsgrundlage, kann das Instrument jedoch gegen Nicht-Deutsche im Ausland einsetzen.

In der vierten beschriebenen Fallkonstellation, das Hacken von Computersystemen zum Zwecke der Manipulation, verfügt allein die Bundeswehr über eine rechtliche Grundlage. Das Eindringen des Militärs in Computersysteme ist allerdings als Einsatz der Bundeswehr zu betrachten, der nur unter sehr hohen Voraussetzungen möglich ist. Außerhalb des Verteidigungsfalls, in dem Deutschland von außen bewaffnet angegriffen wird, darf die Bundeswehr nur im Rahmen von – vom Bundestag bestätigten – internationalen Mandaten eingesetzt werden, so wie derzeit in Afghanistan, Kosovo oder Mali. Bei diesen Einsätzen sind auch Hacking-Operationen erlaubt. Ein sonstiger „digitaler Einsatz“ im In- und Ausland wäre nur als sehr eingeschränkte Amtshilfe für eine inländische Sicherheitsbehörde denkbar. Sie dürfte vom Charakter her die Schwelle eines „Einsatzes der Armee“ nicht überschreiten und würde sich zudem im Rahmen der Befugnisse der Amtshilfe-anfordernden Behörde halten müssen. Mithin existiert für das als Hack-Back bezeichnete Szenario eines staatlichen Eindringens in ausländische IT-Systeme – auch ganz unabhängig von der Problematik der völkerrechtlichen Zulässigkeit – keine nationale Rechtsgrundlage.

## 4 Umsetzungsstand und Umsetzungsschwierigkeiten

Mit den derzeitigen gesetzlichen Grundlagen in Strafprozessordnung, Polizei- und Verfassungsschutzgesetzen dürften bereits mehr als 20 deutsche Behörden zum heimlichen Eindringen in Computersysteme befugt sein. Die verfügbaren öffentlichen Quellen über die Nutzung dieser neuen Befugnisse deuten allerdings auf eine bislang nur geringe praktische Relevanz hin. Amtliche Fallzahlen werden nicht veröffentlicht. Aussagen zur Effektivität und Effizienz von Hacking-Maßnahmen im Verhältnis zu dem jeweiligen Gesetzeszweck sind daher nicht möglich.

Ursächlich für die schwache Nutzung der Befugnisse sind offenkundig nicht der geringe Bedarf an dem Eindringen in digitalen Systeme Verdächtiger, sondern die Schwierigkeiten der praktischen Umsetzung. Staatliches Hacking begegnet in der Praxis drei wesentlichen Problemen: erstens der Qualifizierung der Mitarbeiter/innen und Qualitätssicherung der Werkzeuge, die für staatliches Hacking benötigt werden, zweitens dem Umgang mit den für heimliches Eindringen bedeutsam Schwachstellen in Hardware und Software sowie drittens der Frage der Zuständigkeit von Behörden für staatliches Hacking, ihrer Abgrenzung und Zusammenarbeit.

Staatliches Hacking ist eine Behördenaufgabe, die höchstqualifizierte Mitarbeiterinnen und Mitarbeiter erfordert. Die für die sicherheitstechnische Analyse von ständig weiterentwickelten IT-Systemen benötigte Qualifikation entspricht der Qualifikation zur Absicherung von Unternehmen und Behörden gegen Cyberangriffe, die auf dem Markt derzeit erheblich nachgefragt ist. Gerade bei technisch-wissenschaftlichen Spitzenqualifikation tut sich der öffentliche Sektor jedoch besonders schwer bei der Personalgewinnung und Personalentwicklung. Zudem müsste eine solche Spitzkompetenz grundsätzlich bei jeder Behörde vorgehalten werden, die entsprechende Befugnisse hat. Weiterhin ist die Landschaft der eingesetzten Produkte so vielfältig und eine Voraussage kaum möglich, welche Systeme von mutmaßlich Verdächtigen eingesetzt werden. Daher muss ein weites technologisches Spektrum bedient werden. In der Praxis führt dieses Qualifikationsproblem dazu, dass die Sicherheitsbehörden sich auf Produkte und Dienstleistungen externer Unternehmen verlassen, mit deren Hilfe ein Eindringen in IT-Systeme ermöglicht wird. Der globale Markt hierfür ist recht vielfältig.

Mit dem Einsatz von Programmen zum heimlichen Auslesen von Computern, umgangssprachlich als „Trojaner“ bezeichnet, sind jedoch eine Fülle von Risiken verbunden. Es muss sichergestellt werden, dass die Software auf dem richtigen System die richtige Person überwacht. Nur die erlaubten Daten dürfen aufgezeichnet werden. Ein Ausleiten der Daten muss so sicher erfolgen, dass Dritte die sensiblen Daten nicht mitlesen können. Eine Fernsteuerung der Software darf nur der jeweiligen Behörde gelingen, nicht „anderen Hackern“, die das geöffnete Tor nutzen, um ihrerseits das System auszuspionieren oder einem Verdächtigen falsche Beweise unterzuschieben. Die Software darf durch den Verdächtigen nicht entdeckt werden können, damit er die Beweise nicht manipuliert oder durch eine Veröffentlichung der Software ihre zukünftige Wiederverwendung einschränkt. Aufgrund dieser Risiken eines Einsatzes solcher Software stellen Gesetzgeber und Bundesverfassungsgericht hohe Anforderungen an die Vertrauenswürdigkeit der Software, ihre Kontrollfähigkeit

keit durch die Behörden, die Vorbereitung und Durchführung eines Einsatzes sowie die Dokumentation aller Abläufe. Selbst wenn Produkte externer Unternehmen eingesetzt werden, muss die Behörde mit eigenen Kräften alle wesentlichen Aspekte durchdringen, steuern, kontrollieren und dokumentieren. Dies ist angesichts der hohen Zahl und unterschiedlichen Größe der deutschen Sicherheitsbehörden eine ganz erhebliche Herausforderung.

Zweites praktisches Problem des heimlichen Eindringens in informationstechnische Systeme ist die Überwindung der Sicherheitsvorkehrungen. Wenn die Behörde in ein System eindringen will, muss sie Lücken in der Sicherheit des Systems finden. Solche Lücken können unzureichende Sicherheitsmaßnahmen sein oder auch Schwachstellen in der eingesetzten Hardware und Software, die es erlauben, die Systeme ohne Kenntnis ihres Benutzers zu manipulieren. Nach wie vor weisen die gängigen Hardware- und Softwareprodukte eine Vielzahl von Schwachstellen auf, darunter auch zahlreiche, die für heimliches Eindringen genutzt werden können. Die Bemühungen um Verbesserung der Qualität von IT-Systemen und Reduzierung der Schwachstellen haben nicht nennenswert gefruchtet, weil gleichzeitig die Funktionalität der Produkte, ihre Einsatzbreite und Vernetzung so stark zunehmen, dass neue Schwachstellen entstehen und neue Mechanismen des Eindringens ermöglichen.

Schwachstellen sind für Hacker der Schlüssel, um die Sicherheitsvorkehrungen zu umgehen und in Systeme einzudringen. Hier geht es den staatlichen Hackern nicht anders als den Urhebern von Cyberangriffen, welche üblicherweise ebenfalls auf der Ausnutzung von Schwachstellen beruhen. Diese „Dual-Use-Funktion“ von Schwachstellen in Hardware und Software stellt sich für den Staat als Problem dar. Während der Staat einerseits im Rahmen der Förderung der IT-Sicherheit die Qualitätsverbesserung von Software propagiert und das schnelle Schließen von Schwachstellen rechtlich und praktisch fördert und fordert, ist er auf der anderen Seite auf Schwachstellen angewiesen, um in Systeme Krimineller einzudringen. Damit sind staatliche Behörden Teil eines internationalen Schwachstellenmarktes, den sie eigentlich austrocknen wollen. Ob sie auf dem Schwarzmarkt unmittelbar Schwachstellen kaufen oder ob sie sich der Werkzeuge privater Unternehmen bedienen, die auf Schwachstellen beruhen: staatliche Behörden sind ein wichtiger Nachfrager in diesem Bereich. Ob durch Nachfrage der Behörden die schnelle Beseitigung von Schwachstellen gefördert oder erschwert wird, ist strittig. Klar ist, dass der Staat einen inneren Interessengegensatz auszuhalten und auszutragen hat, wie mit Schwachstellen, insbesondere den noch unbekannten Zero-Days umgegangen wird.

Hieraus hat sich ein schwieriges rechtliches und politisches Problem ergeben. Zur Wahrnehmung der gesetzlichen Befugnisse zu Online-Durchsuchung und Quellen-TKÜ müssen die Polizeien Schwachstellen ausnutzen. Gleichzeitig hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Auftrag, ihm zugegangene Erkenntnisse über Schwachstellen unverzüglich an potenziell Betroffene weiterzugeben, insbesondere die Betreiber kritischer Infrastrukturen, damit diese ihre Systeme absichern können. Eine Abstimmung der verschiedenen Behörden zu diesen unterschiedlichen Interessen findet derzeit nicht statt. Die US-amerikanische Regierung hat dieses Problem schon 2010 gesehen und aufgegriffen. Mit Hilfe eines sogenannten „Vulnerability Equities Process“, eines formalisierten Abwägungsprozesses innerhalb

der US-Regierung wird darüber entschieden, welche der Interessen im Einzelfall schwerer wiegen: das Interesse an der Geheimhaltung der Schwachstelle zwecks Strafverfolgung oder zwecks Abwehr möglicherweise unmittelbar drohender Gefahren einerseits oder das Interesse an der Offenlegung der Schwachstelle gegenüber dem Hersteller zwecks Verbesserung der IT-Sicherheit und Verhinderung von – möglicherweise ebenfalls bedrohlichen – Cyberangriffen andererseits. In Deutschland ist ein solcher Prozess noch nicht etabliert, nach Aussagen der Bundesregierung ist dies aber geplant. Gegen die Einführung der Online-Durchsuchung in die StPO sind mehrere Verfassungsbeschwerden anhängig. Es ist zu erwarten, dass das BVerfG die Frage des Umgangs mit Schwachstellen in diesen Verfahren prominent aufgreift.

Ein weiteres grundlegendes Problem staatlicher Hacking-Aktivitäten ist die Behördenzuständigkeit für Hacking sowie die Abstimmung und Zusammenarbeit zwischen den Behörden. Bislang wurden in Deutschland die neuen Befugnisse der Behörden zum heimlichen Eindringen in IT-Systeme entlang der bestehenden Zuständigkeiten eingerichtet. Als Erweiterung zu Polizei- und Verfassungsschutzgesetzen oder StPO sind demnach viele Behörden zuständig. Wie dargestellt ist es jedoch kaum vorstellbar, dass diese Entwicklung dauerhaft fortgesetzt wird. Die Durchführung von Hacking-Operationen erfordert ein so spezialisiertes Know-How, eine Beschaffung kostspieliger Werkzeuge sowie eine ständige Aktualisierung des Instrumentariums, dass schon allein im Bereich der Polizeien eine hochwertige Wahrnehmung der Aufgabe durch alle Polizeiorganisationen nebeneinander nicht möglich ist. Einige Bundesländer haben sich in verschiedenen Konstellationen zusammengeschlossen, um gemeinsam Software auszuwählen und zu beschaffen oder beim Einsatz zusammenzuarbeiten. Der Bund hat mit der 2017 erfolgten Einrichtung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) eine Servicestelle für BKA, Bundesamt für Verfassungsschutz (BfV) und Bundespolizei im Hinblick auf digitale Ermittlungen geschaffen. Die Entwicklung oder Begutachtung von Software zum Eindringen in Computer gehört zwar fachlich nicht ausdrücklich zu ihrem Auftrag. Gleichwohl wird ZITiS eine bedeutende Rolle für alle Sicherheitsbehörden spielen, weil ihre Zuständigkeit, digitale Forensik, Kryptoanalyse, Telekommunikationsüberwachung und Big Data-Analysen, fachlich sehr nah am staatlichen Hacking liegen.

Offene Fragen der Entwicklung von Verfahren und Technologien zum staatlichen Hacking bestehen zudem in der Kooperation zwischen den in Deutschland tätigen Sicherheitsbehörden und dem Auslandsnachrichtendienst BND sowie zwischen den zivilen Stellen und der Bundeswehr. Letztere unterhält schon seit einigen Jahren ein Zentrum für Computer-Netzwerkoperationen, das sich auf aktive Angriffe auf gegnerische Computersysteme vorbereitet und hierfür auch Kompetenzen und Werkzeuge aufgebaut hat. Noch nicht gelöst ist auch die dauerhafte organisatorische Verknüpfung zwischen denjenigen staatlichen Behörden, die in Computersysteme eindringen und denjenigen Behörden (an der Spitze das Bundesamt für Sicherheit in der Informationstechnik BSI), die Computersysteme schützen sollen. Verpflichtet man letztere zur Mitwirkung an der Entwicklung von Hacking-Verfahren, leidet ihre Glaubwürdigkeit. Lässt man sie außen vor, wird ausgerechnet einer der sensibelsten Bereich der staatlichen digitalen Tätigkeit, das Hacking, nicht von den zuständigen Sicherheitsspezialisten unterstützt und überprüft.

## 5 Perspektiven

Staatliches Hacking, also das Eindringen von Behörden in IT-Systeme von Bürgern und Unternehmen, gehört mehr und mehr zum Standard-Instrumentarium der Sicherheitsbehörden. Es liegt auf der Hand, dass staatliches Hacking sinnvolle Beiträge zur Verhinderung oder Aufklärung von Straftaten bringen kann. Insbesondere existieren Fallkonstellationen, in denen staatliches Hacking das einzige Instrument ist, um bestimmte Erkenntnisse überhaupt zu erlangen. Angesichts der Geschwindigkeit und des Facettenreichtums der Digitalisierung aller Kriminalitätsbereiche ist jedoch kaum überprüfbar, ob die Sicherheitsbehörden in Summe ihrer Arbeit zwingend auf das Hacking-Instrumentarium angewiesen sind oder ob die verschiedenen anderen Ermittlungsmethoden auch ohne Eindringen in Systeme adäquate Ergebnisse bringen können, die den Verzicht von durch Hacking gewonnenen Erkenntnissen kompensieren. Weil diese Frage nicht eindeutig zu beantworten ist und der Bund ebenso wie die Länder staatliches Hacking bereits praktizieren, ist ein Verzicht auf das Instrument kaum wahrscheinlich. Die Diskussion konzentriert sich daher zunehmend auf seine Ausgestaltung. Staatliches Hacking ist eine Aufgabe, deren Wahrnehmung besondere rechtliche und tatsächliche Kompetenzen benötigt, erhebliche Risiken beinhaltet und besondere Qualität und Sorgfalt erfordert. Neben den individuellen Risiken staatlicher Hacking-Operationen für den Betroffenen oder durch Kollateralschäden bestehen auch gesamtgesellschaftliche Risiken wie eine Abschwächung des IT-Sicherheitsniveaus durch Zurückhalten von Schwachstellen oder die Unterstützung weltweiter Diktaturen durch Hacking-Technologie, die für deutsche Sicherheitsbehörden entwickelt wurde.

Den hohen Anforderungen an staatliches Hacking und erheblichen Risiken wird die derzeitige rechtliche, organisatorische und fachliche Struktur in Deutschland nicht gerecht. Zukünftig steht eine weitergehende Vereinheitlichung der Eingriffsgrundlagen einschließlich der technisch-organisatorischen Vorkehrungen auf der Tagesordnung. Nur durch harmonisierte Verfahren kann eine Qualitätssicherung und Kontrolle sichergestellt werden. Organisatorisch spricht sehr viel für eine weitergehende Bündelung der Entwicklung und Betreuung der Technologie durch Gemeinschaftseinrichtungen wie ZITiS. Sie können Verfahren und Werkzeuge auf höchstem Qualitätsniveau entwickeln und externe Auftragnehmer qualifiziert steuern und kontrollieren. Nur an zentraler Stelle kann das fachliche-Know-How so organisiert werden, dass trotz schneller technischer Entwicklung die Leistungsfähigkeit der Sicherheitsbehörden beim Eindringen in Systeme dauerhaft gewährleistet wird.

Über die bisherigen Anwendungsfälle staatlichen Hackings hinaus ist damit zu rechnen, dass auch die vierte beschriebene Fallkonstellation, das Eindringen in Computersysteme zum Zwecke der Manipulation demnächst gesetzlich geregelt wird. In Deutschland vor allem unter dem Begriff „Hack-Back“ diskutiert, sind verschiedene Unterfälle denkbar: von der Vernichtung entwendeter sensibler Daten auf Servern der Täter über das Stoppen eines Servers, der einen laufenden Cyberangriff steuert, bis zum Abschalten eines Kinderpornografie-Shops im sogenannten Darknet. Hack-Back kann im Prinzip Systeme im In- wie im Ausland betreffen, kann Kollateralschäden

verursachen und zu politischen oder diplomatischen Krisen bis hin zu entsprechenden Gegenmaßnahmen anderer Staaten führen, die sich von einer Hacking-Aktivität bedroht sehen. Die Schaffung einer entsprechenden Befugnis wirft daher eine Fülle von völkerrechtlichen, verfassungsrechtlichen und politischen Fragen auf, die im Gesetzgebungsverfahren zu klären sein werden. Zu diesen Fragen gehört auch die Festlegung der Zuständigkeit: Ist das manipulierende Eindringen in Server im In- und Ausland eine Aufgabe des Militärs oder der zivilen Sicherheitsbehörden? Ist es eher eine Aufgabe der Polizei oder eines Nachrichtendienstes? Für alle Konstellationen lassen sich Argumente und internationale Beispiele finden. Angesichts der mit Hack-Back verbundenen besonderen Risiken wäre ein Ansatz sinnvoll, der das Instrument zwar grundsätzlich ermöglicht, es jedoch sehr zivil und sehr rechtsstaatlich verankert, etwa bei einer Polizeibehörde mit Richtervorbehalt.

---

## Literatur

- Bundeskriminalamt. 2018. Quellen-TKÜ und Online-Durchsuchung. Notwendigkeit, Sachstand und Rahmenbedingungen. [https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung\\_node.html](https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html). Zugegriffen am 11.02.2020.
- Bundesverfassungsgericht. 2008. Entscheidung zum Verfassungsschutzgesetz NRW (Online-Durchsuchung). Vom 27.02.2008. BVerfG, Urteil des Ersten Senats vom 27. Februar 2008. – 1 BVer 370/07 –, Rn. (1-333). BVerfGE 120, 274–350. [http://www.bverfg.de/e/rs20080227\\_1bver037007.html](http://www.bverfg.de/e/rs20080227_1bver037007.html). Zugegriffen am 11.02.2020.
- Chaos Computer Club. O. J. Staatstrojaner. <https://www.ccc.de/de/tags/staatstrojaner>. Zugegriffen am 11.02.2020.
- Gusy, Christoph. 2009. Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. *Datenschutz und Datensicherheit* 33(1): 33–41.
- Marxsen, Christian. 2017. Verfassungsrechtliche Regeln für Cyberoperationen der Bundeswehr. Aktuelle Herausforderungen für Einsatzbegriff und Parlamentsvorbehalt. *JuristenZeitung* 72(11): 543–552.
- Netzpolitik.org. o. J. Staatstrojaner. <https://netzpolitik.org/tag/staatstrojaner/>. Zugegriffen am 11.02.2020.
- Reinhold, Thomas, und Matthias Schulze. 2017. Digitale Gegenangriffe. Eine Analyse der technischen und politischen Implikationen von „hack backs“. Arbeitspapier Forschungsgruppe Sicherheitspolitik, Stiftung Wissenschaft und Politik, FG03-AP Nr. 1. Berlin: Stiftung Wissenschaft und Politik. [https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/AP\\_Schulze\\_Hackback\\_08\\_2017.pdf](https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/AP_Schulze_Hackback_08_2017.pdf). Zugegriffen am 11.02.2020.
- Schallbruch, Martin. 2018. *Schwacher Staat im Netz. Wie die Digitalisierung den Staat in Frage stellt*, 79–96. Wiesbaden: Springer.
- Schulz, Wolfgang, und van Hoboken. 2016. *Human rights and encryption*. Paris: United Nations Educational, Scientific and Cultural Organization.
- Singelnstein, Tobias, und Benjamin Derin. 2017. Das Gesetz zur effektiveren und praxistauglichen Ausgestaltung des Strafverfahrens. *Neue Juristische Wochenschrift* 70(37): 2646–2652.
- Whitehouse. 2017. Vulnerabilities Equities Policy and Process for the United States Government. November 15, 2017. <https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF>. Zugegriffen am 11.02.2020.
- Zentralstelle für Informationstechnik im Sicherheitsbereich des Bundes. o. J. <https://www.zitis.bund.de/>. Zugegriffen am 11.02.2020.



---

# Der elektronische Personalausweis

Lasse Gerrits, Martin Wirtz und Sebastian Hemesath

## Inhalt

1 Klärung der Begriffe .....	540
2 Theoretische Grundlagen .....	540
3 Praktische Anwendung .....	541
4 Verbreitung und Nutzerverhalten .....	545
5 Künftige Entwicklung .....	549
Literatur .....	550

---

## Zusammenfassung

Dieses Kapitel betrachtet das Thema „elektronischer Personalausweis“ (eID) aus einer internationalen Perspektive. Es zeigt die Vielfalt der eID-Formate auf und weist auf die starken Schwankungen zwischen EU-Mitgliedstaaten bezüglich der Ausprägungen und der Nutzungsrationen hin. Auch wenn Deutschland hinsichtlich der Nutzungsrate nicht das Schlusslicht bildet, so hinkt die Entwicklung doch hinter der in anderen EU-Ländern her. Mögliche Gründe hierfür werden diskutiert und theoretisch beleuchtet. Die Ursachen werden vor allem in den Faktoren Risikowahrnehmung, Föderalismus und Verbraucherfreundlichkeit gesehen.

---

L. Gerrits (✉)

Politikwissenschaft, Otto-Friedrich-Universität Bamberg, Bamberg, Deutschland

E-Mail: [lass.gerrits@uni-bamberg.de](mailto:lass.gerrits@uni-bamberg.de)

M. Wirtz

Stadt Aachen, Aachen, Deutschland

E-Mail: [WirtzMartin@gmx.de](mailto:WirtzMartin@gmx.de)

S. Hemesath

Otto-Friedrich-Universität Bamberg, Bamberg, Deutschland

E-Mail: [hiwis.complexsys@uni-bamberg.de](mailto:hiwis.complexsys@uni-bamberg.de)

## Schlüsselwörter

Elektronische Identifizierung · e-Government · Implementierung · Technologie-Akzeptanz · Europa

---

## 1 Klärung der Begriffe

Unter „elektronischer Identifizierung“ bzw. „elektronischer Identifikation“ (eID) versteht man im weitesten Sinne eine verifizierte und geschützte elektronische Kennung, die für die sichere Nutzung öffentlicher oder auch privater Dienste im Inland und über Ländergrenzen hinweg eingesetzt werden kann. Somit soll ähnlich der bisherigen Praxis der physischen Identifikation von Bürgern mit Hilfe von Dokumenten wie Reisepässen oder Personalausweisen, eine digitale Form der Identifikation und Legitimation geschaffen werden. Vor dem Hintergrund der voranschreitenden Digitalisierung wurden verschiedene Initiativen verabschiedet (z. B. Richtlinie 1999/93/EG, Richtlinie 2006/12/EG, Verordnung (EU) 910/2014), in denen die EU-Mitgliedstaaten die Umsetzung von eID-Formaten für ihre Bürgerinnen und Bürger vereinbart haben. Insofern ist eID ein Grundpfeiler des digitalen Binnenmarktes geworden. In aller Regel (aber nicht immer) steht der Begriff e-ID für einen Pass (Personalausweis) mit einem RFID-Chip, also einem Chip welcher es ermöglicht, die gespeicherten Daten mittels Funkwellentechnologie auszulesen. Auf diesem Chip sind die biometrischen Daten des Besitzers gespeichert. Europaweit sind alle Systeme so konstruiert, dass Bürgerinnen und Bürger von überall aus Zugang zu staatlichen und – in einigen Ländern – privaten Diensten haben, solange sie eine Internetverbindung und Zugang zur Hard- und Software haben, die für die vollständige Identifikation notwendig ist. Gleichwohl ist es den Mitgliedstaaten freigestellt, eID-Formate nach ihren eigenen Prioritäten zu gestalten, solange sie den generellen Standards entsprechen (Europäische Kommission 2018). Daher lässt sich eine große Bandbreite an eID-Formaten in den verschiedenen Ländern beobachten. Die unterschiedlichen Ausprägungen von eID Formaten in Europa werden in Abschn. 3 vorgestellt.

---

## 2 Theoretische Grundlagen

Generell kann eine elektronische Identifizierung als Mittel verstanden werden, mit Hilfe dessen geprüft werden kann, ob der bzw. die jeweilige Nutzer/-in eines Dienstes tatsächlich die Person ist, die er bzw. sie angibt, zu sein. Darüber hinaus besitzen auch Dinge, Ressourcen und Dienste eine Identität, welche ihnen ebenso eine gewisse Charakteristik bzw. ein Profil zuweist. Die Identifizierung ermöglicht es daher einer bestimmten Einrichtung (sowohl öffentlich als auch privatwirtschaftlich) die unterschiedlichen Nutzer voneinander zu unterscheiden. Gleichzeitig können Nutzer ebenso die Identität der genutzten Dienste oder Ressourcen feststellen und legitimieren.

Bürger, Unternehmen und öffentliche Verwaltung teilen ein gemeinsames Problem bei der elektronischen Identifizierung: Um Missbrauch und Identitätsdiebstahl im digitalen Raum vorzubeugen und sicherzustellen, dass die Vertragspartner bei elektronischen Transaktionen und Rechtsgeschäften tatsächlich jene sind, die sie angeben zu sein, bedarf es einer Lösung, um die tatsächliche Identität der jeweiligen Partei rechtskräftig festzustellen.

Da es im digitalen Raum keinen persönlichen Kontakt zwischen den unterschiedlichen Parteien gibt, ist eine sichere Identifikation für das gegenseitige Vertrauen wichtig und stellt somit eine grundsätzliche Notwendigkeit für die Durchführung von verbindlichen oder sensiblen Rechtsgeschäften und Verwaltungsdienstleistungen im Internet dar. Die Möglichkeit, einen Datensatz an Informationen einem gewissen Nutzer zuzuordnen (sei es zu einem Bürger, einem Unternehmen oder zur öffentlichen Verwaltung) ist somit eine essenzielle Voraussetzung für eine Vielzahl von Interaktionen und Transaktionen. Hierfür bedarf es organisatorischer und technischer Infrastruktur, welche explizit dafür entwickelt wurde, um die Identität einer bestimmten Gruppe an Personen (natürlich oder juristisch) zu definieren, zuzuschreiben und zu verwalten und welche Legitimität garantiert. Die elektronische Identifikation oder elektronische Identität kann somit als Sammelbegriff oder übergreifendes Konzept für unterschiedliche *Identifikationssysteme* verstanden werden, welche unter anderem auch die Form eines digitalen Identifikationsausweises – entsprechend dem deutschen elektronischen Personalausweis – annehmen kann.

---

### 3 Praktische Anwendung

Während die bisherigen Ausführungen den Eindruck erwecken könnten, dass es sich bei e-ID um einen einheitlichen Standard und um eine einheitliche Technologie handelt, so haben in Wirklichkeit die unterschiedlichen Mitgliedsstaaten der Europäischen Union gänzlich unterschiedliche Formen der Implementierung ausgewählt. Gleichzeitig variiert der Stand der Implementation beträchtlich zwischen den einzelnen Ländern. Tab. 1 zeigt exemplarisch die verfügbaren eID Lösungen in zehn europäischen Ländern. Schon auf den ersten Blick zeigt sich die große Vielfalt der gewählten eID-Formate. So hat Estland beispielsweise sowohl eine eID-Karte eingeführt, für deren Nutzung ein elektronischer Kartenleser notwendig ist, als auch eine mobile eID in Form einer verifizierten SIM-Karte. Die Einsatzmöglichkeiten der eID reichen von der Identifikation für öffentliche Dienste über Wahlen bis hin zum öffentlichen Personennahverkehr. Die Karte wurde im Jahre 2001 eingeführt und hier Nutzungsrate liegt heute bei 98 %. Am anderen Ende der Skala hat Frankreich noch praktisch gar nichts implementiert, da der Verfassungsrat (*Conseil constitutionnel*) bisherige eID-Vorhaben für verfassungswidrig erklärt hat.

Zwischen diesen beiden Extremen sehen wir viele verschiedene Arten der Nutzung von elektronischen Vertrauensdiensten. In den Niederlanden nimmt die eID die Form einer verifizierten Daueronlinekennung an, die zur zuverlässigen Identifikation vieler Dienste, von der Steuererklärung bis zur Einschreibung an Schulen und Universitäten, genutzt werden kann. Eine Zwei-Faktor-Identifikation fungiert als

**Tab. 1** Überblick über eID-Formate in ausgewählten EU-Staaten. Grundlagen für die Auswahl dieser zehn Länder waren die Datenverfügbarkeit und der Anspruch, das gesamte Spektrum von Anwendungen, Formen und Funktionalitäten abzudecken. (Quelle: PBLQ 2015 und eigene Recherchen)

Mitgliedsstaat	Zweck	Technologie	Eingeführt durch	Nutzung
<b>Österreich</b>	Online-Legitimation (für Amtswege), Kranken- und Sozialversicherungsausweis	<i>Bürgerkarte</i> Chipkarte mit Lesegerät und PIN <i>Handy-Signatur</i> Zertifikat mit registrierter Mobilfunknummer und SMS-TAN	Öffentliche Hand	2003 Einführung Bürgerkarte 2012 Einführung Handy-Signatur
<b>Belgien</b>	Legitimation für öffentliche Anwendungen und Zugangsberechtigung für öffentliche Gebäude	<i>e-ID</i> Chipkarte mit Lesegerät, Software und PIN <i>Kids-ID</i> Chipkartenlösung für Kinder unter 12 Jahren	Öffentliche Hand	2003 Einführung e-ID 2004 Verpflichtend für alle Neuaustrstellungen (Kinder freiwillig)
<b>Estland</b>	Legitimation für nahezu alle Verwaltungssangelegenheiten, Gesundheitskarte und Nahverkehrssticket	<i>National ID</i> Chipkarte mit Lesegerät, Software und PIN <i>Mobil-ID</i> Registrierte Sim-Karte und Mobilfunknummer in Verbindung mit PIN	Öffentliche Hand/Private Hand	2001 Einführung National ID 2005 Erste e-Wahlen 2007 Einführung Mobil-ID
<b>Frankreich</b>	Geplante Einführung einer digitalen Identifikation am Verfassungsgericht gescheitert	-	-	-
<b>Deutschland</b>	Online Legitimation und Ausweisfunktion	<i>Neuer Personalausweis</i> Chipkarte mit aktivierter Online-Funktion, Lesegerät (NFC-fähiges Smartphone) und PIN	Öffentliche Hand	2011 Einführung neuer Personalausweis 2017 Verpflichtende Freischaltung der Online-Funktion

<b>Italien</b>	Digitales Identifikationsystem für kommunale Verwaltung und Dienstleistungen der Kranken- und Sozialversicherung	<i>SPID</i> Nutzername und Passwort	Öffentliche Hand/Private Hand	2000–2017 Erste Versuche einer e-ID Lösung (z. B. „CIE“) 2016 Einführung SPID	4 % der Bevölkerung
<b>Niederlande</b>	Nutzung digitaler Verwaltung	<i>DigID</i> Nutzername und Passwort, teilweise mit SMS-TAN	Öffentliche Hand/Private Hand	2003 Einführung DigID	71 % der Bevölkerung
<b>Spanien</b>	Elektronischer Identitätsnachweis, Steuererklärung	<i>DNI Electronico</i> Chipkarte mit Lesegerät (NFC-fähiges Smartphone), Software und PIN <i>cl@ve</i> Nutzername und Passwort	Öffentliche Hand	2006 Einführung DNI Electronico 2015 Einführung NFC Nutzung Einführung cl@ve	3 % der Bevölkerung
<b>Schweden</b>	Identifikation und Legitimation für Verwaltungsdienste	Verschiedene öffentliche und privatwirtschaftliche Lösungen (Chipkarte, Mobile Identifikation, Softwarebasiert). Führend: <i>BankID</i>	Private Hand/ Öffentliche Hand	2003 Einführung BankID	75 % der Bevölkerung
<b>Vereinigtes Königreich</b>	Identifikation und Legitimation bei einigen Verwaltungsdiensten	<i>GOV.UK Verify</i> Identifikation durch Unternehmen (z. B. Banken, Post) verifiziert	Private Hand/ Öffentliche Hand	2016 Einführung GOV.UK Verify	892 Millionen Transaktionen pro Jahr

zusätzliche Sicherheitsmaßnahme. Eine ähnliche Technologie wird im Vereinigten Königreich angewandt, wo die eID zum Beispiel für Sozialhilfeanträge oder für einen Führerschein genutzt werden kann. Belgien bietet eine große Bandbreite an Nutzungsmöglichkeiten, einschließlich der Möglichkeit, online Strafanzeige zu erstatten oder Abfälle für Recycling-Depots aufzugeben. Belgien nutzt die eID auch, um Nutzerinnen und Nutzer in VPN-Netzwerken zu identifizieren. Im Gegensatz zu den beiden vorangegangenen Beispielen, wo eID keine zweckbestimmte Hardware auf Seiten der Nutzerinnen und Nutzer benötigt, müssen belgische Staatsangehörige eine Karte und einen privaten Kartenleser nutzen, um sich zu identifizieren. Die Tabelle zeigt noch weitere Beispiele.

Die Länder unterscheiden sich nicht nur in Bezug auf die Funktionen und Technologie der eID, sondern auch maßgeblich in Bezug auf die *Implementierung* und Nutzung (rechte Tabellenspalte). Manche Länder (z. B. Österreich, Belgien, Estland und die Niederlande) erscheinen als Vorreiter, während andere (z. B. Deutschland, Frankreich und Italien) langsamer sind. Des Weiteren muss zwischen der Implementierung und der tatsächlichen Nutzung unterschieden werden. Erstere betrifft die ergriffenen Maßnahmen zur Bereitstellung der Technologie, während Letztere die tatsächliche Nutzung durch die Bürgerinnen und Bürger meint. Italien hat beispielsweise seit dem Jahr 2000 mehrere Versuche zur eID-Implementierung unternommen. Die Implementation ist jedoch dezentral organisiert und verläuft langsam und unstrukturiert. Entsprechend rückständig ist auch die Nutzung durch die Bürgerinnen und Bürger. Andere Länder wie etwa Schweden oder Estland waren nicht nur schneller, sondern haben auch weit höhere Nutzungsrationen.

Was die Funktionalität der deutschen eID betrifft: Deutsche Staatsangehörige können ihre eID durch eine Kombination aus der neuen Version des Personalausweises (der einen RFID-Chip enthält) mit einem Kartenleser oder einem Smartphone mit NFC-Chip (Near-Field Communication) nutzen. Die eID kann auch für einige öffentliche Dienste wie die Steuererklärung und einige kommunale Dienste eingesetzt werden. Sie hat auch einige kommerzielle Anwendungen, etwa die Identifizierung bei der Deutschen Bahn und einigen Versicherungsgesellschaften. Für solche Zwecke sind auch alternative Technologien verfügbar, d. h. es ist nicht immer nötig, sich mit dem Ausweis plus Kartenleser oder Smartphone zu identifizieren. Wenn es um die Implementierung der eID an sich geht, liegt Deutschland im Mittelfeld: nicht so fortgeschritten wie manche, aber auch nicht so langsam wie andere der oben genannten Mitgliedstaaten. Wenn es jedoch um den Nutzungsgrad und die Bandbreite der Nutzungsmöglichkeiten geht, scheint das Land hinterherzuhinken. Vor diesem Hintergrund hat der Gesetzgeber jüngst mit dem Gesetz erneut Maßnahmen ergriffen, um die automatische und dauerhafte Einschaltung der eID-Funktion bei jedem Ausweis voranzutreiben, das Genehmigungsverfahren für die Nutzung der eID-Funktion für Dienstanbieter (Unternehmen und Behörden) zu vereinfachen und die Nutzungsmöglichkeiten zu erweitern.

Zusammengefasst zeigt Tab. 1, dass (1) die europäischen Mitgliedstaaten stark unterschiedliche Typen von eID entwickelt haben, die trotz mancher Gemeinsamkeiten viele verschiedene Formen, Anwendungen und Nutzungsmöglichkeiten haben; und (2) dass die Implementierung und Nutzung sich sehr deutlich zwischen

den Ländern unterscheidet. Deutschland ist ein interessanter Fall, da es die notwendige Technologie installiert hat und doch eine niedrige Nutzungsrate aufweist.

---

## 4 Verbreitung und Nutzerverhalten

In einem im Jahre 2010 von Herbert Kubicek herausgegebenen Sonderheft der Zeitschrift „Identity in the Information Society“ wurde die Vielfalt der nationalen eID-Formate in Europa vergleichend untersucht sowie Erklärungsansätze für die jeweils gewählten Formate präsentiert (Kubicek 2010). Wie aus den obigen Ausführungen deutlich wurde, haben sich seither nicht nur die eID-Formate und ihre jeweiligen Eigenschaften weiterentwickelt, sondern auch Art und Umfang der Nutzung. Insbesondere für den interessanten Fall der Bundesrepublik konnten seinerzeit noch keine Aussagen über die Nutzungsrationen getroffen werden. Im Folgenden wird Deutschland mit anderen Ländern verglichen, um vor dem Hintergrund verschiedener theoretischer Ansätze Gründe für die geringe Nutzungsrate der eID zu eruieren.

Das Auseinanderfallen zwischen einem recht weiten Implementationsstand einerseits und der niedrigen eID-Nutzungsrate andererseits legt stereotype Erklärungsmuster rund um den Begriff der *German Angst* nahe. Indem man Parallelen zum vergleichsweise schleppenden Breitbandausbau zieht, kann man außerdem ein Bild von Deutschland als digitalem Nachzügler zeichnen. Tatsächlich spiegeln sich in den eID-Nutzungsrationen grundsätzliche kulturelle Unterschiede in der Risikowahrnehmung wider. Soziale und kulturelle Normen beeinflussen die Nutzung von Informations- und Kommunikationstechnologien, weshalb Akkaya et al. (2012a, b) diese Variable in ihrer Forschung zu e-Government für ganz zentral erachteten. Sie klassifizieren Deutschland auf Basis des Unsicherheits-Vermeidungs-Index (Uncertainty Avoidance Index, UAI) als relativ risikoavers (als stark risikoavers gilt Griechenland, als stark risikotolerant gilt Singapore). Die Annahme, dass die *German Angst* die Nutzung von eID beeinflusst, ist daher theoretisch plausibel, vorausgesetzt die *Angst* wird dabei nicht als etwas ausschließlich Deutsches angenommen.

Selbst wenn Deutsche sich aufgrund kultureller Filter und (auch historischer) Erfahrungen besonders zurückhalten, können die wahrgenommenen Belohnungen dies doch teilweise ausgleichen. So fokussiert etwa das Technologie-Akzeptanz-Modell (z. B. Venkatesh und Davis 2000) auf den wahrgenommenen Nutzen (perceived benefits) neuer Technologien, der sich untergliedern lässt in a) die wahrgenommene Nützlichkeit (perceived usefulness), definiert als der Grad, zu dem eine Person die Nutzung eines Systems für eine Verbesserung ihrer Leistung hält, und b) den wahrgenommene Nutzungskomfort (perceived ease of use), definiert als Grad, zu dem eine Person die Nutzung eines Systems für mühelos hält. Wenn der Nutzen von eID als gering erachtet wird, wird demnach auch deren Nutzung gering sein. Dies betrifft sowohl den Teil der Nutzerinnen und Nutzer, die sich nicht unbedingt zur Nutzung gedrängt fühlen, als auch für den Part der Verwaltung, wo es keinen unmittelbaren Implementierungsdruck gibt. Besonders in einer insgesamt risiko-

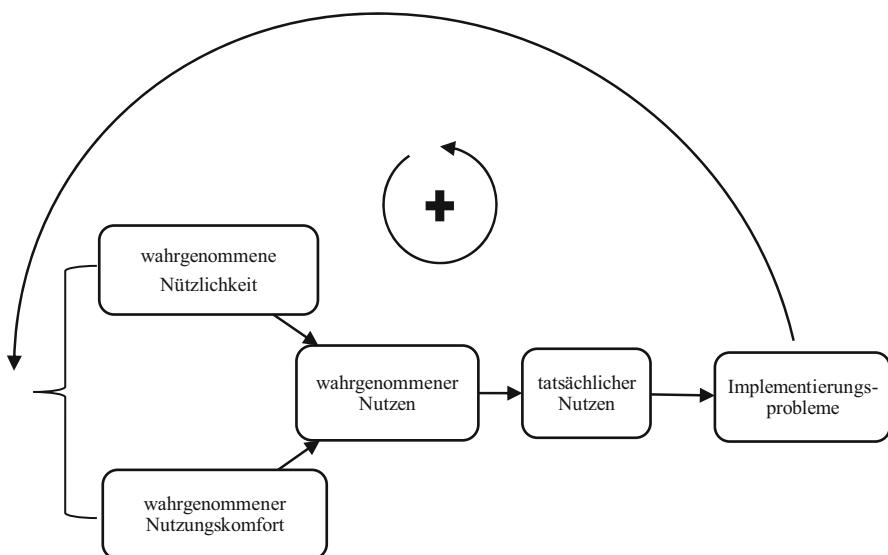
aversen Kultur gibt es dann wenig Anreize für alle Beteiligten, die Nutzung der eID voranzutreiben.

Natürlich wird die Akzeptanz einer Technologie auch von der tatsächlichen, praktischen Verfügbarkeit der Technologie beeinflusst. Dies lenkt unseren Blick auf Implementierungsprobleme neuer Technologien. Insbesondere zwei Faktoren könnten die Implementierungsschwierigkeiten in Deutschland steigern, nämlich (a) seine föderale Verfassung und (b) seine Rechtsstaatstradition. Die erste Eigenschaft bedeutet, dass die Bundesregierung die Länder und Kommunen nicht einfach zwingen kann, die korrekten Maßnahmen umzusetzen. Die zweite Eigenschaft besteht in einer starken Rechtsstaatstradition im Verwaltungssystem. Neue Maßnahmen müssen mit einem ohnehin komplexen Satz von Regeln und Regulierungen in Einklang gebracht werden. Entsprechend mühselig ist die Implementierung. Anhaltspunkte dafür finden sich z. B. im Bereich der Umweltpolitik (Knill und Lenschow 1998). Somit wäre es also auch möglich, dem Bild Deutschlands als allgemeinem Digitalversager eine weitaus solidere theoretische Grundlage zu geben.

Tatsächlich werden in Theorien technologischer Übergänge (z. B. Geels 2002) häufig interagierende Kombinationen verschiedener Faktoren auf unterschiedlichen gesellschaftlichen Ebenen identifiziert, wobei der Übergang von einer Technologie zur nächsten (hier: von papierbasierter ID zu eID) dann vom Zusammenspiel technologischer und sozialer Faktoren abhängt. Wir bewegen uns somit von statischen Ansätzen hin zu dynamischen Mehr-Ebenen-Erklärungen: Intuitiv erscheint es zwar einleuchtend, eID als eine Art ‚Eintrittskarte‘ für umfassendere Formen der e-Governance zu betrachten und sie daher an den Anfang zu setzen. Gleichwohl hängt die eID-Nutzung ebenso von bereits funktionierenden e-Governance-Strukturen ab, die Nützlichkeit und Komfort mit sich bringen. Solch eine dynamische, ko-evolutionäre Perspektive spricht außerdem dem Faktor Zeit eine weitaus größere Rolle zu: Nur weil eine Technologie zu einem bestimmten Zeitpunkt verfügbar ist, wird sie nicht zwangsläufig auch sofort genutzt. Vielmehr muss erst ein Momentum durch verfügbare Anwendungen geschaffen werden, welche die Nutzung anregen, während die Nutzung wiederum weitere Anwendungen auslöst usw.

Abb. 1 fasst das Argument zusammen: Die Technologie-Akzeptanz einerseits und die Implementierungsprobleme andererseits bilden zusammen eine Rückkopplungsschleife (feedback loop): Je mehr Menschen die Technologie nutzen, umso leichter wird die Überwindung von Implementierungsproblemen. Doch werden die Menschen nicht besonders begierig darauf sein, die Technologie zu nutzen, wenn Implementierungsprobleme weiterhin bestehen. Insgesamt sollten Erklärungsansätze also schon allein deshalb über das Klischee der *German Angst* hinausgehen, weil die aktuelle Situation kaum auf einen Einzelfaktor zurückzuführen ist. Wir wenden uns nun einigen empirischen Merkmalen der Lage in Deutschland zu.

Die Lage in Deutschland kann nur im Vergleich mit anderen Ländern verstanden werden. Wir betrachten zunächst den sozio-kulturellen Kontext, in dem eID implementiert und genutzt wird. Einige der Ergebnisse des 2011 veröffentlichten „Special Eurobarometer 359“ zu „Einstellungen zu Datenschutz und elektronischer Identität in der Europäischen Union“ werden hier skizziert, da sie immer noch wichtige



**Abb. 1** Das Technologie-Akzeptanz-Modell bildet zusammen mit Implementationsproblemen einen Rückkopplungseffekt (feedback loop). Dies geschieht im jeweiligen kulturellen Kontext

Hinweise auf themenspezifische Risikowahrnehmungen geben. Die Frage, ob etwa die Preisgabe von Informationen eine „große Sache“ ist, verneint eine knappe Mehrheit in Dänemark, gefolgt von absolutem Gleichstand (47 % dafür/dagegen) in Estland, wiederum dicht gefolgt von Schweden, an einem Ende der Skala. Das andere Extrem bildet Frankreich, wo lediglich 23 % keine große Sache darin sehen, 74 % aber sehr wohl. Deutschland ähnelt hier eher Frankreich (30 % sehen keine große Sache, 68 % schon) (Europäische Kommission 2011, S. 30). Ein ähnliches Bild findet sich hinsichtlich der Wahrnehmung der Risiken des Online-Einkaufs. Darüber hinaus sollte angemerkt werden, dass tatsächliche Erfahrungen mit Daten- oder Identitätsdiebstahl diese Unterschiede nicht widerspiegeln, da beispielsweise direkte Erfahrungen der Befragten mit solchen Vorfällen sowohl in Frankreich und Estland niedrig, in Schweden und dem Vereinigten Königreich aber eher hoch sind (Europäische Kommission 2011, S. 133). Akkaya et al. (2012b) finden kulturell bedingte Unterschiede zwischen deutschen und schwedischen Wahrnehmungen von e-Governance insgesamt, wenngleich die Unterschiede überraschend klein sind: Befragte Deutsche betonen Datenschutzaspekte etwas stärker als die befragten Schweden, die mehr Wert auf Komfort legen. Die geringen Differenzen könnten wahlgemerkter auch darin begründet liegen, dass ausgerechnet eine Online-Umfrage die Datengrundlage der Studie bildete. Zumindest bestätigen bisherige Erkenntnisse zu kontextspezifischen Risikowahrnehmungen damit tendenziell den kulturellen Erklärungsansatz der entsprechenden eID-Nutzungsraten in Deutschland und Frankreich einerseits, sowie Schweden und Estland andererseits.

Der Rückkopplungseffekt zwischen Implementierung, Komfort, Nutzung, weiterer Implementierung und Entwicklung vollzieht sich vor einem kulturellen Hintergrund (siehe Abb. 1). Wie bei allen Rückkopplungsschleifen gibt es keinen klaren Anfangspunkt. Allerdings erscheint eine nähere Betrachtung der Implementierung hier sinnvoll. So sollte nicht außer Acht gelassen werden, wie schwierig insbesondere die Umsetzung von eID in den Kommunen vor Ort sein kann. Dies gilt besonders für Kommunen in föderalen Systemen, die grundsätzlich mehr Implementierungslasten tragen. Die bereits erwähnte Lage in Italien liefert einen Anhaltpunkt für diese These. Auch die Tatsache, dass Bund und Länder in Deutschland erst kürzlich Fördergelder für digitale Modellkommunen bereitgestellt haben, deutet in diese Richtung (BMI 2016). Mit der Ausnahme Belgiens scheinen vor allem stärker zentralisierte Staaten (Estland, die Niederlande, Schweden) die eID schneller zu implementieren (vgl. Tab. 1).

Empirische Anhaltspunkte gibt es allerdings auch für den Einfluss von Rechtsstaatstraditionen. Der Deutsche Bundestag (2017) bemerkt in seinem Evaluierungsbericht:

Dass nur rund ein Viertel dieser Behörden bisher die eID-Funktion einsetzt (12,0 %) bzw. plant diese einzusetzen (14,0 %) ist zum Teil darin begründet, dass die rechtliche Verpflichtung zum Einsatz der eID-Funktion nicht immer eindeutig zu bestimmen ist. Lösungsansätze bieten hier verbindliche Vorgaben durch die rechtliche Verankerung der Online-Ausweisfunktion in Fachgesetzen (Deutscher Bundestag 2017, S. 23).

In Frankreich verhinderten rechtliche Argumente die Bereitstellung von eID sogar gänzlich. Vorreiter wie die Niederlande oder Schweden dagegen folgen eher den Prinzipien des New Public Management (NPM), welche die Entwicklung von Systemen priorisieren, die dann später in bestehende Regeln und Regulierungen eingepasst werden.

Föderalismus und Rechtstaatsprinzipien stellen vermutlich einen Teil der Schleife dar, während ein weiterer Teil den Nutzen der Technologie betrifft. Hier geht es darum, was die Technologie bietet und wie einfach oder schwierig es ist, die Technologie zu erwerben und zu nutzen. Deutschland schneidet hier im Vergleich zu den anderen Ländern nicht sehr gut ab. Erst seit Kurzem brauchen Nutzerinnen und Nutzer keinen Desktop-PC und Kartenleser mehr. Ein Beispiel für den eher unkomfortablen Gebrauch ist die BAföG-Rückzahlung. Hier wurde die bestehende Identifikationsmöglichkeit per E-Mail-Adresse und Passwort lediglich um die Alternative der eID-Nutzung „erweitert“ (Deutscher Bundestag 2017, S. 64), wobei der resultierende Mehrwert nicht leicht zu erkennen ist und erst seit Anfang 2016 überhaupt besteht. Von 18.000 monatlich gestellten Anträgen werden nur vier Prozent (ca. 720) unter Nutzung der eID gestellt (Deutscher Bundestag 2017, S. 65), was natürlich im Kontext der niedrigen Gesamtnutzungsrate der eID insgesamt gesehen werden kann, aber eben auch demonstriert, dass bestehende Anwendungen wenig Anreiz für die Beschaffung bieten.

Dagegen haben Estland und Schweden den Komfort von Beginn an in den Vordergrund gestellt, etwa mit dem Ergebnis der frühen Nutzung der eID per

Smartphone. Gleichwohl stellt Belgien erneut ein Gegenbeispiel dar, da hier eine hohe Nutzungsrate trotz der Kartenleser-anforderung besteht. Auch der Nutzungs-komfort kann somit nicht als alleinige Erklärung dienen, sondern ist Teil einer ganzen Reihe von Faktoren. Interessanterweise erwähnt der Bundestagsbericht auch die Wichtigkeit von Anwendungsfällen wie der BAfÖG-Rückzahlung für die Schaf-fung höherer Akzeptanz *auf Behördenseite*.

Letztlich spielt in dem hier angenommenen dynamischen Rückkopplungsprozess auch der Faktor Zeit eine wichtige Rolle. Tatsächlich hatten wir bereits im Überblick der eID-Formate auf die hohen Nutzungs-raten der Vorreiterländer wie Schweden und Estland verwiesen. Für Schweden ließe sich begründet Folgendes argumentie-ren: Die kulturell bedingte Einschätzung der Risiken (als eher niedrig) begünstigte eine frühe, auf den Nutzungskomfort statt auf die Sicherheit ausgerichtete Ein-führung, die darüber hinaus nicht durch föderale Strukturen verlangsamt wurde. In Deutschland hingegen wurde einerseits die Sicherheit selbst immer als Vorteil des neuen Personalausweises hervorgehoben, gleichzeitig aber von Experten bezweifelt. Zudem wird noch im 2016 verfassten Bundestagsbericht davon gesprochen, eID-gebundene Konten von Bund, Ländern und Kommunen *künftig* zu vernetzen (Deutscher Bundestag 2017, S. 71). Dagegen hat der Staat im Falle der elektroni-schen Steuerklärung (ELSTER), die auch ohne Kopplung an die eID nutzbar war, zunächst einige starke Anreize gesetzt, dadurch Nützlichkeit und Komfort garantiert (Akkaya et al. 2012a), und erreicht seither stetig steigende Nutzungs-raten. Somit scheint eine Dynamik hin zu hohen Nutzungs-raten vergleichbarer Technologien auch in Deutschland möglich, wobei höhere Nutzungs-raten nicht zuletzt eine Frage der Zeit sind.

Eine solch komplexe Interaktion verschiedener Erklärungsfaktoren deutet sich bereits in dem von Herbert Kubicek (2010) herausgegebenen Werk an und konnte dort auch beispielsweise für den Fall Estland schon recht detailliert aufgezeigt werden. Sie bestätigt sich empirisch auch in diesem fast zehn Jahre später und insbesondere auf die Erklärung der Nutzungs-rate in Deutschland fokussierten Beitrag.

---

## 5 Künftige Entwicklung

Angesichts der geringen Nutzungs-rate der eID-Funktion des neuen Personalauswei-ses hat der Bundestag im Juli 2017 die automatische und dauerhafte Einschaltung bei jedem Ausweis, die Vereinfachung des Genehmigungsverfahrens zur Nutzung der eID-Funktion für Dienstanbieter (Unternehmen und Behörden), sowie eine Erwei-terung der Anwendungsmöglichkeiten beschlossen. Dies wurde medial als Versuch bezeichnet, „das tote Pferd“ wiederzubeleben (Kühl 2017). Wie ist diese eher pessimistische Einschätzung der künftigen Entwicklung im Lichte der vorangegan-genen Betrachtung zu bewerten?

Tatsächlich kann die automatische Aktivierung allenfalls eine kleine Hürde beseitigen, wird aber an sich kaum zu einer höheren Nutzung führen. Denn wie bei jeder Rückkopplungsschleife gibt es keinen genauen Start- oder Endpunkt. Gleichwohl scheint das verabschiedete Gesamtpaket zumindest die richtigen

Ansätze zu beinhalten, auch wenn zu diesem Zeitpunkt keine umfassende Prüfung möglich ist: Die vereinfachte Genehmigung für Anbieter behandelt den oben genannten Rechtstaatsaspekt; die Erweiterung des Angebots könnte die Nützlichkeit der eID steigern; und die ebenfalls genannten Fördermittel des Bundes und der Länder für die kommunale Umsetzung könnte den Föderalismusaspekt adressieren. Werden die unterschiedlichen Maßnahmen umgesetzt, so könnte auf Dauer die Nutzungsrate der eID in Deutschland steigen. Denn wie in den vorangegangenen Abschnitten beschrieben, hilft es bei dieser Form von Schleifen nicht, bloß einen Faktor zu ändern, sondern es bedarf der Formierung neuer Rückkopplungsschleifen. Ein weiteres Mittel wäre die einfachere Handhabung der Digitalfunktion des Personalausweises; mit mit der zur Verfügungstellung der Smartphone-App wurde hier ein erster Schritt gemacht. Teil hierfür ist auch der weitere Ausbau der digitalen öffentlichen Verwaltung und somit ein größeres digitales Nutzungsangebot, welches einen weiteren Anreiz zur Nutzung der digitalen Technologie bieten kann. Offen ist allerdings, ob eine mögliche, erst spät einsetzende Dynamik nicht frühzeitig wieder gestoppt wird, falls private Anbieter und/oder neue Technologie (Stichwort: Block-chain) attraktivere funktionale Alternativen bieten. Ob der Faktor Zeit letztlich also ein Aufschließen Deutschlands bezüglich der Nutzungsrate des elektronischen Personalausweises erlaubt oder dessen Ende besiegt, bleibt abzuwarten.

---

## Literatur

- Akkaya, Cigdem, Petra Wolf, und Helmut Krcmar. 2012a. Factors influencing citizen adoption of E-government services. A cross-cultural comparison. Papier vorgestellt auf der 45th Hawaii International Conference on System Sciences. <https://pdfs.semanticscholar.org/f390/2979be2ac9a6df970e9e2edbda41d86829c2.pdf>. Zugegriffen am 12.05.2018.
- Akkaya, Cigdem, Petra Wolf, und Helmut Krcmar. 2012b. The surprisingly low effect of national culture on E-government adoption. A cross-cultural comparison. Association for Information Systems (AIS Electronic Library, AMCIS 2012 proceedings). <http://aisel.aisnet.org/cgi/content.cgi?article=1135&context=amcis2012>. Zugegriffen am 12.05.2018.
- Bundesministerium des Innern, für Bau und Heimat. (BMI). 2016. Digitale Verwaltung 2020 – Evaluierungsbericht 2016.
- Deutscher Bundestag. 2017. Digitale Verwaltung 2020 – Evaluierungsbericht 2016. Drucksache 18/12512. <http://dipbt.bundestag.de/doc/btd/18/125/1812512.pdf>. Zugegriffen am 12.05.2018.
- Europäische Kommission. 2011. Special eurobarometer 359. Attitudes on data protection and electronic identity in the European Union. [http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs\\_359\\_en.pdf](http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf). Zugegriffen am 12.05.2018.
- Europäische Kommission. 2018. Digital single market – Trust services and eID. <https://ec.europa.eu/digital-single-market/en/trust-services-and-eid>. Zugegriffen am 12.05.2018.
- Geels, Frank W. 2002. Technological transitions as evolutionary reconfiguration processes. A multi-level perspective and a case-study. *Research Policy* 31(8–9): 1257–1274.
- Knill, Christoph, und Andrea Lenschow. 1998. Coping with Europe. The impact of British and German administrations on the implementation of EU environmental policy. *Journal of European Public Policy* 5(4): 595–614.

- Kubicek, Herbert, Hrsg. 2010. *Identity in the information society 3 (1). Special issue: The diversity of national e-IDs in Europe. Lessons from comparative research.* Dordrecht: Springer.
- Kühl, Eike. 2017. Elektronischer Personalausweis. Das tote Pferd soll auferstehen. In *ZEIT ONLINE*. <https://www.zeit.de/digital/datenschutz/2017-04/elektronischer-personalausweis-eid-gesetz-biometrie-datenbank/komplettansicht>. Zugegriffen am 12.05.2018.
- PBLQ, Niederländisches Institut für öffentliche Verwaltung. 2015. International comparison eID means, Final report. Vergleichsstudie im Auftrag des niederländischen Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. <https://www.government.nl/documents/reports/2015/05/13/international-comparison-eid-means>. Zugegriffen am 12.05.2018.
- Venkatesh, Viswanath, und Fred D. Davis. 2000. A theoretical extension of the technology acceptance model. Four longitudinal field studies. *Management Science* 46(2): 186–204.



# Digitale Betriebsprüfung

Peter Fettke

## Inhalt

1 Klärung des Begriffs .....	554
2 Theoretische Grundlagen .....	555
3 Praktische Anwendung .....	557
4 Umsetzungsstand und Auswirkungen .....	561
5 Perspektiven für Staat und Verwaltung .....	562
Literatur .....	563

## Zusammenfassung

Betriebsprüfungen bezeichnen die rechtlich legitimierte Überprüfung der von einem Steuerpflichtigen entrichteten Steuern durch die Finanzverwaltung, die grundsätzlich sämtliche Steuerarten umfassen kann. Aufgrund der zunehmend digitalen Aufzeichnung der relevanten Geschäftsvorfälle in einem Unternehmen hat sich bereits frühzeitig der Bedarf einer digitalen Betriebsprüfung gezeigt. Inzwischen entstehen durch die Digitalisierung weitere Möglichkeiten, die sich nicht nur in einer Vollprüfung sämtlicher steuerlich relevanter Daten eines Betriebs zeigen, sondern auch einen Wandel des Selbstverständnisses der Finanzverwaltung in Richtung einer Dienstleistungsorientierung eröffnen.

## Schlüsselwörter

Betriebsprüfung · Digitalisierung · Datenanalytik · Künstliche Intelligenz · Automatisierung

---

P. Fettke (✉)

Universität des Saarlandes und Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI),  
Saarbrücken, Deutschland

E-Mail: [Peter.Fettke@dfki.de](mailto:Peter.Fettke@dfki.de)

## 1 Klärung des Begriffs

Steuern und Zölle sind seit dem Altertum und der Antike bekannt, wobei ihre Bedeutung in den vergangenen Jahrhunderten erheblich zugenommen hat: In modernen Staaten bilden sie das zentrale Instrument zur Finanzierung des Gemeinwesens und zur Lenkung der in einem Land ein- beziehungsweise auszuführenden Wirtschaftsgüter. Auch die Art und Weise der Besteuerung hat sich erheblich geändert. Während in frühen Besteuerungssystemen noch Steine und Tontafeln Verwendung fanden, wurden später Belege und Bücher aus Papier genutzt. Inzwischen sind auch digitale Aufzeichnungen der Finanzströme gängige Praxis im Steuerbereich.

Steuern werden hier in einem weiten Sinne als staatliche Abgaben ohne konkrete Gegenleistungen verstanden, die auch Zölle umfassen. Der Staat ist rechtlich ermächtigt zu überprüfen, ob die zu leistenden Steuern korrekt abgeführt werden. Hierdurch soll neben der Korrektheit auch die Gleichmäßigkeit und Fairness der Besteuerung aller Steuerpflichtigen sichergestellt werden.

Eine Aufgabe der Finanzverwaltung ist es, Prüfungen der Steuerpflichtigen vorzunehmen. Die Prüfungen sind sowohl bei Betrieben als auch Privatpersonen möglich, wobei im Folgenden ausschließlich Betriebsprüfungen betrachtet werden. In der Terminologie der Finanzverwaltung wird die Betriebsprüfung als Außenprüfung bezeichnet. Die Betriebsprüfung ist eine rechtlich legitimierte Gesamtüberprüfung steuerlich relevanter Sachverhalte. Sie bezweckt die Ermittlung, Prüfung und Beurteilung der Verhältnisse eines Steuerpflichtigen. Die Betriebsprüfung stellt – ähnlich wie die Steuerfahndung – einen umfangreichen Eingriff in die Rechte des Steuerpflichtigen dar, sodass hier vielfältige rechtliche Voraussetzungen und Vorschriften für die Finanzverwaltung gelten.

Die Prüfung des Betriebsprüfers kann sich auf sämtliche Steuerarten beziehen. Die ordnungsgemäße Erhebung und Abführung der Beiträge zur Sozialversicherung wird ebenfalls durch Betriebsprüfungen gesichert. Die von der deutschen Zollverwaltung durchzuführenden Prüfungen auf dem Gebiet der Zölle und des Außenwirtschaftsverkehrs werden rechtlich den steuerlichen Betriebsprüfungen gleichgestellt.

Neben der Sicherstellung der Korrektheit, Gleichmäßigkeit und Fairness der Besteuerung sind weitere Aspekte zu berücksichtigen, die sich aus der Arbeitsweise der Finanzverwaltung und den Nutzungsmöglichkeiten bei der Digitalisierung ergeben. Erstens müssen *Compliance*-Maßnahmen seitens der Finanzverwaltung aufwandsarm und wirtschaftlich ausgestaltet werden. Zweitens sind Belastungen für die Steuerpflichtigen zu reduzieren. Drittens ist das Vertrauen in die Besteuerungssysteme nicht nur zu erhalten, sondern möglichst auszubauen. Da inzwischen eine Fülle der zur Prüfung relevanten Daten digital gespeichert werden, ist es notwendig, Betriebsprüfungen auch auf digital gespeicherte Informationen auszudehnen.

Neben den fachlichen Erfordernissen der Betriebsprüfung entsteht zusätzlich ein Technologiedruck: neue Technologien der Datenverarbeitung, beispielsweise Datenanalytik auf betrieblichen Massendaten, Künstliche Intelligenz und *Blockchain* erlauben neue Ansatzpunkte für die digitale Betriebsprüfung. Statt beispielsweise nur wenige ausgewählte Datensätze zu analysieren, sind umfangreichere Prüfungen bis hin zu einer Analyse des vollständigen steuerlich relevanten Datenbestands eines

---

Betriebes denkbar. Die technischen Veränderungen ermöglichen es, die Arbeitsweise von Steuerverwaltungen zu überdenken.

Der Steuer- und Zollbereich ist in vielen Aufgaben als Anwendungsfeld klar abgegrenzt und stark geprägt durch ein fachspezifisches Vokabular. Viele der Aufgaben sind hoch repetitive Routinetätigkeiten und beruhen häufig auf großen Datenmengen. Das alles sind beste Voraussetzungen für eine weitergehende Digitalisierung und Automatisierung von Aufgaben im Bereich der Betriebsprüfung und weiteren Aufgaben in der Finanzverwaltung. Hier entsteht aufgrund der Digitalisierung ein interessantes Feld für Veränderungen in Staat und Verwaltung, das im Folgenden nicht umfassend, sondern konkret anhand der Digitalisierung der Betriebsprüfung beschrieben wird.

Die Digitalisierung der Betriebsprüfung hat spätestens seit dem BMF-Schreiben „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)“ vom 16. Juli 2001 eine praktische Relevanz gewonnen, weil damit ab Januar 2002 diverse rechtliche Pflichten zum Umgang mit digitalen Daten (digitale Rechnungen, Belege etc.) im Unternehmen rechtlich konkretisiert wurden. Dabei ist zu beachten, dass zurzeit unter dem Schlagwort „Digitalisierung“ nicht mehr nur die maschinelle Erfassung, Speicherung, Übertragung und Verarbeitung verstanden wird. Es geht heute nicht mehr um *maschinenlesbare*, sondern um *maschinenverstehbare* Daten: Daten werden mithilfe von Methoden der Informatik und Künstlicher Intelligenz, insbesondere dem maschinellen Lernen, automatisch ausgewertet, verstanden und aktiv genutzt. So können Maschinen inzwischen die auf Bildern dargestellten Personen oder Gegenstände eigenständig erkennen, aus radiologischen Aufnahmen medizinische Diagnosen stellen oder aus Videodata des Straßenverkehrs Automobile autonom steuern.

Diese neuen Anwendungen bilden eine zweite Welle der Digitalisierung und werden zunehmend auch in der digitalen Betriebsprüfung genutzt; gerade weil im Rahmen der ersten Welle der Digitalisierung in den 1980er- und 1990er-Jahren bereits vielfältige Voraussetzungen und Grundlagen zur digitalen Verarbeitung der Daten gelegt worden sind. Beispielsweise ist davon auszugehen, dass Anomalien oder Buchungsfehler durch Softwaresysteme automatisiert erkannt werden können. Auf diese Weise wird es möglich, in Datenspuren fehlerhafte oder problematische Buchungen aufzudecken oder Muster zu identifizieren, die auf ein derartiges fehlerhaftes Verhalten frühzeitig hinweisen.

---

## 2 Theoretische Grundlagen

Theoretische Grundlagen der Betriebsprüfung ergeben sich zunächst aus den normativen Vorgaben der Gesetze eines Staates. Für Deutschland gelten beispielsweise die Abgabenordnung, das Gesetz zur Vereinfachung der Besteuerung und eine Reihe von anderen normativen Grundlagen. International ergeben sich unterschiedliche Entwicklungslinien mit vielfältigen individuellen Besonderheiten. Aufgrund der historisch unterschiedlichen Entwicklung der jeweiligen Staaten sowie der divergierenden Beurteilungsmaßstäbe ist eine allgemeine vergleichende Einschätzung kaum

möglich, insbesondere auch weil umfassende rechts-vergleichende theoretisch-deskriptive Untersuchungen der steuerlich und prüfungsrechtlich relevanten Rechtssysteme weitgehend unbekannt sind.

Neben den rechtlich-normativen Grundlagen bestehen vielfältige konzeptionelle und empirisch-behavioristisch geprägte theoretische Bezugspunkte. Eine erste zentrale begrifflich-konzeptionelle Frage ergibt sich bei der Definition des Ergebnisses einer Betriebsprüfung. Im einfachsten Fall kann in Anlehnung an das Prinzip „*tertium non datur*“ eine binäre Entscheidung getroffen werden: Eine Betriebsprüfung kann eine korrekte oder eine nicht korrekte Steuerdeklaration ergeben.

Zur näheren Differenzierung der Schwere eines steuerlichen Verstoßes taugt ein solches Begriffsverständnis allerdings nur bedingt. Allerdings kann begrifflich eine feinere Konzeption gewählt werden: Beispielsweise kann von einer ordinalen oder gar metrischen Konzeptualisierung ausgegangen werden. Eine ordinale Konzeption erlaubt bereits eine begriffliche Unterscheidung der Schwere des Deklarationsverstoßes, bspw. geringer, mittlerer und schwerer Verstoß. Ein metrisches Verständnis nutzt reelle Zahlen, um den Grad der Angemessenheit einer Steuerdeklaration zu erfassen.

Die begriffliche Diskussion darf nicht als eine der „Spitzfindigkeiten im akademischen Elfenbeinturm“ verstanden werden, sondern ist aus unterschiedlichen Gründen von hoher praktischer Relevanz. Erstens muss bei einer digitalen Betriebsprüfung ein algorithmisches Ergebnis und eine entsprechende technische Implementierung vorgenommen werden. Hier macht es einen Unterschied, ob der Algorithmus als Ergebnis, eine (nicht) korrekte Prüfung ermittelt oder weitere Abstufungen und Prüfungsdetails bietet.

Zweitens zeigen behavioristische Untersuchungen der Auswirkungen alternativer Steuersysteme, dass bestimmte Anreize das Verhalten der Steuerpflichtigen im Allgemeinen und bei der konkreten Steuerdeklaration erheblich beeinflussen können. Vor diesem Hintergrund ist es mehr als sinnvoll, Anreize zu schaffen, die eine korrekte Besteuerung unterstützen. Dieser Weg wird von einzelnen Staaten bewusst gewählt; beispielsweise kann es sinnvoll sein, bei leichten Fällen eines Steuerdeklarationsverstoßes andere Maßnahmen zu ergreifen als bei schweren Verstößen gegen Steuerregularien.

In diesem Zusammenhang ist auf einen weiteren theoretischen Gestaltungsaspekt hinzuweisen: Die Betriebsprüfung kann sich entweder am theoretischen Bezugsrahmen „Polizist-Verbrecher“ oder „Kunde-Dienstleister“ orientieren. Empirisch-deskriptive Untersuchungen zeigen insbesondere im internationalen Vergleich erhebliche Unterschiede. Diese Fragen sind gerade bei der Implementierung einer digitalen Betriebsprüfung von grundsätzlicher Bedeutung: Soll die Digitalisierung der Finanzverwaltung Verbrecher aufspüren oder auch Betriebe bei der korrekten Abführung ihrer Steuern unterstützen? Es ist klar, dass dies keine dichotome Entscheidung sein muss; allerdings ist auch klar, dass bei den normativen Vorgaben der Gesetzgeber nicht einseitig die Belange der Finanzverwaltung unterstützen kann, sondern auch die des Steuerpflichtigen berücksichtigen muss. Für die Attraktivität eines Steuerstandortes kann es von großer Bedeutung sein, auch andere theoretische Leitbilder zu verfolgen.

In diesem Zusammenhang sind auch die Kosten der Besteuerung zu berücksichtigen. Hierzu gibt es verschiedene theoretische Überlegungen, sie aufgrund der

Digitalisierung anders auszustalten. Beispielsweise sinken Kosten für die Dateneingabe seitens der Finanzverwaltung, wenn Daten vom Steuerpflichtigen digital übermittelt werden. Andererseits kann das die Kosten für den Steuerpflichtigen erhöhen, insbesondere dann, wenn das gesetzlich vorgeschriebene Datenformat nur mit erheblichen Aufwendungen automatisiert erzeugt werden kann.

Für die theoretische Analyse der Zusammenhänge sind spieltheoretische Ansätze interessant, in denen die Handlungen verschiedener Akteure modelliert werden können. Die Notwendigkeit hierfür zeigt folgendes Beispiel: Wenn digitale Betriebsprüfungen zu einer größeren Prüfungstiefe seitens der Finanzverwaltungen führen, verringern sich die Anreize für Steuerpflichtige, von Steuerregeln abzuweichen, da diese mit einer höheren Wahrscheinlichkeit erkannt werden. Folglich verbessert sich das Steuerverhalten des Steuerpflichtigen, was wiederum die Notwendigkeit einer höheren Prüfungstiefe reduziert.

Neben den genannten theoretischen Bezugspunkten existieren vielfältige technische Grundlagen, die bei der digitalen Betriebsprüfung zu beachten sind. Neben allgemeinen Digitalisierungsbestrebungen der öffentlichen Verwaltung wie sie sich beispielsweise durch das *E-Government-Gesetz* oder die Grundsätze der elektronischen Aktenführung und des ersetzen Scannens ergeben, sind im Steuer- und Zollbereich exemplarisch in Deutschland zu nennen:

- die Pflicht zur Erstellung elektronischer Bilanzen auf Basis einer Taxonomie in XBRL (<http://www.esteuere.de/>),
- die Abgabe elektronischer Steuererklärungen über ELSTER (<https://www.elster.de/>),
- das automatisierte Tarif- und Zollabwicklungssystem ATLAS ([http://www.zoll.de/DE/Fachthemen/Zoelle/ATLAS/atlas\\_node.html](http://www.zoll.de/DE/Fachthemen/Zoelle/ATLAS/atlas_node.html)) und
- die Ausstellung elektronischer Rechnungen mit ZUGFeRD (<http://ferd-net.de/>).

Dabei ist zu berücksichtigen, dass die genannten technischen Grundlagen spezifisch für Deutschland gelten. Europa- und weltweit existieren sehr unterschiedliche Systeme, deren konkrete Vor- und Nachteile in der Regel nur schwer miteinander verglichen werden können, da sie zum Teil von sehr spezifischen Voraussetzungen und Randbedingungen sowie divergierenden Bewertungsmaßstäben ausgehen. Beispielsweise müssen spanische Betriebe bestimmter Größenklassen ihre Registrierbücher für Umsatzsteuer unterjährig elektronisch an die Finanzverwaltung melden. In Brasilien wurde ein System geschaffen, das die staatliche Registrierung einzelner Rechnungen unterstützt.

---

### 3 Praktische Anwendung

Bei den praktischen Anwendungen der Digitalisierung von Betriebsprüfungen sind mindestens Anwendungen in der Finanzverwaltung, beim Steuerpflichtigen und des Steuerberaters zu unterscheiden. Die drei Anwendungsfelder werden im Folgenden näher erläutert:

1. Die Finanzverwaltung hat verschiedene Anwendungen, um konkrete Prüfungen bei einem Betrieb vorzunehmen. Hier gibt es insbesondere Möglichkeiten, einen einzelnen Betrieb zu analysieren oder verschiedene Betriebe miteinander zu vergleichen.
2. Der Steuerpflichtige muss erstens den gesetzlichen Vorgaben einer Digitalisierung der Betriebsprüfung nachkommen können. So sind entsprechende Maßnahmen zu ergreifen, um die verschiedenen gesetzlich vorgeschriebenen Zugriffarten zu ermöglichen. Darüber hinaus ergeben sich Anwendungen für Unternehmen, um sich auf die digitale Betriebsprüfung und die dabei entstehenden Nach- und Rückfragen besser vorbereiten zu können. Typische Anwendungsfelder ergeben sich hier bei der Simulation von Betriebsprüfungen, die Fragen aufwerfen oder Auffälligkeiten aufdecken kann.
3. Steuerberater können mithilfe von Standardanwendungen zur Betriebsprüfung Mandanten unterstützen. Hierbei ist zu beachten, dass große Unternehmen in der Regel Steuerabteilungen unterhalten, die nennenswerte Größen erreichen. Steuerabteilungen ab einer bestimmten Mindestgröße verfügen über ausreichend Erfahrungen und Ressourcen, um die zuvor genannten Anwendungen aus eigenen Kräften zu realisieren. Für kleinere Steuerabteilungen oder für Unternehmen, die über gar keine Steuerabteilung verfügen, ist es naturgemäß nicht nur schwierig, sondern schlicht und einfach nicht zu realisieren. Hieraus ergibt sich insbesondere für Steuerberater die Möglichkeit, vielfältige Anwendungen für eine Unterstützung der digitalen Betriebsprüfung vorzuhalten und dem Mandanten anzubieten.

Aufgrund der skizzierten gesetzlich-normativen Vorgaben spielen die Anwendungen der Finanzverwaltung bei der digitalen Prüfung der Steuerpflichtigen eine besondere Rolle. In Deutschland sind gesetzlich drei Formen des Datenzugriffs zu unterscheiden:

1. unmittelbarer Zugriff (Z1): Der Prüfer kann die Softwaresysteme des Steuerpflichtigen unmittelbar nutzen. Dafür werden dem Prüfer entsprechende Zugriffsmöglichkeiten auf die steuerlich relevanten Daten eingeräumt. Der Prüfer erhält keine Schreibrechte auf den Datenbestand, sondern nur Leserechte. Die vom Softwaresystem zur Verfügung gestellten Analyse- und Prüffunktionen darf auch der Prüfer nutzen. Ein Recht auf den Einsatz zusätzlicher Funktionen besteht nicht. Allerdings hat der Prüfer weitergehende Möglichkeiten zur Datenanalyse. Der unmittelbare Datenzugriff erfolgt in den Geschäftsräumen des Steuerpflichtigen.
2. mittelbarer Datenzugriff (Z2): Der Steuerpflichtige erhält vom Prüfer Vorgaben zur Datenauswertung. Nach diesen Vorgaben ist der Steuerpflichtige verpflichtet, seine Datenbestände auszuwerten. Die Ergebnisse der Datenauswertung sind dem Prüfer zu übermitteln.
3. Datenträgerüberlassung (Z3): Die steuerrelevanten Daten des Steuerpflichtigen werden vollständig oder in Teilen auf Datenträger übertragen und dem Betriebsprüfer überlassen. Die Auswertung der Daten erfolgt außerhalb der Geschäftsräume.

räume des Steuerpflichtigen, also mithilfe eigener Anwendungen der Finanzverwaltung. Nach Abschluss der Prüfung ist die Finanzverwaltung verpflichtet, den Datenträger wieder an den Steuerpflichtigen zurückzugeben beziehungsweise alle ihr überlassenen Daten oder Kopien zu löschen.

Der Datenzugriff der Finanzverwaltung ist grundsätzlich beschränkt auf steuerlich relevante Daten. Relevante Daten umfassen regelmäßig Daten der Finanz-, Anlagen- und Lohnbuchhaltung. Dabei sind nicht nur die Daten der Hauptsysteme, sondern auch Daten der Vor- und Nebensysteme von Relevanz und können folglich Gegenstand der Prüfung werden. Inwieweit Daten steuerlich relevant sind, ist gleichwohl im Einzelfall zu prüfen. Da allerdings in hochintegrierten betrieblichen Anwendungssystemen (sogenannte „ERP-Systeme“) weitgehend alle Geschäftsvorfälle und die damit zusammenhängenden Geschäftsprozesse abgebildet werden, ist in der Regel davon auszugehen, dass auch sämtliche Unterlagen, die mit der Abwicklung von Aufträgen systemseitig verknüpft sind, den steuerlich relevanten Daten zuzurechnen sind. Damit eröffnet sich der Finanzverwaltung ein breites Spektrum an Daten für eine digitale Analyse und Prüfung.

Bei der Betriebsprüfung ist neben den inhaltlichen Zielen der Korrektheit, Gleichmäßigkeit und Fairness der Besteuerung insbesondere zu berücksichtigen, dass der Prüfungsumfang und die Prüfungstiefe mit erheblichen Aufwänden verbunden sein kann. Derartige Kosten können zwar durch den Einsatz von IT-Systemen grundsätzlich gesenkt werden, allerdings ist eine Vollanalyse weiterhin nicht unproblematisch möglich. Daher sind die Aspekte der Wirtschaftlichkeit und Verhältnismäßigkeit zu wahren. Erst wenn bestimmte Verdachtsmomente vorliegen, Unstimmigkeiten aufgedeckt oder Plausibilitäten verletzt werden, kommt es zu einer vertieften Analyse bestimmter Prüffelder.

Zu beachten ist, dass die steuerlich relevanten Daten, die Gegenstand einer Betriebsprüfung sein können, inzwischen vielfältig zwingend digital vorgehalten werden müssen. So sind beispielsweise Voranmeldungen, zusammenfassende Meldungen der Umsatzsteuer und die Umsatzsteuererklärung elektronisch abzugehen. Derartige Datenmeldungen ermöglichen vielfältige Analysemöglichkeiten, wobei nicht nur auf Basis vorgegebener Regeln eine Prüfung vorgenommen werden kann. Vielmehr können diese Daten auch mit maschinellen Lernverfahren analysiert werden. Inwieweit derartige Anwendungen auch von den Finanzverwaltungen zum Einsatz kommen, ist unbekannt. Gleichwohl ist das erhebliche Anwendungspotenzial offenkundig, wie Erfahrungen mit derartigen Anwendungen im privatwirtschaftlichen Kontext belegen.

Es ist davon auszugehen, dass der Umfang der zwingend digital vorzuhaltenden Daten aus Effizienzgründen zukünftig zunehmen wird. Ein Verlust der Daten entbindet nicht von der Prüfungspflicht, sodass seitens des Steuerpflichtigen zusätzliche Maßnahmen für eine sichere Archivierung der steuerlich relevanten Datenbestände von hoher Bedeutung sind.

Die zuvor geschilderten Zugriffsmethoden ermöglichen eine direkte Prüfung eines Betriebs. Daneben gibt es inzwischen auch Möglichkeiten zur indirekten Prüfung verschiedener steuerlich relevanter Geschäftsvorfälle. Eine indirekte Prü-

fung erkennt Unstimmigkeiten und Fehler in der Buchführung, die aufgrund von Vergleichen mit anderen Betrieben oder Kennziffern Hinweise auf Auffälligkeiten geben. Diese Auffälligkeiten führen dann in einem zweiten Schritt zu einer tieferen Analyse bestimmter Prüfungsfelder. Hierzu zählen verschiedene Methoden, die regelmäßig im Zuge der Digitalisierung der Betriebsprüfung von den Finanzverwaltungen angewendet werden:

- **Betriebsvergleiche:** Der Betriebsvergleich untersucht ausgewählte Parameter in unterschiedlichen Prüfungsjahren oder im Vergleich mit anderen Betrieben. Beim inneren Betriebsvergleich werden verschiedene Prüfjahre eines Betriebs in Bezug auf bestimmte Kennzahlen miteinander verglichen. Eine typische Kennzahl ist beispielsweise der Rohgewinnaufschlagsatz, der sich aus dem Rohgewinn im Verhältnis zum Wareneinsatz ergibt. Derartige Vergleiche werden beim äußeren Betriebsvergleich mit Unternehmen ähnlicher Branche und Größe vorgenommen. Deutliche Abweichungen ergeben Anhaltspunkte für tiefere Analysen der Ursachen. Moderne Analysen erfolgen nicht nur zahlenbasiert, sondern auch mit Hilfe von grafischen Visualisierungen und Analysen.
- **Zeitreihenvergleiche:** Beim Zeitreihenvergleich werden im Unterschied zum Betriebsvergleich nicht ganze Prüfungsjahre analysiert, sondern kleinere Zeitintervalle wie einzelne Tage, Wochen, Monate oder Quartale untersucht. Auch können rollierende Analyseintervalle gebildet werden, um punktuelle Schwankungen und Zufälle auszugleichen. Abweichungen können jeweils mit statistischen Signifikanztests geprüft werden, wobei saisonale Einflüsse zu berücksichtigen sind.
- **Strukturanalyse:** Die Höhe der Tageseinnahmen oder Warenbestände sowie die Auftrags-, Umsatz- oder Rechnungssummen *et cetera* sind zufällig, gehorchen aber gewissen a-priori bekannten Wahrscheinlichkeitsverteilungen. Bei einer Strukturanalyse wird überprüft, ob die realisierten Werte tatsächlich den Annahmen der theoretischen Wahrscheinlichkeitsverteilung entsprechen oder ob hier Auffälligkeiten zu verzeichnen sind. Auffälligkeiten entstehen beispielsweise bei einzelnen Ausreißern (ein extrem hoher Umsatz) oder einer signifikanten Abweichung von der theoretisch erwarteten Wahrscheinlichkeitsverteilung (extrem viele geringe Umsätze oder fehlende Umsätze einer bestimmten Größenordnung). Gleichwohl ist darauf zu achten, dass entsprechende Werte nicht nur normalverteilt, sondern häufig auch logarithmisch-normalverteilt sind. Beispielsweise sind negative Umsätze nicht möglich, was Implikationen für die Verteilung hat. Zwar beweisen Abweichungen von theoretisch erwarteten Wahrscheinlichkeitsverteilungen kein steuerliches Fehlverhalten, liefern aber Anhaltspunkte für vertiefte Prüfungen.
- **Empirisch beobachtete Zifferverteilungen („Benford’s Law“):** Die Ziffern von numerischen Werten wie beispielsweise Umsätzen sind nicht gleich verteilt, sondern weisen unter in der Realität häufig erfüllten Annahmen unterschiedliche Häufigkeiten auf. Beispielsweise ist die Ziffer „1“ in einer 4-stelligen Zahl statistisch signifikant häufiger als andere Ziffern. Statistisch signifikante Abweichungen von diesen Besonderheiten deuten auf Manipulationen der entsprechenden Daten hin.

- Summarische Betriebsprüfung: Die summarische Betriebsprüfung ist ein umfassendes Prüfungsnetz verschiedener Prüfungsansätze und -routinen, die seit einigen Jahren systematisch weiterentwickelt und auch in Softwaresystemen wie beispielsweise IDEA angeboten werden. Dabei werden die oben genannten Analysen sowie weitere Prüfungen systematisch miteinander verknüpft und automatisiert. Hierbei werden insbesondere auch maschinelle Ansätze zur Musteranalyse in den Daten angewendet.

Die zunehmende Digitalisierung der Wirtschaft ermöglicht auch das Einsetzen digitaler Suchmaschinen und -agenten für die Betriebsprüfung. Beispielsweise können Internet-Verkaufsplattformen automatisiert nach bestimmten Anbietern oder Produktgruppen untersucht werden, um steuerlich problematische Anbieter oder Auffälligkeiten bei steuerlich relevanten Transaktionen zu identifizieren.

---

## 4 Umsetzungsstand und Auswirkungen

Am Markt existieren bereits seit Jahren umfassende Softwareprodukte für die Unterstützung der digitalen Betriebsprüfung auf Seiten der Finanzverwaltung und auch der Steuerpflichtigen. Gemäß den Aussagen der Anbieter entsprechender am Markt verfügbarer Standard-Werkzeuge werden diese auch intensiv eingesetzt. Umfassende wissenschaftlich-tragfähige Studien zur Akzeptanz, Nutzung, Evaluation und Wirkung derartiger technischer Lösungen sind öffentlich nicht bekannt, sondern offene Forschungsfragen.

Auch hat die Finanzverwaltung unterschiedliche Projekte gestartet, um individuelle Lösungen auf Basis neuer Methoden zu entwickeln. Beispielsweise wurden Erfahrungen mit derartigen Techniken seitens der Finanzverwaltung im Rahmen des Systems „XPIDER“ gemacht, das automatisch Handelnde auf Internetplattformen identifiziert und die zugrunde liegenden Geschäftsvorfälle analysiert hat.

Neben den bereits umfassend angewendeten Methoden gibt es inzwischen eine Reihe von technischen Entwicklungen, die sich erheblich auf zukünftige Anwendungsfelder auswirken. Exemplarisch seien folgende Entwicklungen genannt:

- Datenanalytik auf betriebliche Massendaten („Big Data Analytics“): Größere Datenmengen können systematisch für die Analysen eingesetzt und ausgewertet werden. Dies ermöglicht neue Ansätze für Branchenanalysen, Betriebsvergleiche, Auffälligkeiten im Zeitablauf, Betrugserkennung und IT-Forensik. Ansätze des *Process Mining* oder der Anomalieerkennung versprechen hier interessante Innovationen. Hierbei können auch Daten aus anderen Quellen, beispielsweise Daten aus sozialen Netzwerken oder Anbieterdaten auf Web-Seiten im Internet, genutzt werden.
- *Visual Analytics*: Die grafische Analyse von großen Datenbeständen ist inzwischen in vielen Anwendungen präsent und bietet sich auch bei der Analyse von Betriebsdaten an.

- Echtzeit-*Compliance*: Abläufe und Prozesse können so gestaltet werden, dass Abweichungen von den Vorgaben sofort von der Steuerverwaltung erkannt werden oder *Compliance*-Verstöße bereits im Systementwurf ausgeschlossen sind. Hier gibt es bereits diverse Pilotprojekte, die unter anderem beispielsweise auch auf der *Blockchain*-Technik arbeiten.
- Assistenzfunktionen für den Steuerpflichtigen: Autofahrer werden im Auto mit einem Navigationssystem und weiteren Assistenzsystemen unterstützt. Es ist davon auszugehen, dass Steuerverantwortliche im Unternehmen spezifische Unterstützungssysteme für die Steuerdeklaration und -analyse zur Verfügung gestellt bekommen. Hierbei ist insbesondere an zusätzliche Systeme zur Simulation von Betriebsprüfungen und die vorrausschauende Betriebsprüfung zu denken.
- Einsatz von neuen Methoden der Künstlichen Intelligenz: Konzepte und Techniken der Künstlichen Intelligenz wie robotergestützte Prozessautomatisierung, Sprachassistenzen, maschinelles Lernen und anderer Techniken der Künstlichen Intelligenz werden die Digitalisierung der Betriebsprüfung zunehmend unterstützen.

---

## 5 Perspektiven für Staat und Verwaltung

Die beschriebenen technischen Möglichkeiten eröffnen eine Reihe reizvoller Entwicklungsperspektiven:

- Wandel von einer Steuererhebungsorganisation hin zu einer Steuer-Service-Funktion: Im Rahmen der Digitalisierung sind neue Dienstleistungen der Finanzverwaltung denkbar. Beispielsweise bietet der Bereich der Steuer-*Compliance* umfangreiche Möglichkeiten, sodass die Finanzverwaltung den Steuerpflichtigen bei der Einhaltung von *Compliance*-Anforderungen unterstützt.
- *Open Data* in der Steuerverwaltung: Offene Daten in der Verwaltung spielen eine große Rolle in verschiedenen Bereichen, insbesondere auch bei Steuerprüfungen. Auf diese Weise entsteht mehr Transparenz über das Verwaltungshandeln.
- Neue Beratungsfelder: Unternehmen für digitale Produkte und Dienstleistungen wie Musik, Video, Bücher oder soziale Netzwerke prägen den privaten Bereich erheblich und bilden ein etabliertes technisches Ökosystem. Ein solches gibt es nicht für den Steuerbereich, insbesondere auch nicht für die Betriebsprüfung. Zwar existieren einzelne Anbieter für bestimmte Werkzeuge zur digitalen Betriebsprüfung, allerdings fehlt ein entsprechendes digitales Ökosystem an Produkten und Dienstleistungen. Dies wäre aber wichtig, um beispielsweise mit großen Datenmengen oder neuen Ansätzen der Künstlichen Intelligenz wirtschaftlich und verantwortungsvoll umgehen zu können.
- Gesetzgebung und technische Standards: Die sich bei der Betriebsprüfung entwickelnden Standards werden die zukünftige Gesetzgebung beeinflussen und selber von der Gesetzgebung beeinflusst werden. In diesem Zusammenhang stellen sich Fragen, wie die Intention des Gesetzgebers bei der technischen Implementierung zu berücksichtigen ist, und wie bei der Ausgestaltung von

Gesetzen, welche die Betriebsprüfung beeinflussen, die Rahmenbedingungen der Digitalisierung vom Gesetzgeber zu berücksichtigen sind.

- Digitale Wertschöpfung: Inzwischen existieren vielfältige Ansatzpunkte für eine digitale Wertschöpfung, beispielsweise der Handel mit digitalen Produkten und Dienstleistungen. Typische Verfahren des Betriebsvergleichs sind aber schwierig, da beim inneren Vergleich keine proportionalen Abhängigkeiten zum Wareneinsatz ausgemacht werden können. Auch der äußere Betriebsvergleich ist in der Regel nicht sinnvoll, da insbesondere digitale Produkte und Dienstleistungen nur unzureichend vergleichbar sind oder Konkurrenzangebote gänzlich am Markt fehlen.

Vor dem Hintergrund der neuen technischen Möglichkeiten bekommen Fragen zum Selbstbild und Grundverständnis der Steuerverwaltung und zu den theoretischen Grundlagen der Besteuerung eine neue Bedeutung. So ist davon auszugehen, dass spieltheoretische Analysen von Steuer-*Compliance*-Modellen sowie verhaltensökonomische Analysen des Steuerverhaltens in Kombination mit ingenieurwissenschaftlichen Gestaltungsansätzen innovativer Anwendungen wichtige Erkenntnisse für die Zukunft der digitalen Betriebsprüfung eröffnen könnten.

---

## Literatur

- Buck, Rainer, und Marcus Klopfer. 2011. *Betriebsprüfung. Grundlagen, Ablauf, Prüfungsbericht*. Wiesbaden: Springer Gabler.
- Fettke, Peter. 2018. TaxTech – Die vierte Disziplin der Steuerwissenschaft. *Der Betrieb* [Sonderausgabe 1/2018]:19–24.
- Fettke, Peter. 2019. Künstliche Intelligenz für die Digitalisierung der Steuerfunktion. *Rethinking Tax* 1(1): 12–22.
- Harle, Georg, und Uwe Olles. 2017. *Die moderne Betriebsprüfung*, 3. Aufl. Herne: NWB Verlag.
- Houy, Constantin, Maarten Hamberg, und Peter Fettke. 2019. Robotic Process Automation in Public Administrations. In *Digitalisierung von Staat und Verwaltung*, Hrsg. Michael Räckers, Sebastian Halsbenning, Detlef Rätz, David Richter und Erich Schweighofer, 62–74. Bonn: Gesellschaft für Informatik e.V.
- Hruschka, Franz. 2018. Tax-compliant dank IT? *Der Betrieb* [Sonderausgabe 1/2018]:2–4.
- Krüger, Ralph, Bernd Schult, und Rainer Vedder. 2010. *Digitale Betriebsprüfung, GDPdU in der Praxis – Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen*. Wiesbaden: Springer Gabler.
- Maier, Moritz. 2017. Verfassungsrechtliche Aspekte der Digitalisierung des Besteuerungsverfahrens. *Juristen Zeitung (JZ)* 72(12): 614–619.
- OECD. 2017. *Technology tools to tackle tax evasion and tax fraud*. <https://www.oecd.org/tax/crime/technology-tools-to-tackle-tax-evasion-and-tax-fraud.pdf>. Zugegriffen am 04.11.2019.
- Schanz, Deborah, und Michael Sixt. 2018. Die Steuerfunktion 4.0. *Der Betrieb* 71(19): 1097–1101.
- Scholz, Tobias. 2018. Der Quantensprung für die Schätzung – Die Quantilsschätzung. Ein Bestandteil der Summarischen Risikoprüfung SRP. *WP Praxis* 9:281–288.
- Wähnert, Andreas. 2016. Zeitgemäße Datenanalyse der Betriebsprüfung – Das Datenprüfungsnetz „Summarische Risikoprüfung (SRP)“. *Der Betrieb* 69(45): 2627–2631.



# Digitale Daseinsvorsorge

Sönke E. Schulz

## Inhalt

1 Klärung des Begriffs .....	566
2 Konzeptionelle Grundlagen .....	567
3 Praktische Anwendungsfelder .....	568
4 Umsetzungsstand und Auswirkungen .....	569
5 Perspektiven für Staat, Kommunen und Verwaltung .....	572
Literatur .....	573

## Zusammenfassung

„Digitale Daseinsvorsorge“ umschreibt den Anspruch, die Bevölkerung nicht nur mit Strom, Wasser und ähnlichem zu versorgen, sondern auch mit Infrastrukturen, Gütern und Diensten, die für eine digitale Gesellschaft essenziell sind. Zusammen mit dem Ausbau der Infrastruktur (Glasfaser) handelt es sich dabei um das zentrale Politikfeld der kommenden Jahre. Welche Aufgaben Staat und Kommunen übernehmen (sollen) und wie sie diese erfüllen, hängt nämlich immer auch von den technischen Möglichkeiten ab, die sie dafür nutzen können. Im digitalen Zeitalter haben sich daher die Erwartungen, wie die öffentliche Verwaltung arbeiten und mit den Bürgerinnen und Bürgern kommunizieren und kooperieren soll, verändert. Gleiches gilt für die Erwartungen, was der Staat leisten soll, wenn der Markt bestimmte Dienste nicht zur Verfügung stellt. Dies betrifft insbesondere den Zugang zu schnellem Internet.

## Schlüsselwörter

Sozialstaat · Digitale Teilhabe · Subsidiaritätsprinzip · Gewährleistungsstaat · Smart Region

S. E. Schulz (✉)

Schleswig-Holsteinischer Landkreistag, Kiel, Deutschland

E-Mail: [sschulz@lvstein.uni-kiel.de](mailto:sschulz@lvstein.uni-kiel.de)

## 1 Klärung des Begriffs

Unter staatlicher oder kommunaler „Daseinsvorsorge“ versteht man den allgemeinen Zugang zu existenziellen Gütern und Leistungen, die einerseits gewissen Standards genügen und andererseits zu sozial verträglichen Preisen angeboten werden sollen. Die Grundversorgung der Bevölkerung mit dem, was für ein menschliches Dasein unverzichtbar erscheint, gilt als eine öffentliche Aufgabe, die allerdings je nach zeitlichem und räumlichen Kontext sehr unterschiedlich interpretiert wird. Sich darauf verlassen zu können, dass diese Aufgabe wahrgenommen wird, ist für alle Bürgerinnen und Bürger wichtig, aber besonders bedeutsam für Regionen, die schwach besiedelt oder schwer zu erschließen sind, weshalb für private Anbieter eine Versorgung dieser Gebiete nicht rentabel ist. Diese Aufgabe ist – neben der Gewährleistung der inneren und äußeren Sicherheit – eine Rechtfertigung für Staatlichkeit überhaupt. Zur kommunalen Daseinsvorsorge gehören u. a. Schulen, Sportstätten, Krankenhäuser und Friedhöfe, aber auch Müllabfuhr, Abwasserbeseitigung und das öffentliche Transportwesen (ÖPNV).

Der Begriff der Daseinsvorsorge ist ein politischer *und* rechtlicher Begriff und daher schwierig zu fassen. In der Verfassung wird zwar vereinzelt auf Güter der öffentlichen Daseinsvorsorge verwiesen (so. z. B. auf die Eisenbahnverkehrsverwaltung (Artikel 87e GG), Post und Telekommunikation (Artikel 87f GG) oder die Bundeswasserstraßen (Artikel 89 GG)), es gibt aber keine klare rechtliche Definition von Daseinsvorsorge mit einem umfassenden Katalog an entsprechenden Gütern und Dienstleistungen oder gar Rechtsansprüche, die man gegenüber dem Staat einklagen könnte. Dies gilt auch für die kommunale Ebene, wo die meisten Güter und Dienstleistungen der öffentlichen Daseinsvorsorge erbracht werden: Lediglich in einigen Gemeindeordnungen taucht der Begriff explizit auf, ohne dass sich daraus individuelle oder kollektive Ansprüche ableiten ließen. Wie weit die öffentliche Daseinsvorsorge gehen soll, gehen kann oder gehen muss, ist politisch seit jeher umstritten. Schon Lorenz von Stein, der staatliche Leistungen grundsätzlich befürwortet hat, sah durchaus, dass eine sehr weitgehende Unterstützung negative Anreize setzen und leicht auch in Bevormundung umschlagen könnte. Ein vernünftiges Leistungsniveau zwischen Überversorgung und Unterversorgung zu finden, bleibt insofern eine ständige Aufgabe.

Im digitalen Zeitalter genügt es nicht mehr, etwas zu essen, Strom, Wasser und ein Dach über dem Kopf zu haben, um ein menschenwürdiges Dasein führen zu können. Ohne einen Zugang zu möglichst schnellem Internet und einen Zugriff auf digitale Angebote ist heute nach verbreiteter Auffassung soziale Teilhabe kaum noch möglich. In diesem Sinne meint „digitale Daseinsvorsorge“ den Auftrag und die Pflicht des Staates, eine angemessene, d. h. den jeweiligen zeitlichen und örtlichen, wirtschaftlichen und technischen Gegebenheiten angepasste Grundversorgung möglich zu machen, soweit diese nicht vom Markt oder gemeinnützigen Akteuren angeboten wird (Subsidiaritätsprinzip). Der bloße Zweck allein genügt nicht, um geeignete Maßnahmen zu bestimmen, sondern es ist stets eine Orientierung an den Maßstäben der Erforderlichkeit und Verhältnismäßigkeit sowie hinsichtlich der subjektivierten Schutzpflichten des Untermaßverbots geboten (Luch und Schulz 2009).

## 2 Konzeptionelle Grundlagen

Was unter Daseinsvorsorge verstanden wird, steht nicht ein- für allemal fest, sondern muss immer wieder neu ausgehandelt werden. Was früher als unabdingbar für ein würdiges menschliches Dasein angesehen wurde, kann später als entbehrlich betrachtet werden, weil sich die Zustände verändert haben. Galten einst Post und Bahn als öffentliche Aufgaben, die nur der Staat organisieren konnte, so sind diese Unternehmen inzwischen längst privatisiert worden. Ähnliches kann man auch bei Krankenhäusern, Schwimmbädern, Mülldeponien, Orchestern oder Theatern beobachten. Die Debatte darüber, was alles zu einem würdigen Dasein gehört, ist insofern immer auch eine Debatte darüber, wo die Grenze zwischen Markt, Staat und Zivilgesellschaft verlaufen soll. Das gilt nicht nur für die öffentlich-rechtliche Grundversorgung mit Rundfunk und Fernsehen.

Die moderne Leistungsverwaltung ergänzt die traditionelle Eingriffsverwaltung, wie Ernst Forsthoff schon relativ früh herausgearbeitet hat (Forsthoff 1938, 1959, 1971). Die Erkenntnis, dass im technischen Zeitalter jeder Mensch, um ein würdiges Leben führen zu können, auf bestimmte Leistungen angewiesen ist, die er selbst nicht erbringen kann und die der Markt nicht adäquat anbietet, was sich in Grundrechten des Einzelnen oder in allgemeiner Daseinsvorsorge niederschlagen kann, ist jedoch wesentlich älter. Sie markiert den Übergang vom „Nachtwächterstaat“, der sich vorrangig um Ruhe und Ordnung kümmert, zum Wohlfahrts- bzw. Sozialstaat. Das Ringen um die Frage, ob etwas noch zur öffentlichen Daseinsvorsorge gehört oder inzwischen privat getragen werden könnte bzw. ob etwas noch nicht zur öffentlichen Daseinsvorsorge gezählt wird, was heute eigentlich längst dazu gehören müsste, ist deshalb auch das Ringen um eine zeitgemäße Ausgestaltung des Sozialstaates. „Digitale Daseinsvorsorge“ ist insofern nicht nur ein Thema des Verwaltungsrechts, sondern gehört in jede Allgemeine Staatstheorie und in jede Theorie des Wohlfahrtstaats.

Nicht nur das, was als öffentliche Aufgabe angesehen wird, kann sich wandeln, sondern ändern kann sich auch die Art und Weise, wie die Verwaltung für das Dasein vorsorgt. Während sie ihre Leistungen früher meist selbst erbracht hat, soll der Gewährleistungsstaat heute vorrangig – durch Regulierung und Überwachung privater Markakteure – dafür sorgen, dass eine bestimmte Grundversorgung zu vertretbaren Preisen allgemein verfügbar ist. Auf regulierende Eingriffe in den Markt zu setzen, statt alles selbst zu machen, geht auf die Annahme zurück, private Unternehmen würden eine ähnliche Leistung effizienter erbringen. Nur dort, wo sich für elementare Bedürfnisse kein privater Anbieter findet, bliebe der Staat noch selbst in der Pflicht.

Welche neuen Aufgaben im digitalen Zeitalter zur öffentlichen Daseinsvorsorge gehören, also vom Staat garantiert werden sollen, wenn der Markt nicht für entsprechende Angebote sorgt, ist nicht abschließend geklärt. Konsens herrscht darüber, dass sie mehr umfasst als die Versorgung mit Breitband. Digitalisierung kann die kreative Antwort auf strukturelle Probleme anderer Natur sein, z. B. auf die Frage, wie Vereinbarkeit von Familie und Beruf (im ländlichen Raum) umgesetzt werden kann, wie in dünn besiedelten Regionen Nahversorgung und Nahverkehr gesichert

werden können, welche neuartigen Lernkonzepte anstelle der überkommenen Schulstruktur treten oder inwieweit E-Health und Telemedizin ein funktionales Äquivalent für die fehlende Arztpraxis vor Ort sein können. All diese Themenfelder sind Beispiele dessen, was überkommener Weise als Daseinsvorsorge definiert wird und was in der analogen und zunehmend in der digitalen Welt' die Entscheidung der Wohnortwahl entscheidend beeinflussen kann. War die Anbindung der kreisangehörigen Gemeinden an den öffentlichen Nahverkehr und den nächsten Zentralort, z. B. die Kreisstadt, eine Messgröße für die Attraktivität eines Wohngebiets, dürfte dies heute die Versorgung mit breitbandigem Internet (zu angemessenen Bedingungen und Preisen) sein. Bei der Übertragung bestimmter Grundversorgungselemente ins Internet ist nämlich zu berücksichtigen, dass ohne eine solche breitbandige Internetverbindung vieles gar nicht realisierbar ist. Besonders deutlich wird dies am Beispiel E-Health und an modernen Mobilitätskonzepten unter Einbeziehung des autonomen Fahrens, die perspektivisch auf die 5G-Technologie angewiesen sein werden. Dass der Zugang zum Internet mittlerweile Teil der Grundversorgung der Bevölkerung ist, lässt sich kaum bestreiten; er sichert die sozio-kulturelle Teilhabe an der Gesellschaft. Das Internet wird zur Pflege zwischenmenschlicher Beziehungen eingesetzt, ebenso bildet es Teilbereiche des gesellschaftlichen, kulturellen und politischen Lebens ab, von dem derjenige, der die technischen, wirtschaftlichen, körperlichen oder intellektuellen Fähigkeiten zur Nutzung des Internets nicht besitzt, ausgeschlossen wird. Der Bedeutungszuwachs des Internets korreliert zudem mit der sich verschlechternden Ausstattung des ländlichen Raums mit herkömmlichen Infrastrukturen und sozio-kulturellen Angeboten – Online-Shop, Online-Nachrichten und Online-Kommunikation sind geeignet, den (fehlenden) Dorfladen und die gesellschaftlich-kommunikative Bedeutung der (fehlenden) Dorfkneipe oder einer guten Verkehrsanbindung an die nächste größere Stadt zumindest teilweise zu ersetzen. Die Digitalisierung der Daseinsvorsorge umfasst also die Auswirkungen der Digitalisierung auf das Zusammenleben in der örtlichen Gemeinschaft, insbesondere in den Bereichen Verkehrs- und Beförderungswesen, Gas-, Wasser- und Elektrizitätsversorgung, Müllabfuhr, Abwasserbeseitigung, Bildungs- und Kultureinrichtungen, Krankenhäuser, Friedhöfe, Schwimmbäder und Feuerwehr.

---

### **3 Praktische Anwendungsfelder**

Wenn von der „Digitalisierung aller Lebensbereiche“ die Rede ist oder davon, die digitale Revolution werde Gesellschaft, Wirtschaft und Politik radikal verändern, dann deutet das schon darauf hin, dass es für eine digitale Daseinsvorsorge eigentlich wenig Grenzen gibt, auch wenn das Handeln immer durch politische Schwerpunktsetzungen und knappe Ressourcen begrenzt ist. Digitale Technologien können intelligente Lösungen für Probleme anbieten, die sich analog nur schwer lösen lassen.

Weithin unstrittig ist, dass drei große Felder zur digitalen Daseinsvorsorge gehören: Infrastruktur (Breitband, WLAN-Hotspots usw.), Inhalte (*Live-Streaming, Social Media, Open Data etc.*) und neue Dienste (wie *Coworking-Spaces, Innovations-*

*tion-Labs u. ä.). Diskutiert wird darüber, wie diese Felder am besten bearbeitet werden, sodass möglichst schnell möglichst viele die Vorteile solcher Angebote nutzen können. Mittlerweile verfolgen nahezu alle Bundesländer und der Bund eine Glasfaser-Strategie, die auf flächendeckende Versorgung mit Gigabit-Anschlüssen setzt. Dies ist erforderlich, da viele zukünftige Dienste, insbesondere Telemedizin und autonomes Fahren auf 5G-Mobilfunknetze angewiesen sind, die ihrerseits auf stationärer Glasfaser basieren. Demgegenüber ist es für den ‚Normalnutzer‘ derzeit nur schwer vermittelbar, warum er in diese Zukunftstechnologie investieren soll, von der er nur einen Bruchteil nutzt. So werden die Netzbetreiber derzeit nur die Hälfte ihrer 30-Mbit-Kapazitäten los (Gerken und Roosebeke 2018, S. 16).*

Bund und Länder müssen zwar dafür sorgen, dass möglichst schnelles Internet möglichst überall genutzt werden kann, also eine zeitgemäße Infrastruktur gewährleisten. Aber wenn es um Inhalte und neue Dienste geht, dann sind vor allem nicht-staatliche Akteure und die Kommunen gefordert. Nicht Bund und Länder, sondern die Kommunen sind es, die täglich mit den Sorgen und Nöten und mit den Wünschen und Erwartungen der Bürgerinnen und Bürger konfrontiert werden. Sie wissen am besten, was vor Ort fehlt und am meisten vermisst wird. Die Gestaltung des unmittelbaren Lebensumfeldes, wozu auch die digitale Daseinsvorsorge gehört, ist Aufgabe der Kommunen im Sinne einer eigenständigen Regelung der örtlichen (und überörtlichen) Angelegenheiten. Netzinfrastrukturen und auch manche digitalen Angebote lassen sich zwar nur in größeren Dimensionen sachgerecht denken und realisieren, müssen aber immer an den konkreten Bedürfnissen vor Ort ansetzen.

Digitale Daseinsvorsorge erstreckt sich horizontal praktisch über alle Politikfelder und orientiert sich vertikal an den Zuständigkeiten und Kompetenzen, die Bund, Länder und Kommunen nach dem Grundgesetz jeweils haben. Als Bereiche, die überörtlich gebündelt werden müssen, nennt der Deutsche Landkreistag Gesundheit und Soziales, Bildung und Kultur, Mobilität und Verkehr, Umwelt und Energie sowie Wohnen und Arbeiten. „Der Begriff der digitalen Daseinsvorsorge umfasst hier all diejenigen – öffentlichen und privaten – digitalen Hilfestellungen, die es Bürger und Unternehmen ermöglichen, sowohl in urbanen Gebieten als auch im ländlichen Raum am gesellschaftlichen und wirtschaftlichen Leben teilzunehmen“ (Deutscher Landkreistag 2018, S. 9).

---

## 4 Umsetzungsstand und Auswirkungen

CDU, CSU und SPD wollen bis 2025 nicht nur „Gigabit-Netze“ flächendeckend ausbauen („Glasfaser in jeder Region und jeder Gemeinde, möglichst direkt bis zum Haus“), sondern bis dahin auch einen „rechtlich abgesicherten Anspruch“ auf schnelles Internet schaffen. Öffentliche Einrichtungen wie Schulen, Hochschulen, Krankenhäuser, Sozialzentren, aber auch Gewerbegebiete, sollen vorrangig angebunden werden; für den „Digitalpakt für Schulen“ will der Bund in fünf Jahren 5 Mrd. € bereitstellen, davon 3,5 Mrd. € noch in der laufenden Legislaturperiode (CDU/CSU/SPD 2018).

Da die meisten Ziele erst kürzlich beschlossen bzw. bekräftigt wurden und nur mittelfristig zu erreichen sind, können diese Beschlüsse und Programme noch nicht viel bewirkt haben. Sie sind aber ein Zeichen dafür, dass die digitale Daseinsvorsorge inzwischen auf der Agenda der Regierung steht. Auch die Berufung einer Staatsministerin für Digitalisierung verfolgt das Ziel, diese Querschnittsaufgabe in sämtlichen Ressorts voranzutreiben.

Ob alle Vorhaben fristgemäß abgeschlossen werden können, muss abgewartet werden. Zweifel sind nicht nur angebracht, dass die vorgesehenen Mittel letztlich ausreichen, sondern auch daran, ob überhaupt genügend Kapazitäten in Wirtschaft und Verwaltung frei sind, sie sinnvoll auszugeben. Für den Netzausbau will die Regierung bis 2021 etwa 10 bis 12 Mrd. € investieren, die aus der Versteigerung der 5G-Mobilfunkfrequenzen kommen sollen; Experten schätzen den Finanzbedarf jedoch auf bis zu 80 Mrd. €. Ob die Netzbetreiber den Fehlbedarf selbst aufbringen, ist wegen höchst unterschiedlicher Interessen und unsicheren Rahmenbedingungen durchaus fraglich. Wenn in den nächsten Jahren vielleicht nicht alle, aber doch die meisten Maßnahmen wie geplant umgesetzt werden könnten, wäre die digitale Daseinsvorsorge hierzulande auf ein deutlich höheres Niveau gehoben worden.

Die Länder flankieren die Planungen und Programme des Bundes mit eigenen Anstrengungen. Niedersachsen hat kürzlich einen „Masterplan Digitalisierung“ vorgelegt, für den in den nächsten Jahren über eine Milliarde Euro investiert werden sollen und mit dem das Land u. a. zu einem „nationalen Benchmark in der digitalen Nachwuchsförderung“ werden möchte (Niedersächsisches Ministerium für Wirtschaft, Arbeit, Verkehr und Digitalisierung 2018). Ähnliche Planungen, die sich nicht grundsätzlich unterscheiden, aber unterschiedliche Schwerpunkte setzen, haben praktisch alle Länder entwickelt. Die Digitalisierungsstrategie der baden-württembergischen Landesregierung deckt alle Handlungsfelder ab. Schon die Überschriften (wie „schnelles Internet in Stadt und Land“, „Bildung und Weiterbildung in Zeiten der Digitalisierung“, „intelligente Mobilität“ und „digitale Gesundheitsanwendungen“, aber auch „Die Zukunft von Kommunen und Verwaltung ist digital“) lassen erkennen, dass es nicht nur um die Stärkung des Standortes, sondern immer auch um digitale Daseinsvorsorge geht (Ministerium für Inneres, Digitalisierung und Migration 2017).

Die „Digitale Kommune“ kennt viele unterschiedliche Handlungsfelder. Die Definition der Rolle der kommunalen Gebietskörperschaft – Stadt, Amt, Gemeinde, Kreis – sollte planvoll erfolgen und z. B. eine fokussierte und priorisierte Mehrjahresplanung zugrunde legen. Im Mittelpunkt einer solchen Digitalisierungsplanung steht ein an den identifizierten Bedarfsprioritäten ausgerichtetes Konzept für die stufenweise Entwicklung und Etablierung digitaler Angebote im Bereich der Daseinsvorsorge. Das Erfordernis einer strategischen Planung für zahlreiche Sachgebiete wird in den nächsten Jahren noch zunehmen: Soweit sich gesellschaftliche Prozesse nämlich auf Basis der Informations- und Kommunikationstechnik vollziehen, gelten für sie auch die die IT prägenden Grundparadigmen, insbesondere die Raum- und Zeitunabhängigkeit. Laut Deutschem Landkreistag haben bisher lediglich sechs Prozent der 294 Landkreise, darunter auch drei Regionalverbände, eine ausgearbeitete Digitalisierungsstrategie, mit der sie die digitale Daseinsvorsorge

sicherstellen wollen. Die technische Virtualisierung bewirkt nicht nur, dass IT raum- und zeitunabhängig eingesetzt werden kann, sondern führt dazu, dass diese Möglichkeiten auf die mittels der IT verwirklichten Arbeitsvorgänge ausstrahlen. Es bedarf daher einer Vernetzung von Elementen, die in der Vergangenheit möglicherweise noch weitgehend isoliert nebeneinander stehen konnten. Ein Beispiel kann der Mobilitätssektor sein: Während früher eine Abstimmung „nur“ hinsichtlich der Spurweite, der Straßenbeschaffenheit und Ähnlichem erforderlich war, kam schon beim ÖPNV – ein Netzwerk im besten Sinne – die Abstimmung von Fahrplänen, Taktungen und Tarifen etc. hinzu. Denkt man weiter im Sinne von vollintegrierten Mobilitätslösungen ist die Verknüpfung einer Vielzahl von Akteuren, Fortbewegungsalternativen, Infrastrukturen und Dienstleistungen erforderlich.

Bei den angesprochenen Aufgaben handelt es sich vielfach um (über-)örtliche Aufgaben. Diese sind zu eigenverantwortlichen Bewältigung den Kommunen zugewiesen. Die ausschließliche Verortung planerischer Aufgaben bei Landesbehörden (wie derzeit z. B. hinsichtlich der Regionalplanung in Schleswig-Holstein) liegt weder nahe noch ist sie vor dem Hintergrund der kommunalen Selbstverwaltungsgarantie zu rechtfertigen. Strategische Planungen müssen heruntergebrochen werden. Eine Landesentwicklungsstrategie bleibt ohne regionale und lokale Entwicklungsstrategien praxisfern, die digitale Agenda des Landes bedarf einer Abbildung in regionalen und lokalen digitalen Agenden, Nachhaltigkeitskonzepte des Landes brauchen regionale und lokale Nachhaltigkeit und ein zentrales Konzept zur Bewältigung der demografischen Herausforderungen kann ohne regionale und lokale Ausfüllung (in den Bereichen Pflege, Fachkräfte sicherung, Bildung etc.) nicht gelingen. „Der weit verbreitete Irrtum, Planung und die ‚Freiheit zu politischer Entscheidung‘ als einen Gegensatz zu verstehen, ist in letzter Konsequenz die Forderung, intuitiv und ohne ausreichende Information über die Grundlagen und Auswirkungen zu entscheiden. Nach richtigem Verständnis ist Kreisentwicklungsplanung die Forderung nach qualifiziertem Verwaltungshandeln“ (Conrad 1992, S. 62).

Auch wenn die Aufgabe der digitalen Daseinsvorsorge nicht überall schon strategisch angegangen wird, heißt das nicht, dass es nicht vielfältige Aktivitäten gibt, ihr gerecht zu werden. Es bedarf digitaler Agenden jeder einzelnen Kommune und dann auch – im Sinne von Vernetzung – einer übergreifenden digitalen Agenda z. B. aller Kreise oder gar aller Kommunen eines Bundeslandes. Dies ist nicht nur erforderlich, um den Bürgern ein Angebot zu machen und zu zeigen, dass sich kommunale Selbstverwaltung weiterentwickelt und alle – auch digitale – Bedürfnisse der Bürger aufnimmt, sondern auch, um sich gegenüber Land und Bund als relevanter Akteur und Gestalter zu positionieren. Jede Region sollte sich vergewissern, wo sie – jenseits einer optimalen Breitband-, Mobilfunk- und WLAN-Versorgung – im Jahr 2030 stehen will. Exemplarisch ist der vom Amt Hüttener Berge eingeleitete Agendaprozess: Um den 14.468 Einwohnern im Amt das Leben mit digitaler Technik zu erleichtern, wurden acht Handlungsfelder identifiziert (digitale Infrastruktur, Gesundheitsvorsorge, Kultur und Freizeit, E-Government, Mobilität, Nachbarschaftshilfe, Partizipation, Tourismus und Wirtschaftsförderung), die bis Frühjahr 2018 aufgearbeitet wurden und nun umgesetzt werden (Amt Hüttener Berge 2018).

## 5 Perspektiven für Staat, Kommunen und Verwaltung

Die Europäische Kommission hat bereits 2003 ein Grünbuch zu Dienstleistungen von allgemeinem Interesse vorgelegt, das als ihre Position zur öffentlichen Daseinsvorsorge gelesen werden kann. „Als unverzichtbarer Bestandteil des europäischen Gesellschaftsmodells gehören sie zu den Werten, die allen europäischen Gesellschaften gemeinsam sind. Sie spielen bei der Erhöhung der Lebensqualität aller Bürger und der Überwindung von sozialer Ausgrenzung und Isolierung eine entscheidende Rolle. In Anbetracht ihres Stellenwertes in der Wirtschaft und ihrer Bedeutung für die Herstellung von Waren und die Erbringung sonstiger Dienstleistungen zählt die Effizienz und Qualität dieser Leistungen zu jenen Faktoren, die insbesondere im Hinblick auf die Attraktivität benachteiligter Regionen für Investoren zu größerer Wettbewerbsfähigkeit führen und den Zusammenhalt verbessern. [...] Da diese Leistungen Rechte widerspiegeln, die die Bürger Europas in Anspruch nehmen können und sie Gelegenheit für den Dialog mit den Behörden im Rahmen des verantwortungsvollen Regierens in Europa bieten, stellen die Dienstleistungen von allgemeinem Interesse darüber hinaus einen Pfeiler der europäischen Staatsbürgerschaft dar“ (Europäische Kommission 2003, S. 3). Die digitale Komponente der Daseinsvorsorge wird dabei nicht explizit herausgestellt, wird aber als einer von mehreren Faktoren seit 2013 im Rahmen des *Digital Economy and Society Index* (DESI) von der EU erfasst. Im Bericht für 2018 landete die Bundesrepublik Deutschland unter 28 EU-Mitgliedern wie schon im Vorjahr auf Platz 14, also im Mittelfeld (Europäische Kommission 2018).

Die Bundesregierung hat sich zunehmend dem Thema verschrieben. Sie arbeitet schon länger daran, eine gemeinsame Strategie aller Ressorts zu entwickeln, die über eine bloße Liste mit einzelnen Projekten hinausgehen soll. Auch die Länder sind dabei, ihre Digitalstrategien zu überdenken, wie die oben genannten Beispiele zeigen, und berücksichtigen dabei zunehmend auch die Daseinsvorsorge und gesellschaftliche Veränderungen.

Die Hauptlast der digitalen Daseinsvorsorge dürfte jedoch in den Kommunen anfallen, wo die örtlichen Angelegenheiten eigenständig geregelt werden sollen. Um die Entwicklung zu gestalten, genügt es nicht, eine „Digitale Agenda“ aufzustellen, in der Projekte der Ämter gesammelt sind, die ohnehin betrieben werden, sondern bedarf es einer klaren Strategie mit Prioritäten und Meilensteinen, die mittel- und längerfristig verfolgt wird. Wo kleinere Gemeinden mit strategischen Überlegungen überfordert sind, bedürfen sie der überörtlichen Unterstützung. Die Kommunalen Landesverbände in Schleswig-Holstein haben ihren Mitgliedern „Zwölf Goldene Regeln für den Weg zur Digitalen Kommune“ an die Hand gegeben (SHGT et al. 2018).

Wo weder Markt noch Staat hinreichend zur digitalen Daseinsvorsorge beitragen und auch die Kommune nicht alle Aufgaben gleichzeitig bewältigen kann, sollte darüber nachgedacht werden, bürgerschaftliches Engagement zu nutzen, um voran zu kommen. „Gerade bei ... Infrastrukturvorhaben könnte in einer öffentlich-rechtlichen Genossenschaftsform die Mitwirkung der ... Bürger auch bei staatlichen und kommunalen Aufgaben bzw. Vorhaben institutionell kanalisiert werden“ (Schliesky

2014, S. 157). Genossenschaften von Bürgern, die ein Breitbandnetz betreiben, würden an den Chancen einer derartigen Unternehmung und etwaigen Gewinnen partizipieren (ebd.). Ähnliche Beispiele gibt es bereits für die Bereiche Stromtrassen oder Windpark. Wie diese Beispiele zeigen, bedürfen sie in der Regel einer fachlichen Unterstützung durch das kommunale Hauptamt. Und solche Initiativen können zwar Lücken in der Infrastruktur schließen, aber natürlich keine flächendeckende Breitbandversorgung gewährleisten. Hier sind eher Kreise und Zweckverbände moderierend, fördernd, investierend und anbietend gefragt.

---

## Literatur

- Amt Hüttenberge. 2018. *Hüttis Digitale Agenda 1.0*. [https://www.amt-huettenberge.de/fileadmin/Bilder/Digitale\\_Agenda/Huetts\\_Digitale\\_Agenda\\_-\\_Fassung\\_AA.pdf](https://www.amt-huettenberge.de/fileadmin/Bilder/Digitale_Agenda/Huetts_Digitale_Agenda_-_Fassung_AA.pdf). Zugegriffen am 21.11.2019.
- CDU/CSU/SPD, Hrsg. 2018. *Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land*. Koalitionsvertrag, 19. Legislaturperiode. [https://www.cdu.de/system/tdf/media/dokumente/koalitionsvertrag\\_2018.pdf?file=1](https://www.cdu.de/system/tdf/media/dokumente/koalitionsvertrag_2018.pdf?file=1). Zugegriffen am 21.11.2019.
- Conrad, Carl-August. 1992. Die Aufgaben der Kreise. In *125 Jahre Kreise in Schleswig-Holstein*, Hrsg. Schleswig-Holsteinischer Landkreistag, 49–84. Neumünster: Wachholtz.
- Deutscher Landkreistag, Hrsg. 2018. *Der digitale Landkreis. Herausforderungen – Strategien – Gute Beispiele*. Berlin: Deutscher Landkreistag. <https://www.landkreistag.de/images/stories/publikationen/bd-136.pdf>. Zugegriffen am 21.11.2019.
- Europäische Kommission. 2003. *Grünbuch zu Dienstleistungen von allgemeinem Interesse*. Brüssel: Europäische Kommission (KOM[2003] 270 endgültig).
- Europäische Kommission, Hrsg. 2018. *Index für die digitale Wirtschaft und Gesellschaft (DESI) 2018. Länderbericht Deutschland*. Brüssel: Europäische Kommission. [www.ec.europa.eu](http://www.ec.europa.eu).
- Forsthoff, Ernst. 1938. *Die Verwaltung als Leistungsträger*. Stuttgart: Kohlhammer.
- Forsthoff, Ernst. 1959. *Rechtsfragen der leistenden Verwaltung*. Stuttgart: Kohlhammer.
- Forsthoff, Ernst. 1971. *Der Staat der Industriegesellschaft*. München: C.H. Beck.
- Gerken, Lüder, und Bert Van Roosebeke. 2018. Glasfaser, der große Plan und sein Preis. *Frankfurter Allgemeine Zeitung*, 24. August 2018, 16.
- Luch, Anika D., und Sönke E. Schulz. 2009. E-Daseinsvorsorge. Staatliche Schutzpflichten und Sozialstaatsprinzip im Lichte der Virtualisierung des Lebens. In *Herausforderung E-Government. E-Volution des Rechts- und Verwaltungssystems*, Hrsg. Hermann Hill und Utz Schliesky, 305–335. Baden-Baden: Nomos.
- Ministerium für Inneres, Digitalisierung, und Migration, Hrsg. 2017. *Digitalisierungsstrategie der Landesregierung Baden-Württemberg*. Stuttgart: Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg.
- Niedersächsisches Ministerium für Wirtschaft, Arbeit, Verkehr, und Digitalisierung, Hrsg. 2018. *Die Strategie Niedersachsens zur digitalen Transformation. Masterplan Digitalisierung*. Hannover: Niedersächsisches Ministerium für Wirtschaft, Arbeit, Verkehr und Digitalisierung.
- Schliesky, Utz. 2014. Das Modell der öffentlich-rechtlichen Genossenschaften als Träger öffentlicher Daseinsvorsorge und Infrastruktur. In *Der Dritte Sektor als Infrastrukturrektruktur. Jahrbuch Recht und Ökonomik des Dritten Sektors 2013/2014 (RÖDS)*, Hrsg. Hans-Jörg Schmidt-Trenz und Rolf Stober, 149–160. Baden-Baden: Nomos.
- SHGT (Schleswig-Holsteinischer Gemeindetag), et al. Hrsg. 2018. *12 Goldene Regeln für den Weg zur Digitalen Kommune*. <https://www.dataport.de/Download/DigitaleKommune-12GoldeneRegeln.pdf>. Zugegriffen am 21.11.2019.



---

# Koordination und Integration im E-Government

Thurid Hustedt und Philipp Trein

## Inhalt

1 Alte und neue Koordinationsprobleme .....	576
2 Koordination und Integration als analytische Begriffe .....	576
3 Strukturelle Grundlagen für Koordination und Integration im <i>E-Government</i> .....	578
4 Umsetzungsstand und Auswirkungen .....	580
5 Perspektiven für Staat und Verwaltung .....	582
Literatur .....	583

---

## Zusammenfassung

Der föderale Staatsaufbau und die konsensorientierten Institutionen des deutschen Regierungssystems schaffen einen hohen Koordinationsbedarf und erschweren die Integration neuer Technologien und Politiken in bestehende Strukturen. Dies zeigt sich auch beim *E-Government*, also der Digitalisierung der Verwaltung. Besonders die föderale Organisation von Verwaltungszuständigkeiten verkompliziert die Koordination beim *E-Government*, während beispielsweise im Gesundheitsbereich die konsensorientierten Institutionen die Einführung technischer Innovationen verlangsamen. Gewisse Fortschritte Deutschlands sind im internationalen Vergleich gleichwohl zu erkennen.

---

## Schlüsselwörter

Federalism · Multilevel Governance · Coordination · E-government · Germany · Policy integration

---

T. Hustedt  
Hertie School, Berlin, Deutschland  
E-Mail: [hustedt@hertie-school.org](mailto:hustedt@hertie-school.org)

P. Trein (✉)  
University of Lausanne, Lausanne, Schweiz  
E-Mail: [josefphilipp.trein@unil.ch](mailto:josefphilipp.trein@unil.ch)

## 1 Alte und neue Koordinationsprobleme

*Koordinationsprobleme* zwischen Verwaltungseinheiten, Regierungsebenen und politischen Akteuren im Allgemeinen sind ein bekanntes Phänomen politischer Prozesse. Sowohl aufgrund des bundesdeutschen *Föderalismus* als auch der ausgeprägten Ressortautonomie und der Einbindung gesellschaftlicher Akteure in vielen Politikfeldern bedarf erfolgreiches politisches Handeln immer der *Koordination* einer Vielzahl von Akteuren, was im Umkehrschluss mit besonderen Herausforderungen einhergeht. Prominente Beispiele sind Koordinationsprobleme zwischen der Bundesregierung und Landesregierungen, aber auch zwischen verschiedenen Ministerien auf Bundes- oder Landesebene. Die Einbindung der Länder in die Bundespolitik, aber auch die Delegation von Kompetenzen an Spitzenverbände wie etwa im Gesundheitswesen, erhöhen den Koordinationsbedarf zusätzlich.

*E-Government* bezeichnet die Verwendung von Informations- und Kommunikationstechnologien (IuK) in öffentlichen Verwaltungen, beispielsweise in Meldeämtern oder als elektronisches Patientendossier. Die Digitalisierung öffentlicher Dienstleistungen stellt erhebliche Anforderungen an die Koordinationsfähigkeit von Politik und Verwaltung in Bund, Ländern und Kommunen, weil digitale Leistungen auf allen Ebenen nahtlos zugänglich gemacht werden können und sollen. Die mit der Digitalisierung einhergehenden Möglichkeiten, Datenaustausch zu automatisieren und große Datenbestände zu speichern, ermöglichen technisch die ebenen- und behördenübergreifende Bereitstellung und damit letzliche Vereinfachung von Verwaltungsleistungen. Dazu aber müssen sich die zuständigen Ministerien und Behörden koordinieren und darüber verständigen, welche Leistungen wie digital bereitgestellt werden sollen. Die technische Integration der Aufgaben funktionaler Teilbereiche, wie etwa Krankenkassen, Krankenhäusern und Arztpraxen im Bereich der Gesundheitspolitik, aber auch die Integration der Aufgaben von Behörden in Bund, Ländern und Gemeinden ist besonders anspruchsvoll. Zum Beispiel muss das Integrationspotenzial von *E-Government* mit dem Verbot von Mischverwaltungen in Einklang gebracht werden und die verschiedenen Interessengruppen müssen zusammenarbeiten, wenn die digitale Transformation gelingen soll. In Anbetracht dieser strukturellen Gegebenheiten schaffen Einführung und Reform des *E-Government* einen besonderen Koordinationsbedarf, insbesondere in einem föderal und dezentral organisierten Regierungssystem wie dem bundesdeutschen. *E-Government* hat das Potenzial, die bestehenden Koordinationsmechanismen innerhalb von und zwischen Politikbereichen, aber auch unter Bund, Ländern und Gemeinden zu verändern.

---

## 2 Koordination und Integration als analytische Begriffe

Die Begriffe Koordination und Integration werden in unterschiedlichen Kontexten verwendet und sind wichtige Konzepte in der Politik- und der Verwaltungswissenschaft.

*Koordination* ist ein zentrales Element politischer Prozesse. Der Gesetzgebungs- und Implementationsprozess in demokratischen Staaten erfordert eine konti-

nuierliche Abstimmung zwischen verschiedenen Akteuren wie der Regierung, politischen Parteien, Interessengruppen, Gebietskörperschaften, parastaatlichen Akteuren und privaten Organisationen. In der *Governance*-Forschung unterscheidet man generelle Formen sozialer Handlungskoordination wie Netzwerke, Wettbewerb und Hierarchie und es wird argumentiert, dass in Netzwerken geführte Verhandlungen ein zunehmend wichtiger Koordinationsmechanismus in der Interaktion privater und staatlicher Akteure sind, während eine strikt hierarchische Koordination, selbst in der Verwaltung, an Bedeutung verliert (Benz 2009). Die Vetospielertheorie, mit der unter anderem in der Vergleichenden Politikwissenschaft gearbeitet wird, besagt, dass die Anzahl und der ideologische Abstand zwischen kollektiven Akteuren mit Vetomacht das Ergebnis des politischen Prozesses beeinflussen. Je mehr Vetospieler vorhanden sind, desto mehr Akteure müssen sich koordinieren, um Ergebnisse zu erzielen (Tsebelis 2002; Sager 2006). Dieser Ansatz lässt sich nutzen, um abschätzen zu können, unter welchen Bedingungen Koordination gelingt oder nicht gelingt, etwa im Falle von Katastrophen oder Krisensituationen.

Ein anderer konzeptioneller Zugriff unterscheidet zwischen negativer und positiver Koordination (Scharpf 1973). Negative Koordination beschreibt den üblichen Standard horizontaler Regierungskoordination: Das zuständige – federführende – Ministerium erarbeitet einen Entwurf, beispielsweise für eine Gesetzesvorlage, und versendet diesen an alle in ihrer Zuständigkeit ebenfalls betroffenen Ressorts. Diese prüfen den Entwurf unter dem Blickwinkel negativer Folgen für ihren eigenen Zuständigkeitsbereich und melden diese an den Federführer zurück, der den Entwurf entsprechend ändert. Die Ministerien passen sich in der Festlegung ihrer Positionen also nur soweit an andere Häuser an, als dies den Status quo oder ihre eigenen Interessen nicht tangiert. Positive Koordination ist hingegen deutlich seltener zu beobachten: Hier werden die Vorschläge aller beteiligten Ressorts zu einem gemeinsamen und verzahnten Entwurf verarbeitet.

Mit dem Begriff der Politikverflechtungsfalle wird darüber hinaus ein ebenfalls für die Schwierigkeiten der Koordination im deutschen Regierungssystem zentrales Charakteristikum bezeichnet. Dieser Begriff verweist auf institutionell angelegte Politikblockaden, die in einem föderalen Regierungssystem mit zentralisiertem Parteiensystem entstehen, in dem die Landesregierungen im Bundesrat zustimmungspflichtige Gesetze unterstützen müssen. Daraus erwachsen Innovationsstau und Reformhemmnisse (Scharpf 1985). Im Grundgesetz ist nicht nur geregelt, welche Gesetze einer Zustimmung der Länder bedürfen, sondern eine „Mischverwaltung“ von Bund und Ländern ist grundsätzlich ausgeschlossen, weshalb Ausnahmen einer speziellen Regelung bedürfen.

*Integration* ist ein Begriff, der in mehreren Literatursträngen prominent vertreten ist. Hier ist insbesondere seine Verwendung in der Politikfeldanalyse sowie der verwaltungswissenschaftlichen Literatur relevant. In der Politikfeldanalyse bezeichnet Integration die „Eingemeindung“ neuer Probleme in Gesetze und Verwaltungseinheiten. Das prominenteste Beispiel dafür ist die Umwelt- und Klimapolitik, die in der internationalen Diskussion unter den Begriffen *Environmental Policy Integration* und *Climate Policy Integration* verhandelt wird (Adelle und Russel 2013). Klima- und Umweltfragen können einzeln in bestehende Gesetze integriert werden,

ohne diese wirklich zu verbinden, oder in einem Rahmengesetz gebündelt werden, welches systematisch Konsequenzen für viele andere Politikbereiche hat. Im Unterschied zur Koordination zwischen Behörden, beispielsweise bei der Umsetzung von Gesetzen oder der Krisenbewältigung, bezeichnet die Integration von Verwaltungseinheiten deren organisatorische Verschmelzung. Solche Reformen sind jedoch aufgrund der rechtlichen und organisatorischen Autonomie empirisch seltener und haben oft symbolischen Charakter (Trein 2017).

---

### **3 Strukturelle Grundlagen für Koordination und Integration im E-Government**

In der Literatur zum *E-Government* wird argumentiert, dass eine effiziente Verwendung von digitalen Technologien in der öffentlichen Verwaltung die Integration unterschiedlicher Politiksektoren, aber auch der verschiedenen Gebietskörperschaften erfordert. Hier gilt *E-Government* dann als effizient, wenn digitalisierte Verwaltungsdaten mit individuellen Informationen zu Bürgerinnen und Bürgern automatisch zwischen verschiedenen Verwaltungen und Gebietskörperschaften ausgetauscht werden können (Dunleavy et al. 2006; Baqir und Iyer 2010, S. 19–20). So tauschen zum Beispiel manche Steuerverwaltungen und städtische Sozialämter in der Schweiz ihre Daten automatisch aus, um Ansprüche auf staatliche Zusüsse zu den Krankenkassenbeiträgen zu ermitteln. Integrierte und digital bereitgestellte Verwaltungsdienstleistungen sind für viele Bürger einfacher und besser zugänglich, sie sind nicht an behördliche Öffnungszeiten gebunden, ermöglichen den nahtlosen Zugriff verschiedener Behörden auf einmal gespeicherte Dokumente und reduzieren den Aufwand in der Beantragung. Digitalisierung schont auch die Ressourcen der Verwaltung. In Zeiten des Fachkräftemangels (auch) in der Verwaltung ist dieses Einsparpotenzial relevant. Zugleich können digital erbrachte Leistungen Inkongruenzen zwischen politischen Programmen, aber auch in der Implementation aufzeigen.

Allerdings sind der umfassenden Integration von *E-Government* Grenzen gesetzt: Erstens verhindern die horizontale Spezialisierung von Zuständigkeiten in verschiedene Ministerien und Behörden sowie die vertikale Arbeitsteilung die Integration elektronischer Verwaltungsleistungen. Zum Beispiel ist die Autonomie von Ländern und Gemeinden in Deutschland vor allem eine Verwaltungsautonomie, während Gesetzgebungs- und Besteuerungskompetenzen zum großen Teil entweder der übergeordneten Gebietskörperschaft obliegen oder gemeinsam mit dieser ausgeübt werden. Die Verteilung von Zuständigkeiten zwischen Ressorts sowie zwischen Bund, Ländern und Gemeinden bremst also die Integration, verweist allerdings gleichermaßen auf den Koordinationsbedarf der Digitalisierung von Verwaltungsleistungen. Auf Bundesebene ist das Innenministerium für die Verwaltungsdigitalisierung zuständig und mit Amtsantritt der derzeitigen Bundesregierung wurde die Rolle des Bundeskanzleramtes deutlich gestärkt. Darüber hinaus unterhalten alle Ressorts eigene Organisationseinheiten, die für IT und/oder Digitalisierung zuständig sind.

Zweitens erschwert der generell hohe Koordinationsbedarf des bundesdeutschen Regierungssystems die Einführung von *E-Government*-Lösungen. Insbesondere die

föderale Ordnung mit ihren Vetopunkten verhindert die zentralistische Einführung digitaler Verwaltungsdienstleistungen. Vielmehr müssen die *differentia specifika* des bundesdeutschen Exekutivföderalismus, die Kompetenzverteilung zwischen Bund und Ländern sowie die wichtige Rolle der Kommunen bei der Erbringung von Verwaltungsleistungen in den Blick genommen werden, um diese auch digital zugänglich zu machen. Mit Art. 91c GG wurde 2009 die verfassungsrechtliche Grundlage für den IT-Planungsrat geschaffen, der heute das zentrale Bund-Länder-Koordinationsgremium zur Verwaltungsdigitalisierung ist (Schardt 2017). Art. 91c sieht explizit vor, dass Bund und Länder bei der „Planung, der Errichtung und dem Betrieb der für ihre Aufgabenerfüllung benötigten informationstechnischen Systeme zusammenwirken“ können (Art. 91c 1 GG) und gemeinsame Standards festlegen dürfen. Die Gesetzgebungskompetenz zur Regelung des Zugangs zu digitalen Verwaltungsdienstleistungen wurde mit dieser Grundgesetzänderung dem Bund (mit Zustimmung des Bundesrates) übertragen. Der 2010 per Staatsvertrag eingesetzte IT-Planungsrat löste die vorherigen Koordinationsgremien – „Arbeitskreis der Staatssekretäre für E-Government in Bund und Ländern (St-Runde Deutschland-Online)“ und „Kooperationsausschuss von Bund und Ländern für automatisierte Datenverarbeitung (KoopA ADV)“ – ab. Mitglieder im IT-Planungsrat sind der/die Beauftragte der Bundesregierung für Informationstechnik sowie jeweils ein für Informationstechnik zuständiger Vertreter aus jedem Bundesland – in der Regel sind Bund und Länder auf Ebene der Staatssekretäre vertreten. Darüber hinaus können die kommunalen Spitzenverbände beratende Mitglieder entsenden sowie der/die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit beratend teilnehmen (IT-Planungsrat 2019). Als regelmäßig tagendes Gremium mit Vertretern aus Bund und Ländern, welches Steuerungs- und Koordinierungsaufgaben wahrnimmt (siehe unten), hat der IT-Planungsrat eine dezentrale Organisationsstruktur, in der es vorrangig um die föderale Abstimmung geht. Diese dezentrale Organisationsform wird gelegentlich kritisiert. Stattdessen wird die Einrichtung einer zentralen Stelle zur Koordination der bundesdeutschen Verwaltungsdigitalisierung – zum Beispiel im Bundeskanzleramt (Schardt 2017) oder sogar ein eigenständiges Digitalisierungsministerium – gefordert, welches die verschiedenen Dimensionen der Digitalisierungspolitik integriert.

Drittens begrenzen die Anforderungen des Datenschutzes den Austausch und die Speicherung von Daten und damit die Integration digitaler Verwaltungsleistungen. In Deutschland ist der Datenschutz im Rahmen der EU-Datenschutzgrundverordnung geregelt, welche striktere Bestimmungen hat als beispielsweise der Datenschutz in den USA. Während eine optimistische Vision von *E-Government* eine technische und politische Integration und Koordination von existierenden Verwaltungseinheiten mit mehr Effizienz gleichsetzt, verweisen Datenschützerinnen und Datenschützer darauf, dass eine umfassende und zentrale Speicherung von Verwaltungsdaten aus unterschiedlichen Politiksektoren wie Steuer-, Sozial-, und Gesundheitspolitik – theoretisch – einem Überwachungsstaat Tür und Tor öffnen würde – wie etwa im chinesischen Sozialkreditsystem realisiert. In dieser Sichtweise reduziert also der bewusste Verzicht auf Integration die Gefahr des Datenmissbrauches. Wenngleich der Nutzen integrierter *E-Government*-Lösungen bisher wenig erforscht ist, zeigen Länderbeispiele wie etwa

Österreich oder Dänemark, dass auch unter den strengen Auflagen des europäischen Datenschutzes Verwaltungsleistungen digital erbracht (und genutzt) werden können.

---

## 4 Umsetzungsstand und Auswirkungen

Dass Deutschland beim *E-Government* noch Nachholbedarf hat, ist unstrittig. „E-Government in Deutschland gibt es praktisch nicht“, lautete 2015 das provokante Urteil des Nationalen Normenkontrollrates (Weber 2018, S. 150). In internationalen Vergleichen liegt Deutschland beim *E-Government* meist im hinteren Mittelfeld. Im vielbeachteten *Digital Economy and Society Index* (DESI) der Europäischen Kommission etwa, der unter dem Begriff „digitale Verwaltung“ die Nutzung von Online-Verwaltungsdienstleistungen, den Einsatz von Online-Formularen, die Nutzung frei verfügbarer Daten in der Verwaltung sowie die vollständige digitale Abwicklung administrativer Prozesse misst, landet Deutschland 2018 nur auf dem 21. Platz der EU-Mitgliedstaaten (Europäische Kommission 2018, S. 3). Die Vereinten Nationen sehen Deutschland beim *E-Government* immerhin auf Platz 12 im weltweiten Vergleich (nach Platz 22 im Jahre 2008) (Vereinte Nationen 2018). Es sind also durchaus Fortschritte zu verzeichnen, die Platzierungen deuten aber auch auf Potenziale hin, die noch nicht ausgeschöpft wurden. Als Vorreiter der Verwaltungsdigitalisierung in der EU gelten Estland und Dänemark; aber auch Großbritannien und das föderale Österreich schneiden regelmäßig gut ab.

In Deutschland variieren sowohl die Quantität als auch die Qualität elektronischer Dienstleistungen teilweise erheblich zwischen den Ländern und zwischen den Kommunen; eine vollständige Digitalisierung des Leistungsangebots gibt es praktisch nirgendwo. Zwar können häufig bereits elektronische Formulare genutzt werden, aber die Bürgerinnen und Bürger müssen in den meisten Fällen noch die zuständige Behörde aufsuchen, um den Verwaltungsvorgang abzuschließen. Die Vielfalt der existierenden technischen Lösungen (Weber 2018) führt zu Kompatibilitätsproblemen zwischen den unterschiedlichen Systemen, beispielsweise weil verschiedene persönliche Anlaufstellen (*Frontoffices*) in der Verwaltung heterogene Informations- und Kommunikationssysteme haben. Die Koordination zwischen verschiedenen Regierungsebenen („Government-to-Government“), also „die digitale und analoge Kooperation der Verwaltungen untereinander“ (Stember und Hesse 2018a, S. 80), ist vor allem aus der Perspektive der Nutzerinnen und Nutzer noch stark verbessерungsbedürftig. Aus Sicht des Nationalen Normenkontrollrates sind Koordinationsprobleme, sowohl zwischen den Ressorts als auch föderaler Natur, für den Rückstand der Verwaltungsdigitalisierung ursächlich (Nationaler Normenkontrollrat 2018, S. 36).

Diese Situation soll sich insbesondere mit der Umsetzung des 2017 beschlossenen Onlinezugangsgesetzes (OZG) ändern. Bereits in den Jahren zuvor haben sowohl der Bund (2013) als auch die Länder mit ihren E-Government-Gesetzen die rechtlichen Voraussetzungen für digitale Kommunikation mit und in der Verwaltung geschaffen. Allerdings zeigt eine 2018 durchgeführte Evaluation des E-Government-Gesetzes des Bundes, dass dieses zwar das Bewusstsein für Verwaltungsdigitalisierung in den

Behörden stärkte und Ausstrahlungseffekte auf die Ländergesetzgebung hatte, vier Jahre nach Inkrafttreten aber noch erhebliche Umsetzungsdefizite bestehen. Neben fehlendem Budget, Datenschutzregelungen, mangelnder Nutzerakzeptanz und mangelnder Digitalisierungskompetenz in der Verwaltung wird auch das Fehlen standarisierter IT-Lösungen für die Umsetzungsdefizite verantwortlich gemacht (Deutscher Bundestag 2019a). Das Evaluierungsgutachten empfiehlt verstärkte föderale und verwaltungsübergreifende Koordinationsmechanismen. Darunter etwa eine *E-Government-Agentur*, deren Etablierung derzeit vorbereitet wird (Deutscher Bundestag 2019b). Das 2016 abgeschlossene Projekt „E-Government-Modellkommunen“, vom Bundesinnenministerium gemeinsam mit den kommunalen Spitzenverbänden aufgelegt, sollte dem interkommunalen Erfahrungsaustausch dienen und den Transfer innovativer Lösungen ermöglichen (Stember und Hesse 2018b). Die in acht Modellkommunen erprobten *E-Government*-Lösungen in Einzelprojekten richten sich entweder an den Bürger oder die Bürgerin, wie etwa Online-Anträge für BAföG (Bundesausbildungsförderungsgesetz), oder betreffen inneradministrative Verfahren, beispielsweise die Einführung der elektronischen Akte in der Stadt Norderstedt oder die Einführung einer elektronischen Rechnung in Halle. Auch in diesem Projekt zeigten sich typische Probleme der Koordination: So rangierten interne Kooperations- und Kommunikationsprobleme sowie Probleme in der behördenübergreifenden Koordination unter den wichtigsten Ursachen für Umsetzungsprobleme in den Modellkommunen (Stember und Klähn 2016, S. 43). Der Projektbericht betont, dass zur Überwindung dieser Probleme sowohl integrative Strategien zur Umsetzung digitaler Reformen, sorgfältiges Change- und Projektmanagement sowie die frühzeitige und dauerhafte Abstimmung zwischen allen beteiligten Verwaltungen wichtige Erfolgsfaktoren sind (Stember und Klähn 2016, S. 50).

Als zentrales föderales Koordinierungsgremium verfolgt der IT-Planungsrat eine Reihe von Steuerungsprojekten, wie etwa die Weiterentwicklung des Deutschen Verwaltungsdienstverzeichnisses, sowie Koordinationsprojekte, wie die Digitalisierung des Asylverfahrens (Beck 2018). Eine herausgehobene Stellung kommt dem IT-Planungsrat bei der Steuerung der Umsetzung des OZG zu: Durch das OZG sollen bis 2022 alle Verwaltungsdienstleistungen flächendeckend online angeboten werden. Herzstück der Umsetzung ist der sogenannte Portalverbund, über den die Verwaltungsleistungen von Bund, Ländern und Gemeinden gemeinsam zugänglich gemacht werden sollen. In dem Portalverbund werden die Leistungen nach dem Lebenslagen- und Geschäftslagenprinzip abgebildet und sind über einmal einzurichtende individuelle Benutzerkonten zugänglich. Um die 575 vorgesehenen Verwaltungsleistungen zu digitalisieren, bedarf es erheblicher föderaler Koordination, die in einer für die bundesdeutsche Politik ungewöhnlichen Art organisiert ist. Nach dem „Einer-für-Alle-Prinzip“ (Vitt 2019, S. 159) übernimmt je ein Bundesministerium gemeinsam mit mindestens einem Bundesland die Federführung für die Digitalisierung der diesem Themenfeld zugeordneten Leistungen und stellt sie dann allen zur Verfügung. Die Entwicklung dieser digitalen Leistungen erfolgt zum Teil in Digitalisierungslaboren, in denen die Verwaltungen gemeinsam mit Expertinnen und Experten, Designerinnen und Designern sowie Nutzerinnen und Nutzern Ideen entwickeln, Prototypen umsetzen, testen und fortentwickeln.

Alle Verwaltungsleistungen zeitgleich systematisch zu digitalisieren gilt im internationalen Vergleich als „einzigartige Vorgehensweise, die so systematisch in keinem anderen Land umgesetzt wird“ (Mergel 2019, S. 163). Insgesamt zeigt sich, dass Deutschland nach wie vor erheblichen Nachholbedarf in der Verwaltungsdigitalisierung hat, obgleich in jüngerer Zeit insbesondere mit der begonnenen OZG-Umsetzung Fortschritte zu verzeichnen sind. Der Nationale Normenkontrollrat kritisiert, dass sich nicht alle Bundesländer gleichsam an der OZG-Umsetzung beteiligen und mahnt an, dass die OZG-Umsetzung als prioritäre politische Aufgabe zu sehen sei, in die auch die Regierungschefs von Bund und Ländern einzubinden seien, um Koordinationsprobleme zu bewältigen (Nationaler Normenkontrollrat 2018, S. 39). Neben der bereits erwähnten *E-Government*-Agentur befindet sich mit der FITKO (Föderale IT-Kooperation) derzeit eine weitere Organisation in der Gründung, die als Anstalt des öffentlichen Rechts von 2020 an in gemeinsamer Trägerschaft von Bund und Ländern den IT-Planungsrat in der OZG-Umsetzung unterstützen und insbesondere die föderale Koordination sichern soll.

Neben den Herausforderungen der föderalen Koordination, gilt es auch sektorale Koordinationsprobleme der Digitalisierung zu bewältigen wie etwa das folgende Beispiel aus der Gesundheitspolitik zeigt: Durch die Einführung einer elektronischen Patientenakte, deren Entwicklung allerdings an nicht-staatliche Akteure delegiert wurde, sollen die verschiedenen Teilbereiche des Gesundheitssystems wie Krankenversicherer, Ärzte und Krankenhäuser koordiniert werden, indem die Daten des Patienten zentral in einer Datei gespeichert werden. Neben Verwaltungsdaten können dabei idealerweise auch die Patientendaten in Form einer elektronischen Patientenakte gespeichert werden. Das alles soll die Behandlung vereinfachen und eine bessere Koordination zwischen den verschiedenen Teilbereichen des Gesundheitssystems schaffen (gematik 2018). Aufgrund von Koordinationsproblemen zwischen verschiedenen Verbänden, beispielsweise Ärzten und Krankenkassen, und wegen Bedenken zur Datensicherheit verteuerte sich das System und seine Einführung wurde bis 2019 verzögert. Das Beispiel der elektronischen Gesundheitskarte zeigt wie der generell hohe Koordinationsbedarf in Deutschland Neuerungen im Bereich des *E-Government* bremsen kann. Die Koordinationsprobleme zwischen Spitzerverbänden als Ursache für Reformblockaden und Innovationsstau sind nichts Besonderes im deutschen Gesundheitswesen (Klenk 2008; Trein 2018). Von daher ist es nicht überraschend, dass diese Faktoren bei der Einführung des elektronischen Patientendossiers ebenfalls eine Rolle spielen.

---

## 5 Perspektiven für Staat und Verwaltung

*E-Government* und Verwaltungsdigitalisierung lassen die in den institutionellen Strukturen des bundesdeutschen Regierungssystems angelegten Koordinationsprobleme wie unter dem Brennglas hervortreten. Da Digitalisierung eine genuine Querschnittsaufgabe ist, die alle Ressorts und alle staatlichen Ebenen betrifft, entsteht mit der föderalen sowie der ressortübergreifenden Abstimmung ein ausgeprägter Koordinations- und teilweise Integrationsbedarf. Daher spielen Integrations- und Koordinationsfragen im

*E-Government* auf der aktuellen politischen Agenda eine zentrale Rolle. Mit dem IT-Planungsrat, der geplanten *E-Government-Agentur*, der sich in der Gründung befindenden FITKO, der Neuordnung der Zuständigkeiten mit der Stärkung des Bundeskanzleramts in der Digitalisierungspolitik sowie der neuartigen arbeitsteiligen „Einer-für-alle“-Umsetzung des OZG wird deutlich, dass gerade in jüngerer Zeit die Koordinationsprobleme, die als ursächlich für die mangelnde Verwaltungsdigitalisierung in Deutschland gesehen werden, in Angriff genommen werden. Es wird nicht unwesentlich von der Koordinationsleistung dieser neuen Strukturen abhängen, ob die OZG-Zielsetzung erreicht wird und Deutschland in der Verwaltungsdigitalisierung aufholt. Der Ausbau von *E-Government* wird den Koordinationsbedarf zwischen den Regierungsebenen, aber auch den verschiedenen Ressorts erhöhen und muss gleichzeitig mit den Anforderungen des Datenschutzes und den Präferenzen von Interessengruppen in Einklang gebracht werden.

Insgesamt hat die Digitalisierung der Verwaltung das Potenzial, Strukturen, Prozesse und auch die Kultur der deutschen Verwaltung zu verändern. Allerdings wird diese Transformation nicht allein durch die Bereitstellung digitaler Leistungen für Bürgerinnen und Bürger und Unternehmen erreicht werden, sondern vor allem auch durch die konsequente Digitalisierung interner Prozesse sowie die Einführung und Stärkung digitaler Elemente im *Policy-Making*. Algorithmische Steuerung oder die Nutzung künstlicher Intelligenz etwa in der Formulierung wie der Implementation von *Policies* können (und werden) das Handeln von Politik und Verwaltung in den kommenden Jahren ebenso verändern wie die an sie gerichteten Erwartungen und lassen kontroverse Diskussionen über Legitimität, *Accountability*, Transparenz und Datensicherheit erwarten. Ob die etablierten und neuen Steuerungsinstrumente der deutschen Politik dem gewachsen sind, bleibt abzuwarten.

---

## Literatur

- Adelle, Camilla, und Duncan Russel. 2013. Climate policy integration. A case of *déjà vu?* *Environmental Policy and Governance* 23(1): 1–12.
- Baqir, Muhammad Naveed, und Lakshmi Iyer. 2010. E-government maturity over 10 years. A comparative analysis of e-government maturity in select countries around the world. In *Comparative e-government*, Hrsg. Christopher G. Reddick, 3–22. New York: Springer.
- Beck, Wolfgang. 2018. Wirkungsorientierte Verwaltungssteuerung durch E-Government-Gesetze in Deutschland. In *Wirkungen von E-Government. Impulse für eine wirkungsgesteuerte und technikinduzierte Verwaltungsreform*, Hrsg. Jürgen Stember, Wolfgang Eixelsberger und Andreas Spichiger, 181–206. Wiesbaden: Springer Fachmedien.
- Benz, Arthur. 2009. *Politik in Mehrebenensystemen*. Wiesbaden: VS Verlag für Sozialwissenschaften.
- Deutscher Bundestag. 2019a. *Unterrichtung durch die Bundesregierung. Bericht der Bundesregierung zur Evaluierung des Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften*. BT-Drucksache 19/10310. <https://dip21.bundestag.de/dip21/btd/19/103/1910310.pdf>. Zugegriffen am 17.12.2019.
- Deutscher Bundestag. 2019b. *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Uwe Schulz, Joana Cotar, Dr. Michael Espendiller und der Fraktion der AfD – Drucksache 19/9375. E-Government-Agentur*. BT-Drucksache 19/9837. <https://dip21.bundestag.de/dip21/btd/19/098/1909837.pdf>. Zugegriffen am 17.12.2019.

- Dunleavy, Patrick, Helen Margetts, Simon Bastow, und Jane Tinkler. 2006. New public management is dead. Long live digital-era governance. *Journal of Public Administration Research and Theory* 16(3): 467–494.
- Europäische Kommission. 2018. *Digital public services. Digital economy and society index report 2018 (DESI)*. Brüssel: Europäische Kommission.
- gematik. 2018. *gematik. Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH 2018*. <https://www.gematik.de>. Zugegriffen am 17.12.2019.
- IT-Planungsrat. 2019. *IT-Planungsrat. Digitale Zukunft gestalten*. [www.it-planungsrat.de](http://www.it-planungsrat.de). Zugegriffen am 17.12.2019.
- Klenk, Tanja. 2008. *Modernisierung der funktionalen Selbstverwaltung. Universitäten, Krankenkassen und andere öffentliche Körperschaften*. Bonn: Friedrich Ebert Stiftung.
- Mergel, Ines. 2019. Digitale Transformation als Reformvorhaben der deutschen öffentlichen Verwaltung. In *dms – der moderne staat. Zeitschrift für Public Policy, Recht und Management* 12(1): 162–171.
- Nationaler Normenkontrollrat (NKR). 2018. *Deutschland. Weniger Bürokratie, mehr Digitalisierung, bessere Gesetze Einfach machen!* Berlin: Nationaler Normenkontrollrat.
- Nationen, Vereinte. 2018. *United nations e-government survey 2018. Gearing e-government to support transformation towards sustainable and resilient societies*. New York: Department of Economic and Social Affairs, United Nations.
- Sager, Fritz. 2006. Policy coordination in the European metropolis. A meta-analysis. *West European Politics* 29(3): 433–460.
- Schardt, Marc. 2017. Der IT-Planungsrat. Zentrum der Digitalisierung der öffentlichen Verwaltung? *VM Verwaltung & Management* 23(5): 227–235.
- Scharpf, Fritz W. 1973. *Planung als politischer Prozess. Aufsätze zur Theorie der planenden Demokratie*. Frankfurt a. M.: Suhrkamp.
- Scharpf, Fritz W. 1985. Die Politikverflechtungsfalle. Deutscher Föderalismus und Europäische Gemeinschaft im Vergleich. *Politische Vierteljahresschrift* 26(4): 323–356.
- Stember, Jürgen, und Emanuel Hesse. 2018a. Handlungsempfehlungen aus Deutscher Sicht. In *Wirkungen von E-Government. Impulse für eine wirkungsgesteuerte und technikinduzierte Verwaltungsreform*, Hrsg. Jürgen Stember, Wolfgang Eixelsberger und Andreas Spichiger, 79–83. Wiesbaden: Springer Fachmedien.
- Stember, Jürgen, und Emanuel Hesse. 2018b. Das Projekt E-Government-Modellkommunen des Bundesministeriums des Innern in Deutschland. In *Wirkungen von E-Government. Impulse für eine wirkungsgesteuerte und technikinduzierte Verwaltungsreform*, Hrsg. Jürgen Stember, Wolfgang Eixelsberger und Andreas Spichiger, 345–382. Wiesbaden: Springer Fachmedien.
- Stember, Jürgen, und Christin Klähn. 2016. *Projektbericht. E-Government-Modellkommunen*. Berlin: Bundesministerium des Innern.
- Trein, Philipp. 2017. Coevolution of policy sectors. A comparative analysis of healthcare and public health. *Public Administration* 95(3): 744–758.
- Trein, Philipp. 2018. *Healthy or sick? Coevolution of health care and public health in a comparative perspective*. Cambridge: Cambridge University Press.
- Tsebelis, George. 2002. *Veto players. How political institutions work*. Princeton: Princeton University Press.
- Vitt, Klaus. 2019. Die Digitalisierung der Verwaltung braucht effiziente föderale Kooperation. In *dms – der moderne staat. Zeitschrift für Public Policy, Recht und Management* 12(1): 157–161.
- Weber, Mike. 2018. Stand des eGovernment in Deutschland. In *Wirkungen von E-Government. Impulse für eine wirkungsgesteuerte und technikinduzierte Verwaltungsreform*, Hrsg. Jürgen Stember, Wolfgang Eixelsberger und Andreas Spichiger, 159–180. Wiesbaden: Springer Fachmedien.

---

## **Teil VII**

### **Personal, Organisation, Prozesse**



---

# Digitaler Organisationswandel

Moritz Heuberger

## Inhalt

1 Einleitung .....	588
2 Theoretische Grundlagen .....	589
3 Praktische Anwendung .....	592
4 Fazit .....	597
Literatur .....	597

---

## Zusammenfassung

In diesem Artikel werden die Voraussetzungen für eine erfolgreiche Digitalisierung der öffentlichen Verwaltung diskutiert. Dabei liegt der Fokus auf den internen Verwaltungsprozessen sowie auf der Kommunikation und Koordination innerhalb und zwischen Behörden. Zur richtigen Anlage eines digitalen Organisationswandels sind vor allem das Personalmanagement, die Organisationsform des Veränderungsprozesses sowie der Technologieeinsatz von zentraler Bedeutung.

---

## Schlüsselwörter

Technologischer Wandel · Organisationswandel · Change Management · Digitale Transformation · Public Management · Digitalisierungsprozesse

---

M. Heuberger (✉)

Lehrstuhl für Politikwissenschaft, Verwaltung und Organisation, Universität Potsdam, Potsdam, Deutschland

E-Mail: [moritz.heuberger@uni-potsdam.de](mailto:moritz.heuberger@uni-potsdam.de)

## 1 Einleitung

Die Digitalisierung von öffentlichen Dienstleistungen bedarf der Digitalisierung des Datenmanagements und Datenaustauschs sowie von Abläufen und Prozessen im Verwaltungsaltag (*E-Administration*). Um digitale Angebote im „*front office*“ zu schaffen, ist also die Digitalisierung des „*back office*“ nötig. Um einen Blick auf Erfolgsfaktoren dieser internen Verwaltungsdigitalisierung zu erhalten und den digitalen Wandel in der Verwaltung mit Management-Konzepten zu begleiten, ist der Fokus auf die *Kommunikation und Koordination* im Bereich *Government to Government* (G2G) nötig, welche inter-organisatorische (zwischen Behörden, horizontal und vertikal) als auch intra-organisatorische Abläufe (innerhalb von Behörden) abdecken.

Weil es bei der Digitalisierung um die praktische Umsetzung von grundlegenden technologischen Innovationen im Bereich der Informationstechnologie geht, handelt es sich dabei nicht nur um die Übertragung vormals analoger Prozesse in digitale (elektronische Akte statt Hängeordner, *E-Mail*- statt Brief-Verkehr), sondern um eine Steigerung der Vernetzung, die Ermöglichung von Kommunikation in Echtzeit und die damit verbundene Überwindung von räumlichen Grenzen, die nahezu unendliche Skalierbarkeit von Abläufen sowie den Einbezug von IT-Innovationen wie zum Beispiel Künstlicher Intelligenz (KI). Bei der Digitalisierung der Verwaltung geht es demnach um technologischen Wandel in einer Organisation und damit um *kein isoliertes informationstechnisches Phänomen*, sondern um ein Phänomen, welches aus einer Reihe von sozialen Praktiken und individuellen Faktoren der Mitarbeitenden, dem Wandel der (Verwaltungs-)Kultur und aus verfügbaren technischen Anwendungen und deren Charakteristika zusammengesetzt ist.

Der Umgang von Organisationen mit dynamischen Situationen und Prozessen im Umbruch wird als Organisationswandel bezeichnet, die aktive Gestaltung dieses Wandels wiederum als *Change Management*. Im Rahmen der Digitalisierung ziehen digitale Technologien auch in die Büros der öffentlichen Verwaltung ein. E-Mails statt Briefe, Word statt Schreibmaschine oder die elektronische Akte an Stelle eines Ordners im Regal sind das eine. Die Veränderung von Hierarchien, Abläufen, Zuständigkeiten und Arbeitsweisen, die sich auf die Papierförmigkeit der Verwaltung stützen, sind das andere. Dabei geht es nicht nur um Fragen der Entgrenzung, Vervielfältigung und Zugänglichkeit, die sich mit der Einführung von digitalen Arbeitsweisen stellen. Zentral für das Verständnis von Organisationswandel durch Digitalisierung sind auch die *vorherrschenden Normen, Verhaltensmuster und Kulturen*, sowohl auf der Mikroebene – also auf Ebene des (individuellen) Akteurs – als auch auf der Makroebene, d. h. auf der Ebene der Regeln, Abläufe, des Selbstverständnisses und der Traditionen einzelner Behörden. Die *öffentliche Verwaltung* ist eben nicht nur als ein zweckorientiertes Werkzeug, sondern auch als eine soziale Struktur mit einem nicht-zweckbezogenen Eigenleben zu verstehen (Seibel 2016, S. 31) und auch als solche zu untersuchen.

Aufbauend auf der Digitalisierung einzelner Prozesse können auch umfangreiche Abläufe und Prozessketten (*Workflow*) effektiver und effizienter gestaltet werden –

also weniger Zeit und Personal für den gleichen Output benötigt werden und durch diese Produktivitätssteigerung weniger Kosten anfallen. Außerdem kann die Digitalisierung von Abläufen durch Standardisierung und durch Eliminieren menschlicher Fehlerquellen zur Qualitätssteigerung führen. Diese tief gehende Integration von digitalen Elementen in Arbeitsabläufe – oder besser: die vollständige Integration der Arbeitsabläufe in digitale Systeme – bedarf eines Wandels einiger tief verwurzelten Ideale und Prinzipien der Verwaltung sowie einer Umgestaltung von Aufbau- und Ablauforganisation.

---

## 2 Theoretische Grundlagen

### 2.1 Bedingungen für den Organisationswandel

Um Wandel in einer Organisation aktiv zu gestalten, kann auf wissenschaftliche Modelle zurückgegriffen werden, die Schritte für die Gestaltung von Organisationswandel in der Verwaltung beschreiben. Einen Überblick über Bedingungen, die für einen Wandlungsprozess gegeben sein sollten, liefern Fernandez und Rainey (2006), deren Modell sich auf acht Punkte reduzieren lässt, welche in ihrer Arbeit jeweils ausführlich besprochen und mit empirischen Studien belegt werden:

1. Neben der Bereitschaft für den Wandel, muss die *Dringlichkeit* für den Wandel bestehen. Ohne ein Verständnis für die Notwendigkeit des Wandels fehlt verwaltungsintern jegliche Motivation für aufwendige Wandlungsprozesse.
2. Ein *Plan* für den Prozess des Wandels muss bereitgestellt werden. Das heißt: offene und klare Kommunikation über die Ziele des Wandels, die notwendigen Schritte und die zur Verfügung stehenden Mittel.
3. Verwaltungsintern muss zu Beginn jedes Wandlungsprozesses *interne Unterstützung* für den Wandel hergestellt werden, um Widerstand zu reduzieren bzw. auftretendem Widerstand auf verschiedenen Ebenen entgegenzuwirken. Diese Unterstützung kann vor allem durch Partizipation und Kooptation der Beteiligten („alle mit ins Boot holen“) erreicht werden.
4. Die *Unterstützung auf Führungsebene* und das entsprechende *Commitment* muss gesichert werden. Bei mangelnder Führung, Vorbildfunktion und Glaubwürdigkeit, lässt sich die Verwaltung nicht für Organisationswandel gewinnen.
5. Auch *externe Unterstützung* muss gesichert werden. Damit sind zum einen relevante Stakeholder (Nutzer\*innen von elektronischen Dienstleistungen, Behörden mit direktem Kontakt, private Partner), zum anderen aber die relevanten politischen Akteure gemeint. Ohne politische Unterstützung oder zumindest Akzeptanz sind Wandlungsprozesse nur schwer durchzusetzen.
6. Die nötigen *Ressourcen* für den Wandel müssen bereitgestellt werden. Ohne die Instrumente (*Software*, *Hardware*, elektronische *Tools*), bei fehlendem Personal beziehungsweise fehlenden Personalstunden für den Wandel wird an bestehenden Routinen festgehalten.

7. Der Wandel muss *institutionalisiert* werden und darf nicht als singuläres Projekt begriffen werden. Dazu muss er in den Arbeitsalltag integriert werden, indem neue Gewohnheiten und Routinen alte ersetzen.
8. Wandel muss *integrativ über Ebenen* hinweg gestaltet werden. Dazu muss ein verständlicher Ansatz gefunden werden, der existierende Beziehungen und Verknüpfungen in einer komplexen Organisation im Blick behält und die Identifikation der Mitarbeitenden mit den Zielen des Wandels sicherstellt.

## 2.2 Unterschiedliche Formen von Organisationswandel

Grundsätzlich werden in der Debatte um Organisationswandel zwei Arten des Wandels unterschieden. Auf der einen Seite wird von *geplantem (organisiertem) Wandel* gesprochen, wenn es sich um beabsichtigten, aktiv vorangetriebenen und gesteuerten Wandel handelt, auf der anderen Seite steht der *ungeplante (emergente) Wandel*, welcher ohne zentrale Planung abläuft. Darüber hinaus wird die Intensität des Wandels kategorisiert: *Wandel erster Ordnung (gradual change*, evolutionärer/adaptiver Wandel, lockerer Wandel) bezeichnet die kleinteilige, inkrementelle Modifikation von Aufbau und Ablauf in Organisationen. Dabei verändert sich jedoch weder der vorherrschende Bezugsrahmen noch das dominante Interpretations-schema. *Wandel zweiter Ordnung (radical change*, revolutionärer/transformativer Wandel, strenger Wandel) liegt hingegen dann vor, wenn sich jener Bezugsrahmen ändert und sich Paradigmen im Wandel befinden, was eine grundsätzliche Veränderung der Organisation hervorruft (Kuijpers et al. 2014, S. 2–3).

## 2.3 Besonderheiten der öffentlichen Verwaltung

In der Literatur finden sich verschiedene Faktoren, die eine Hemmung des Organisationswandels in der öffentlichen Verwaltung im Zusammenhang mit der Digitalisierung erklären. Ein Aspekt ist die fachliche und organisatorische Heterogenität in der Verwaltung, welche die Planbarkeit von IT-Projekten einschränkt (Lemke 2013, S. 128). Gleichzeitig bergen große IT-Projekte auch politisches Risiko und die Gefahr der öffentlichen Skandalisierung. Beides führt dazu, dass Rechtfertigungsarbeit auf der einen Seite und Distanz zwischen Projektleitung und politischer Führung auf der anderen Seite den Fortschritt von Projekten bremsen (ebd.). Darüber hinaus ist der Organisationstyp im öffentlichen Sektor zumeist monopolistisch, es droht keine Konkurrenz – lediglich Unmut der Bürger\*innen. Dies nimmt den Wettbewerbsdruck und senkt die Veränderungsbereitschaft. Auch ein Vergleich der jeweiligen Arbeit ist nur beschränkt möglich, da die gleiche Tätigkeit am gleichen Ort und unter vergleichbaren Bedingungen nicht von anderen Organisationen gemacht wird und auch ein kritischer Vergleich mit anderen Organisationen im Alltag nicht notwendig oder möglich ist.

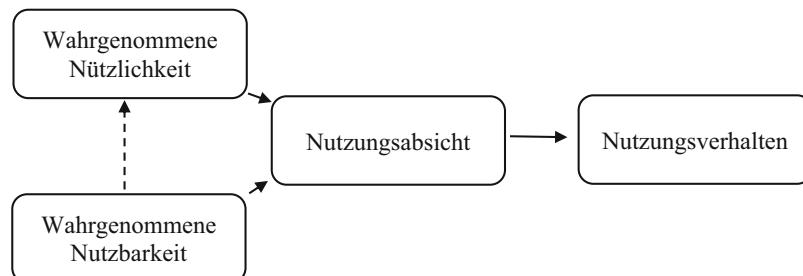
Die Unterschiede im Change Management des öffentlichen Sektors im Vergleich zu privatwirtschaftlichen Organisationen lassen sich empirisch vor allem auf drei

Aspekte reduzieren: Prozesse in der Verwaltung laufen *bürokratischer* und *formalisierte* ab (vor allem aus Risikoaversion und wegen notwendiger Kontrollmechanismen), *Führungskräfte* sind *weniger materialistisch* eingestellt (die Reaktionen auf finanzielle Anreize fallen geringer aus) und aufgrund von unflexiblen Personalstrukturen, die meist nicht projekt-, sondern dauerhaft funktionsspezifisch differenziert sind, ist eine *geringere Hingabe* an die Arbeitsaufgabe zu verzeichnen (Boyne 2002, S. 118).

## 2.4 Besonderheiten des technologischen Wandels

Um organisatorischen und technologischen Wandel gezielt gestalten zu können, müssen die zentralen Faktoren, die den Wandel beeinflussen, beschrieben und analysiert werden. So beschäftigt sich die Forschung – in der Betriebswirtschaftslehre, der Wirtschaftsinformatik und in den Sozialwissenschaften – mit diversen Modellen, in welchen Faktoren definiert werden, die für den Erfolg und Misserfolg von digitalem Wandel in Organisationen verantwortlich sind. So existiert zum Beispiel das *Technology Acceptance Model* (TAM), das 1989 definiert und 2000 weiterentwickelt wurde (Venkatesh und Davis 2000), auf das oft Bezug genommen wird. Hier geht es um die Akzeptanz von technologischer Innovation. Das Nutzungsverhalten wird im Modell beschrieben als Folge der Nutzungsabsicht, welche wiederum Folge aus der wahrgenommenen Nutzerfreundlichkeit (*perceived ease of use*) und der wahrgenommenen Nützlichkeit (*perceived usefulness*) ist. Dabei hat die wahrgenommene Nutzbarkeit (wie leicht sich etwas anwenden lässt, wie schwer der Umstieg fällt etc.) gleichzeitig auch einen Einfluss auf die wahrgenommene Nutzerfreundlichkeit (In welchem Ausmaß beschleunigt die Innovation Prozesse oder vereinfacht den Arbeitsalltag?). Diese beiden Faktoren werden wiederum im erweiterten Modell durch diverse Einflussfaktoren erklärt, wie zum Beispiel durch die Faktoren Erfahrung, *Output-Qualität* oder Vorhandensein subjektiver Normen (Venkatesh und Davis 2000, S. 188) (Abb. 1).

Zwei weitere theoretische Modelle, entlehnt aus der Betriebswirtschaftslehre, sind für das Verständnis von technologischer Innovation in der Verwaltung hilfreich:



**Abb. 1** Das Technology Acceptance Model; eigene Übersetzung und Darstellung, nach Venkatesh und Davis (2000, S. 188)

So eignet sich das Framework der Managementtechnik *Public Management Information Systems* (PMIS) sehr gut, um die speziellen Begebenheiten im öffentlichen Sektor zu berücksichtigen. Dazu werden drei relevante Kontexte von Organisationswandel bestimmt (Bozeman und Bretschneider 1986, S. 477):

- Individual-Kontext (Charakteristika, Einstellungen und Motivation der individuellen Akteure)
- Organisations-Kontext (Größe, Struktur, Zeitrahmen etc.)
- Umfeld-Kontext (externe Einflüsse wie zum Beispiel Erwartungen der Bürger\*innen).

Das *Technology-Organization-Environment-Framework* (TOEF) nach Baker (2012) legt den Fokus weniger auf den öffentlichen Sektor, sondern konzentriert sich mehr auf die technologische Innovation. Hierbei werden folgende drei Faktorenbündel bzw. Kontexte unterschieden:

- Technologie-Kontext (bestehende und genutzte Technologie; neu hinzukommende/nicht genutzte Technologie)
- Organisations-Kontext (Strukturen, Kommunikations-Prozesse, Größe, etc.)
- Umfeld-Kontext (Branche, beziehungsweise den Sektor und die darin vorherrschende Kultur)

---

### 3 Praktische Anwendung

Angesichts von theoretischen Grundlagen, die gezielter auf die öffentliche Verwaltung ausgerichtet sind, empfiehlt sich eine Melange aus den beiden aufgeführten Modellen als Leitlinie der Darstellung. Der Umfeld-Kontext ist zwar auch von großer Bedeutung, vor allem, wenn die Zufriedenheit und Akzeptanz von *E-Services* betrachtet wird. Bei einem Blick auf die Digitalisierung von verwaltungsinternen Abläufen (*E-Administration*) kann dieser Kontext jedoch zunächst vernachlässigt werden. Im Folgenden werden daher drei Faktoren – individueller, Technologiebezogener und organisationaler Kontext – eingehender beschrieben.

#### 3.1 Personal

Das Selbstverständnis und die berufliche Sozialisation spielen eine große Rolle für das Verständnis der Veränderungsbereitschaft von Beschäftigten in der öffentlichen Verwaltung. Verwaltungshandeln kann nicht als abstraktes Handeln einer Institution betrachtet werden, sondern ist zugleich auch Ergebnis individuellen Handelns der beteiligten Akteure. Daher ist der Blick auf handlungsleitende Faktoren auf Seiten der Akteure ein wichtiges Feld, um Wandel zu erklären und zu gestalten. Die Bereitschaft und die individuelle Bemühung um den erfolgreichen Organisationswandel hängt mit der individuellen Motivation zusammen. Da empirische Belege für einen starken Einfluss der wahrgenommenen Selbstbestimmung über die eigene Arbeit

(*autonomy*) auf die intrinsische Motivation vorliegen (Jensen und Bro 2018, S. 543) und sich die Digitalisierung der Arbeit durch erhöhte Vernetzung, Kommunikation und Zusammenarbeit auszeichnet, ist die Aufrechterhaltung der Motivation und das Setzen von Anreizen im digitalen Wandlungsprozess von besonderer Bedeutung. Dabei ist es vor allem die *intrinsische Motivation*, die hier näher betrachtet werden soll: Diese ist dann vorzufinden, wenn Mittel (Handlung) und Zweck (Handlungsziel) thematisch übereinstimmen, wenn also aus innerem Anreiz heraus das Organisationsziel verfolgt wird. Intrinsische Motivation lässt sich weder hervorrufen noch steuern. Jedoch zeigt die vorliegende Forschung im Bereich der Arbeitspsychologie, dass das Auftreten von intrinsischer Motivation mit großen Handlungs- und Gestaltungsspielräumen der Mitarbeiter\*innen zusammenhängt (Hackman und Oldham 1976). Besonders relevant ist die intrinsische Motivation beim Erlernen neuer Tätigkeiten. Hier zeigt sich ebenfalls ein positiver Zusammenhang zwischen einer auf Selbstbestimmung beruhenden Lernmotivation und der Qualität des Lernens (Deci und Ryan 1993). Die Gefahr besteht jedoch, durch Managementhandeln intrinsische Motivation gerade zu verhindern. Der sogenannte „Verdrängungseffekt“ tritt dann auf, wenn externe Anreize an Stelle der intrinsischen Motivation treten: Monetäre Anreize, Aufstiegsversprechen oder ähnliche zur Motivation gedachte Mittel – indes zur extrinsischen Motivation – verdrängen die ursprünglich greifende intrinsische Motivation. Fällt dann die extrinsische Motivation weg oder wird schwächer, kehrt die intrinsische Motivation nicht wieder zurück (Osterloh und Frey 1997).

Neue Verfahren und Verfahrensabläufe werden oftmals zurückgewiesen, wenn diese von dem abweichen, woran Mitglieder einer Organisation gewöhnt sind. In diesem Fall wird auch von *Beharrungsvermögen* gesprochen – einem Phänomen, das in der Verwaltung häufig beobachtet werden kann (Heckmann 2013, S. 6). Dies führt dazu, dass an gewohnten und etablierten Organisationsweisen festgehalten wird. Wandel bedeutet Veränderung und Veränderung wiederum führt zu einem *Verlust an Stabilität und Sicherheit*. Daher löst Wandel immer auch in stärkerer oder schwächerer Form Widerstand aus – in der Literatur als *resistance to change* bekannt (Wirtz et al. 2016). Dabei kann zwischen fehlender Anpassungsbereitschaft (Nicht-Wollen) und fehlendem Anpassungsvermögen (Nicht-Können) unterschieden werden (Vahs 2015, S. 326). Dabei ist vor allem der Dialog mit den Beschäftigten und die Kommunikation der Vorteile des Wandels sowie das Schlagen einer Brücke zwischen bestehenden Werten und neuen Entwicklungen in einer Organisation wichtig (Roux 2015, S. 239–240). Auch das Ausräumen von Ängsten und Bedenken gegenüber wahrgenommenen Risiken der neuen Technologie muss dabei thematisiert und glaubhaft ausgeräumt werden, da hierin eine der hauptsächlichen Barrieren bei Verwaltungsmitarbeitenden besteht. Eine Studie, die den Widerstand in der Verwaltung gegenüber *Open Government Data* – also dem Paradigma der (digitalen) Bereitstellung von öffentlichen Daten – untersucht hat, ergab, dass dieser Aspekt an erster Stelle steht, gefolgt von der wahrgenommenen Transparenz in der Organisation, wahrgenommenen Hierarchie-Barrieren, wahrgenommenen rechtlichen Schranken sowie der wahrgenommenen bürokratischen Entscheidungskultur (Wirtz et al. 2016, S. 1352).

Interne Widerstände lassen sich an verschiedenen Punkten festmachen, die bei der Implementation von Wandel zu berücksichtigen sind (Vahs 2015, S. 332–333):

- Zum einen kann es zu Zielkonflikten zwischen den Organisations- und Individualzielen kommen. Das Gefühl persönlicher Herabwürdigung kann die Folge von Prestigeverlust, Verlust an Handlungs- und Entscheidungskompetenzen oder Einkommenseinbußen sein.
- Außerdem können mangelndes Problemverständnis und Problembewusstsein zu Anpassungsschwierigkeiten führen, weil der Wandel nicht akzeptiert wird.
- Wenn die Kommunikation bezüglich des Wandels (Ziele, Vorgehen, Ansprechpersonen) nicht funktioniert, führt dies zu einem schlechten Informationsstand bei den vom Wandel betroffenen Individuen. Dies kann zu mangelndem Vertrauen in den Wandel führen.
- Passives Verhalten kann oftmals durch mangelnde Möglichkeiten aktiver Beteiligung an Veränderung und an der Gestaltung von Wandel erklärt werden.
- Schließlich kann Wandel zu Mehrarbeit führen – oder Mitarbeiter\*innen gehen davon aus, dass der Wandel eine erhöhte Arbeitsbelastung mit sich bringen wird.

Diese Aspekte werden empirisch gestützt und zeigen, dass der Widerstand der Mitarbeiter\*innen ein zentraler Punkt ist, der Wandel verhindert (Vonk et al. 2007), vor allem, weil Unsicherheit, die mit Wandel einhergeht, ein *erhöhtes Stresslevel* verursacht (Ashford 1988). Hier muss von der Führungsebene aktiv gegengesteuert werden, Vertrauen geschaffen und Möglichkeiten zur Beteiligung und Mitwirkung bereitgestellt werden. Der (kurzfristige) Mehraufwand während des Wandels muss berücksichtigt und Stress reduziert werden.

### **3.2 Technologie**

Die *fachliche und organisatorische Heterogenität* der öffentlichen Verwaltung stellt den Wandlungsprozess vor besondere Herausforderungen: Dies führt dazu, dass Innovation im Bereich der Informationstechnik (IT) in verschiedenen Behörden separat mit eigener IT-Abteilung und eigener IT-Infrastruktur eingeführt und umgesetzt wird – zum Teil wird die identische Herausforderung in verschiedenen Fachbehörden der gleichen Verwaltungseinheit eigenständig angegangen und Lösungen werden parallel entwickelt. Die *Verbreitung und Bekanntmachung von Innovation* ist in der Organisation von großer Bedeutung, weil die bloße Verfügbarkeit einer Technologie (z. B. die Einführung eines neuen Dokumenten-Management-Systems) noch nicht bedeutet, dass die Innovation und ihre Vorteile tatsächlich bekannt und damit auch praktisch und nicht nur theoretisch nutzbar sind. Daher ist die Bereitstellung von Instrumenten (*Software*, *Hardware*, Netzwerke), Ressourcen (Zeit, Geld, Zugang zu Daten), aber auch Information (was steht zur Verfügung, wie kann es genutzt werden?) elementar. Auch das Wissen um und die Verfügbarkeit von entsprechenden Ansprechpartnern bei Fragen rund um neue Technologien ist hier zu beachten. Letztere müssen die Rolle von *Change Agents* einnehmen, also den

Wandel transportieren. Dazu genügt nicht eine IT-Abteilung, die zur Fehlerbehebung und für technische Fragen zur Verfügung steht, sondern Personal, das den Wandel aktiv bewirkt und neue Arbeitsweisen „vorlebt“ (Kickert 2014, S. 704).

Erst durch die Bereitstellung von digitaler Technologie in einer nutzbaren Form kann sie einen Einfluss auf die Arbeit nehmen. Durch den vermehrten Einsatz von digitaler Technologie erhöht sich die Zahl geteilter Daten und gemeinsamer Prozesse. Außerdem ist wichtig, dass Innovationen kombiniert werden und in Kombination miteinander eine Verbreitung erfahren. Das ist gerade wegen der erhöhten Vernetzung von Bedeutung, da verschiedene Systeme miteinander kompatibel sein müssen. Das bedeutet auch, dass digitale Produkte von Haus aus „unvollständig“ sein sollten, weil Veränderung durch Weiterentwicklung unvorhersehbar und damit die *notwendige Anpassungsfähigkeit* des Produkts unabdingbar ist (Yoo et al. 2012, S. 1403). Technologische Innovation muss in ihrer Ausgestaltung daher immer eine gewisse Flexibilität mitbringen, um Wandel zu ermöglichen. Dazu ist eine Abkehr von in sich geschlossenen Implementationsprozessen nötig, hin zu zirkulären Prozessen von ständiger (Re-)Evaluation und Nachjustierung – weg von Technologie-Lösungen, die bei ihrer Einführung schon wieder veraltet sind, hin zu Lösungen, die sich das Smartphone als Vorbild nehmen: Es stellt nur eine Plattform, eine grundlegende Infrastruktur zur Verfügung. Die konkreten Funktionen werden erst später über Apps hinzugefügt, wobei manche Apps zum Anschaffungszeitpunkt des Geräts noch nicht einmal erfunden sind (Yoo et al. 2012, S. 1399).

Die *Interoperabilität* – also die Arbeit und Kommunikation über verschiedene Schnittstellen und Softwarelösungen hinweg – ist ein zentraler Aspekt, der von technischer Seite her zu beachten ist. Hierzu sind nicht nur gemeinsame Standards, sondern auch Vorgaben für die formale Datenstruktur notwendig (Lips et al. 2011). Außerdem fallen die *Datensicherheit* und damit auch der *Datenschutz* unter die technischen Bedingungen für den Wandel. Dazu gehört die Sicherheit bei der Datenspeicherung (vor allem, wenn diese *online* in der *Cloud* erfolgt), bei der Datenübermittlung und bei der Verwendung (Verwaltung von Zugangsrechten). Diese Aspekte werden vor allem dann wichtig, wenn einer dieser Schritte an Dritte – unter Umständen sogar private – Anbieter ausgelagert wird. In diesem Fall sind klar kommunizierte Vorgaben, aber auch die strikte Kontrolle von Regeln nötig.

Ein weiteres Problem sind Redundanzen und die Heterogenität im IT-Einkauf und beim Betrieb von IT-Infrastruktur: Einzelne Behörden haben eine eigene IT-Abteilung, die sich um die Beschaffung kümmert, einzelne Behörden betreiben einzelne *Server* und während die Bundesländer in der Regel eigene Landesrechenzentren betreiben, ist dies bei Kommunen die Ausnahme (z. B. okom21 als gemeinsames Rechenzentrum aller hessischen Kommunen oder das ITDZ Berlin). Statt dessen schließen sich Kommunen oftmals zu Zweckverbänden zusammen oder engagieren private IT-Dienstleister. All dies führt zu hohen Lizenzgebühren, hohen Anschaffungs- und Wartungskosten und zu einem sehr hohen Aufwand bei Anpassungen, die in allen kommunalen Rechenzentren einzeln durchgeführt werden müssen.

Die Heterogenität der genutzten Software und der IT-Zuständigkeiten erschwert das *Change Management*. Daher sind die *Festlegung von gemeinsamen Standards*

und die *Konsolidierung der öffentlichen IT* zwei zentrale Punkte, um den digitalen Wandel zu vereinfachen und damit zu beschleunigen. Um Standards setzen und die IT-Konsolidierung vorantreiben zu können, sind angeglichene und standardisierte Verwaltungsabläufe (intern) und Verwaltungsleistungen (extern) notwendig (Heckmann 2013).

### 3.3 Organisation

Gleichzeitig bestehen *verfassungsrechtliche Beschränkungen* in der Zusammenarbeit (Gewaltenteilung) sowie Prinzipien wie das auf Ebene der Ministerien herrschende Ressortprinzip, das die Unabhängigkeit der Steuerung der einzelnen Ressorts voneinander sichert und oft auch eine politisch gewollte Hürde für die Zusammenarbeit zwischen verschiedenen Häusern (bei verschiedener Parteizugehörigkeit der Minister\*innen) darstellt. Hinzu kommen organisatorische Hindernisse wie Föderalismus, kommunale Selbstverwaltung und das Subsidiaritätsprinzip, die allesamt die Koordination erschweren, da sie die Zahl der beteiligten Akteure und potenziellen Veto-Spielern erhöhen (Berger 2018). All dies steht einer Einführung von einheitlichen Systemen im Weg und damit auch dem Prinzip der Vernetzung, das ganz grundlegend ist für die Digitalisierung. Ein Schritt in Richtung mehr Zusammenarbeit – oder zumindest der Erlaubnis von Zusammenarbeit – wurde 2009 gegangen, als das Verbot von Mischverwaltung gelockert wurde. In Art. 91c GG wird seither dem Bund und den Ländern erlaubt, bei Planung, Errichtung und Betrieb informationstechnischer Systeme miteinander kooperieren zu dürfen. Dabei darf der Einfluss einer über 60 Jahren gewachsenen Kultur der Trennverwaltung nicht außer Acht gelassen werden (Lemke 2013, S. 127). Die Digitalisierung der öffentlichen Verwaltung vollzieht sich, insofern sie geplant vonstattengeht, in großen Digitalisierungsprojekten, welche oftmals *zeitliche und organisatorische Inflexibilität* mit sich bringen. So wird bei der E-Akte von 30 Jahren Planungshorizont gesprochen – von Planung über Einführung bis hin zur Nutzung (Lemke 2013, S. 132).

Die Netzwerkstruktur der IT steht hierarchischen Organisationsformen diametral gegenüber. Ein Ebenen-übergreifender Austausch von Individuen, thematisch und an Projekten orientiert, wird durch IT enorm vereinfacht und in Echtzeit ermöglicht. Das Problem ist die Aufgabenerfüllung in digitalen Projekten auf der einen Seite (netzwerkartig organisiert) und Befehls- und Machtstrukturen auf der anderen (hierarchisch). Dies führt dazu, dass die notwendige Information von oder Mitzeichnung durch andere Ebenen oder fehlende Eigenständigkeit auf unteren Hierarchieebenen zu einer massiven Behinderung von netzwerkartigem Arbeiten führt. Hier müssen Lösungen zur Flexibilisierung von Organisationsstrukturen in der Verwaltung gefunden werden, da sonst lediglich die Anstrengung der Einführung digitaler Technologie unternommen wird, ohne von den positiven Effekten profitieren zu können. Die als „*Red Tape*“ in der Wissenschaft bekannte exzessive Bürokratie, die überflüssige Verwaltungsvorschriften und Verfahren bezeichnet, kann durch Netzwerke (wie zum Beispiel einem *Intranet* oder durch andere Infrastruktur zum

Datenaustausch) überwunden werden, indem Verantwortlichkeiten besser sichtbar und Arbeitsprozesse übersichtlicher gestaltet werden können. *Red Tape* selbst kann den Wandel zwar behindern – wenn Mitarbeiter\*innen aus Eigeninteresse daran festhalten –, Welch und Pandey (2007) zeigen jedoch, dass durch den Wandel hin zu mehr digitaler Technologie *Red Tape* vor allem abgebaut wird. Prozesse werden übersichtlicher und effektiver. Unnötige Strukturen und Abhängigkeiten werden überwunden – wenn auch oftmals nicht formell, jedoch praktisch im Vollzug der alltäglichen Aufgaben.

---

## 4 Fazit

Zusammenfassend lässt sich sagen, dass zuerst die Voraussetzungen für Organisationswandel geschaffen werden müssen, bevor Wandlungsprozesse erfolgreich angestoßen und durchgeführt werden können. Technische und rechtliche Rahmenbedingungen müssen angepasst, bestehende Strukturen und Prozesse hinterfragt und Mitarbeitende aus vorherrschenden Denkmustern herausgelöst werden.

Erst wenn die grundlegenden Bedingungen für die Digitalisierung des *Back Offices* der Verwaltung erfüllt sind, können die nächsten Schritte gegangen werden, wie zum Beispiel die Automatisierung von Verwaltungsprozessen. Erst wenn zusammenhängende Prozesse in der Verwaltung vollständig digitalisiert sind, also von Anfang bis Ende alle Daten und alle Vorgänge digital erfolgen, können automatisierte Abläufe überhaupt eingesetzt werden. Damit fallen nicht nur für die Service-Empfänger unnötige Behördengänge weg, auch im *Back Office* der Verwaltung werden Kommunikations- und Koordinationsschritte eingespart und automatische Überprüfung von Informationen sowie die Umsetzung der daraus resultierenden Folgen tritt an die Stelle vieler Arbeitsschritte, die Zeit kosten und zudem durch vermeidbare Fehler belastet werden. Digitaler Organisationswandel lässt sich gezielt herbeiführen, es bedarf zu seiner Gestaltung aber eines Personal, Technologie und Organisation zusammendenkenden Ansatzes des *Change Managements*.

---

## Literatur

- Ashford, Susan J. 1988. Individual strategies for coping with stress during organizational transitions. *The Journal of Applied Behavioral Science* 24(1): 19–36.
- Baker, Jeff. 2012. The technology – organization – environment framework. In *Information systems theory. Explaining and predicting our digital society*, Hrsg. Yogesh K. Dwivedi, Michael R. Wade und Scott L. Schneberger, Bd. 1, 231–245. New York: Springer.
- Berger, Ariane. 2018. Die Digitalisierung des Föderalismus. *Die Öffentliche Verwaltung* 71(19): 799–806.
- Boyne, George A. 2002. Public and private management. What's the difference? *Journal of Management Studies* 39(1): 97–122.
- Bozeman, Barry, und Stuart Bretschneider. 1986. Public management information systems. Theory and prescription. *Public Administration Review* 46(Special Issue: Public Management Information Systems): 475–487.

- Deci, Edward L., und Richard M. Ryan. 1993. Die Selbstbestimmungstheorie der Motivation und ihre Bedeutung für die Pädagogik. *Zeitschrift für Pädagogik* 39(2): 223–238.
- Fernandez, Sergio, und Hal G. Rainey. 2006. Managing successful organizational change in the public sector. *Public Administration Review* 66(2): 168–176.
- Hackman, J. Richard, und Greg R. Oldham. 1976. Motivation through the design of work. Test of a theory. *Organizational Behavior and Human Performance* 16(2): 250–279.
- Heckmann, Dirk. 2013. Perspektiven des IT-Einsatzes in der öffentlichen Verwaltung. *Die Verwaltung* 46(1): 1–20.
- Jensen, Ulrich Thy, und Louise Ladegaard Bro. 2018. How transformational leadership supports intrinsic motivation and public service motivation. The mediating role of basic need satisfaction. *The American Review of Public Administration* 48(6): 535–549.
- Kickert, Walter J. M. 2014. Specificity of change management in public organizations. Conditions for successful organizational change in Dutch ministerial departments. *The American Review of Public Administration* 44(6): 693–717.
- Kuipers, Ben S., Malcolm Higgs, Walter Kickert, Lars Tummers, Jolien Grandia, und Joris Van der Voet. 2014. The management of change in public organizations. A literature review. *Public Administration* 92(1): 1–20.
- Lemke, Harald. 2013. IT-Einsatz in der öffentlichen Verwaltung. Sachstand, Herausforderungen, Perspektiven. *Die Verwaltung* 46(1): 123–134.
- Lips, A., Miriam B., Rose R. O'Neill, und Elizabeth A. Eppel. 2011. Cross-agency collaboration in New Zealand. An empirical study of information sharing practices, enablers and barriers in managing for shared social outcomes. *International Journal of Public Administration* 34(4): 255–266.
- Osterloh, Margit, und Bruno S. Frey. 1997. Sanktionen oder Seelenmassage? Motivationale Grundlagen der Unternehmensführung. *Die Betriebswirtschaft* 57(3): 307–321.
- Roux, Laetitia. 2015. Public service values and E-administration. An explosive mix? Illustration drawing on the case of the family allowance funds (Caisse d'Allocations Familiales) in France. *International Review of Administrative Sciences* 81(2): 227–244.
- Seibel, Wolfgang. 2016. *Verwaltung verstehen. Eine theoriegeschichtliche Einführung*. Berlin: Suhrkamp.
- Vahs, Dietmar. 2015. *Organisation. Ein Lehr- und Managementbuch*, 9. Aufl. Stuttgart: Schäffer-Poeschel.
- Venkatesh, Viswanath, und Fred D. Davis. 2000. A theoretical extension of the technology acceptance model. Four longitudinal field studies. *Management Science* 46(2): 186–204.
- Vonk, Guido, Stan Geertman, und Paul Schot. 2007. New technologies stuck in old hierarchies. The diffusion of geo-information technologies in Dutch public organizations. *Public Administration Review* 67(4): 745–756.
- Welch, Eric W., und Sanjay K. Pandey. 2007. E-Government and bureaucracy. Toward a better understanding of intranet implementation and its effect on red tape. *Journal of Public Administration Research and Theory* 17(3): 379–404.
- Wirtz, Bernd W., Robert Piehler, Marc-Julian Thomas, und Peter Daiser. 2016. Resistance of public personnel to open government. A cognitive theory view of implementation barriers towards open government data. *Public Management Review* 18(9): 1335–1364.
- Yoo, Youngjin, Richard J. Boland Jr., Kalle Lyytinen, und Ann Majchrzak. 2012. Organizing for innovation in the digitized world. *Organization Science* 23(5): 1398–1408.



---

# E-Leadership

Manuel Misgeld

## Inhalt

1 Klärung des Begriffs .....	600
2 Theoretisch-konzeptionelle Ansätze .....	601
3 Praxisbezogene Anwendungen und deren Probleme .....	603
4 Umsetzungsstand und Auswirkungen .....	606
5 Perspektiven für Staat und Verwaltung .....	607
Literatur .....	608

---

## Zusammenfassung

*E-Leadership* bezeichnet eine Personalführung, die mittels IT erfolgt, sich auf digitale Arbeitskontakte erstreckt und eine digitale Organisationsentwicklung und -kultur befördert. Die Interaktion von Führungskräften und Mitarbeiter\*innen in digitalen Kontexten ist komplex und lässt die Forderung nach neuen Methoden der Führung und des Führungsverständnisses aufkommen. Die digitale Transformation von Staat und Verwaltung lässt *E-Leadership* bedeutsamer werden, allerdings zeigen sich empirisch erst wenige Veränderungen in eine derartige Richtung.

---

## Schlüsselwörter

Digitale Führung · Transformationale Führung · Virtuelle Teams ·  
Medienreichhaltigkeitstheorie · Agile Methoden

---

M. Misgeld (✉)

Deutsches Forschungsinstitut für öffentliche Verwaltung Speyer, Speyer, Deutschland  
E-Mail: [misgeld@gmx.de](mailto:misgeld@gmx.de)

## 1 Klärung des Begriffs

Personalführung (synonym verwendet: „*Leadership*“) richtet sich darauf, das Arbeitsverhalten von Beschäftigten (ziel- und leistungsorientiert) zu beeinflussen. Sie wird direkt und indirekt durch Digitalisierung herausgefordert. Das zeigt sich in veränderten Arbeitsprozessen, neuen Formen der Kommunikation oder auch in erweiterten Aufgaben und Anforderungen der Beschäftigten. Zugleich kann die Führungstätigkeit durch IT unterstützt und verbessert werden. Daher erfolgt heute der Ruf nach einer Personalführung, die den dynamischen Rahmenbedingungen der Digitalisierung innerhalb der Verwaltung gerecht wird und diese befördert. Eine den digitalen Kontexten angepasste Personalführung wird in der Literatur als *E-Leadership* bezeichnet.

Sie lässt sich (1) so verstehen, dass mithilfe von Informations- und Kommunikationstechnik *instrumentell* ein leistungsrelevantes Verhalten der Mitarbeiter\*innen zielgerichtet beeinflusst werden kann. Dem zugrunde liegt (2) die *soziotechnische* Analyse einer fortschreitenden Digitalisierung der Arbeitswelt als eines Kontextes, der die Führungsbeziehung prägt respektive Personalverantwortliche und Beschäftigte zu neuen Formen des Kommunizierens führt. Schließlich verweist *E-Leadership* darauf, dass (3) über IT *gesellschaftliche Herausforderungen* und *organisatorische Anforderungen* entstehen oder sich verstärken können, die es nicht zuletzt seitens der Führungskräfte in der öffentlichen Verwaltung zu bewältigen gilt. Hierzu gehört auch, durch Personalführung personell und strukturell dazu beizutragen, dass *E-Government*-Projekte zielgemäß umgesetzt werden können. Dabei werden partizipativ-kooperative Führungsverständnisse, -konzepte und -stile präferiert, um die Mitarbeiter\*innen zu befähigen, sie in Entscheidungen einzubinden und dadurch auch eine höhere Akzeptanz von Digitalisierungsprozessen und einer neuen Ausrichtung der Organisation zu erreichen (Wald 2014). Die drei Perspektiven lassen sich wie folgt zusammenfassen: *E-Leadership* bezeichnet eine mittels IT erfolgende, an digitale Arbeitskontakte angepasste und auf eine zu digitalisierende (Arbeits-)Organisation ausgerichtete Personalführung. *Leadership* lässt sich dabei als strategische Personalführung begreifen. Sie umfasst ein komplexes Verhalten von Führungskräften in der Interaktion mit Beschäftigten und geht insofern über ein nach Leistungsoptimierung suchendes Management hinaus (Avolio et al. 2000; Wald 2014).

Zu berücksichtigen sind in allen drei Elementen dieser Definition von *E-Leadership* die Rollen, Aufgaben und Ziele von Führungskräften, etwa wie und welche Werte, Ziele und Erwartungen sie vermitteln, welche Organisationskulturen und Gemeinschaftsgefühle sie pflegen und wie sie Tätigkeiten der Beschäftigten koordinieren und Führungsaufgaben delegieren. Aber auch das dyadische Verhältnis respektive die wechselseitige Beeinflussung zwischen Mitarbeiter\*innen und Führungskräften ist bedeutsam. Dabei ist das Verhalten der Beschäftigten nicht nur eine abhängige, nachgeordnete Variable. Zu klären ist, wie digitales Arbeiten und Kommunizieren beispielsweise in ortsverteilten Teams abläuft, wie Teammitglieder die Führungskraft wahrnehmen und bewerten oder wie sich *E-Government*-Projekte und eine digitale Organisationsentwicklung fördern lassen, um auf veränderte Anforderungen an die öffentliche Verwaltung angemessen zu reagieren.

Die Rolle von IT in der *E-Leadership* lässt sich verschieden begreifen. In einem weiten Verständnis zählen Interaktionen zwischen Führungskräften und Mitarbeiter\*innen dazu, bei denen IT relevant ist oder verwendet wird. Enger gefasst werden darunter neue (orts- und zeitunabhängige) Arbeitsmodelle verstanden, die auch unter den Begriffen (mobile) Telearbeit oder Heimarbeit bekannt sind. Dabei muss nicht notwendigerweise oder von allen und jederzeit über IT kommuniziert werden. Ferner können anlassbezogen oder langfristig innerhalb einer Organisation und auch darüber hinaus Arbeitsgruppen (virtuelle Teams) oder Gemeinschaften entstehen, die über IT-Netzwerke, *Online-Foren* oder soziale Medien kommunizieren. Mitunter bezieht sich das Digitale aber auch darauf, dass veränderte Führungsansätze und Managementmethoden von IT-Unternehmen übernommen werden, die partizipative Entscheidungsfindungen und experimentelle sowie auf Lernen ausgerichtete Arbeitskulturen zu verbreiten suchen.

Der seit etwa zwei Dekaden verwendete Begriff der *E-Leadership* (Avolio et al. 2000) wird weder einheitlich verwendet noch ist er einzigartig. Auf ähnliche Inhalte beziehen sich oder werden mitunter synonym verwendet: Tele- oder *Distance-Leadership*, *Digital Leadership*, *Virtual Leadership*, *Computer-mediated Leadership*, *Remote* oder *Distributed Leadership* sowie *Leadership 2.0*. Auch eine geteilte, flüssige (*liquid*), agile Führung oder eine *Network Leadership* greifen ähnliche Überlegungen auf. Gemeinsam ist diesen Begriffen, dass sich eine Personalführung über IT verändert oder zu verändern ist. Adressiert sind dabei nicht nur der *Chief Information Officer* oder IT-Projektmanager, sondern grundsätzlich alle politisch gewählten oder ernannten Entscheidungsträger und beschäftigten Personalverantwortlichen in Staat und Verwaltung. Schließlich lässt sich Personalführung nicht ohne die (Interaktion zwischen) Mitarbeiter\*innen verstehen, die eine (digitale) Führungsbeziehung mitgestalten.

---

## 2 Theoretisch-konzeptionelle Ansätze

Ob es sich bei *E-Leadership* um eine eigenständige Theorie handelt oder das beigelegte „E-“ lediglich neue Anforderungen und aktuelle Kontextbedingungen von Führung aufgreift, ist kaum hinterfragt. So kann kritisiert werden, dass sich Ziele und Ausrichtung von Führung kaum oder nicht notwendigerweise von herkömmlichen Ansätzen einer Personalführung unterscheiden. Für eine eigenständige Bedeutung spricht dagegen, dass erst neue Kompetenzen und ein deutlich verändertes Führungsverhalten der Herausforderung durch Digitalisierung angemessen sind (Lilian 2014). Zudem wird IT nicht nur kontextuell, sondern auch instrumentell betrachtet und ist manifester Teil des Untersuchungsobjekts (Avolio et al. 2000). Dagegen ist einzuwenden, dass sich *E-Leadership* der ohnedies vielgestaltigen oder unklaren theoretischen Grundlagen des teils moralisch überhöhten Führungskonstrukts bedient. So sind die verschiedenen Ansätze teils verhaltenswissenschaftlich (Motivation und Kognition in dyadischen Beziehungen oder Gruppen) teils persönlichkeitspsychologisch (Rollen und Kontexte sowie charakterliche Eigenschaften von Führungskräften) ausgerichtet.

Grundsätzlich lassen sich nach den drei Perspektiven getrennt unterschiedliche theoretische Schwerpunkte ausmachen. So zeigt sich für

- (1) die Führung über IT, dass überwiegend Medientheorien zur Anwendung kommen. Prominent vertreten ist die Medienreichhaltigkeitstheorie (*Media Richness Theory*), wonach eine komplexe Kommunikationsaufgabe ein reichhaltiges (audiovisuelles, synchron übertragendes) Medium benötigt. Demzufolge zeigt sich eine wirkungsvolle Personalführung – also eine zielgerichtete Beeinflussung von Mitarbeiter\*innenverhalten und -einstellung – darin, dass die Führungskraft ein für die Aufgabe angemessenes Medium wählt. Somit ist zentral, welche medienbezogenen Effekte in der Führungstätigkeit wahrzunehmen sind.
- (2) Virtuelle Teams stehen im Vordergrund, wenn es um die Frage der Führung in digitalen Arbeitskontexten geht. Mitglieder virtueller Teams arbeiten teils örtlich und zeitlich unverbunden oder sind unterschiedlichen Einheiten und/oder Organisationen zugehörig, arbeiten aber mindestens in einigen Arbeitsbereichen vermittelt über moderne Technologie zusammen. Dabei kommt es zu einer Rückkoppelung: Die Verwendung von IT verändert einerseits die Art und Weise der Personalführung – insbesondere durch eine örtlich oder personell verteilte Führung. Andererseits vermag die Personalführung zu beeinflussen, welche und wie IT von den Teammitgliedern verwendet wird. Diese gegenseitige Beeinflussung seitens IT ist als emergent zu beschreiben – sie entwickelt sich eigenständig über die Gruppeninteraktion (Avolio et al. 2014). Bei der Frage, welches Führungsverhalten für solche virtuellen Teams zu empfehlen ist, wird häufig die Teamleistung zwischen „transaktional“ und „transformational“ geführten Arbeitsgruppen verglichen. Grundsätzlich sind beide Führungsstile in der *E-Leadership* möglich und auch anzutreffen: Die transaktionale Führung erfolgt eher direktiv und aufgabenorientiert. Sie ähnelt dem Menschenbild der sogenannten „Theorie X“, wonach eher arbeitsscheue Mitarbeiter\*innen über messbare Ziele und Leistungsanreize motiviert, kontrolliert und gegebenenfalls sanktioniert werden sollen. Die transformationale Führung ist eher partizipativ-kooperativ und folgt der „Theorie Y“, wonach soziale Bedürfnisse wie Anerkennung und Selbstverwirklichung die entscheidenden Motivatoren sind, die es zu nutzen und zu erhalten gilt (Lee 2009).
- (3) Führungsstile und organisatorische Strukturen können entscheidend dazu beitragen, Veränderungsprozesse zu unterstützen. Eine Führungsaufgabe besteht darin, günstige Rahmenbedingungen für eine digitale Verwaltungsarbeit zu schaffen. Für eine *E-Leadership*, die eine derartige digital-affine Organisation zu etablieren sucht, sind veränderte betriebswirtschaftliche Konzepte sowie neue Führungs- und Managementmethoden leitend. Theoretische Ansätze richten sich darauf, welche Persönlichkeitseigenschaften eine Führungskraft aufweisen sollte, wie diese zur Sinnstiftung in Veränderungsprozessen beitragen kann und wie ein *Change Management* respektive die Organisationsentwicklung mit einer demokratischen Führung verbunden werden können. Zugleich ist die Bereitschaft der Beschäftigten für Veränderungen sicherzustellen: Ein partizipatives, schrittweises Vorgehen soll dazu verhelfen, gemeinsame Ziele zu etablieren,

Umsetzungshürden und Widerstände zu verkleinern sowie kleine und sichtbare Fortschritte zu erzielen. Auf diesen Überlegungen basieren anwendungs- und beratungsorientierte Konzepte. Zu nennen sind beispielsweise die „Holokratie“ (partizipative Entscheidungsfindung mit wechselnden Arbeitsrollen und -aufgaben) sowie die „agile Führung“. Damit ist gemeint, dass eine Führungskraft phasenweise auf ein kurzfristiges Handeln und Entscheiden setzt. Eine langsame und aufwändige Abstimmung über verschiedene Hierarchieebenen hinweg soll damit abgelöst werden, womit die Bereitschaft zu und die Möglichkeiten für Veränderungen steigen sollen. Hierfür lassen sich auch agile Methoden verwenden, die der Softwareentwicklung entlehnt sind und beispielsweise als *Scrum* oder *Innovation Lab* bezeichnet werden. Zentral ist ein Lernen über kreativitätsfördernde Experimentierräume, flache Hierarchien und kurzfristige, gegenseitige Rückmeldungen.

---

### 3 Praxisbezogene Anwendungen und deren Probleme

Digitales Arbeiten oder von der IT-Nutzung beeinflusste Tätigkeiten sind im öffentlichen Sektor weit verbreitet. Zugleich ändern sich bereits Arbeitsmodelle, wenn mithilfe von IT örtlich verteilte oder mobile, zeitflexible Tätigkeiten und neue Formen der Zusammenarbeit möglich werden, etwa unter Nutzung von sozialen Netzwerken. Insofern ist das Anwendungsfeld von *E-Leadership* als hochaktuell anzusehen, da IT in der Arbeitsorganisation alltäglich geworden ist. Zugleich stellen sich besondere Anforderungen an eine *E-Leadership*, wenn *E-Government*-Ziele und -Projekte nicht erreicht oder nicht erfolgreich sind, sich vielmehr eine eklatante Lücke zwischen Anspruch und Wirklichkeit zeigt: Auf der einen Seite bestehen (lange vorhandene) Leitbilder, welche soweit gehen, eine nicht mehr spürbare Verwaltung und einen weitest gehenden Bürokratieabbau zu skizzieren. Hierzu zählen mögliche Automatisierungspotenziale Künstlicher Intelligenz sowie in anderen europäischen Ländern bereits etablierte, miteinander vernetzte sowie teilautomatisiert ablaufende Verwaltungsdienstleistungen. Auf der anderen Seite bestehen Verwaltungssilos fort, existiert ein föderales *E-Government* nur in Ansätzen und scheitern Leuchtturmprojekte nach langwierigen und kostenintensiven Planungen. Ebenfalls verbleibt die Zahl an *E-Government*-Nutzern unterdurchschnittlich und deren Zufriedenheit mit der Verwaltung ebenso. Angesichts dieser Lücke stellen sich erhöhte Anforderungen an die Personalführung im Sinne einer *E-Leadership* sowohl in der bereits etablierten digitalen Verwaltungsarbeit als auch in neuen Projekten wie etwa dem eines Portalverbundes und einem für Bürger und Unternehmen einheitlichen *Online*-Zugangs zu allen Verwaltungsleistungen (Misgeld und Wojtczak 2018).

Vielfältige Themen und Fragestellungen, die einen konkreten Anwendungsbezug für *E-Leadership* bieten, lassen sich dabei erkennen und skizzieren: In der *instrumentellen* Perspektive zeigt sich, dass digitale Werkzeuge wie *Social Media*, Videokonferenzen, Organisationsforen, *Wikipedia* oder *Cloud*-basierte Kollaborationsanwendungen in der Führungstätigkeit nutzbar sind und diese erweitern können. Entsprechend kann sich eine Informationsaufnahme und -verarbeitung erweitern

oder verbessern, wenn semantische Technologien aktuell diskutierte Inhalte aus sozialen Netzwerken zusammenfassen. Zugleich versprechen die genannten Werkzeuge, Mitarbeiter\*innen stärker zu beteiligen, neues Wissen aufzubauen, Ideen zu generieren und eine mögliche Distanz unter den Nutzern oder zur oberen Führungsebene zu verringern, die über zusätzliche Medienkanäle präsent sein kann. Gleichwohl ist auf die negativen Seiten einer ständigen Erreichbarkeit zu verweisen, auf erweiterte Kontrollmöglichkeiten und die damit zusammenhängenden Probleme des Datenschutzes und der mangelnden Privatsphäre. Außerdem ist die digitale Image- und Kontaktpflege unter Umständen aufwändig und erfordert Erfahrung sowie Feingefühl. Ferner ist einer verringerten organisatorischen Bindung entgegenzuwirken, die mit wegfallenden, direkten Kontaktmöglichkeiten aufgrund physischer Abwesenheit einhergeht. Auch hängt von den verwendeten Medien ab, ob reichhaltige Informationen übermittelt werden können. So fehlen nonverbale Informationen in sprach- oder textbasierter Kommunikation (*E-Mail* oder Telefon), was zu Missverständnissen führen kann. Um kreative Ideen zu entwickeln, mit denen komplexe Probleme zu lösen sind, erweisen sich solche Medien als unzureichend. Es gilt daher für die Personalführung, die neuen Werkzeuge auf ihre Chancen und Risiken kritisch zu reflektieren, um diese gezielt und umsichtig einzusetzen.

In der *soziotechnischen* Perspektive geht *E-Leadership* mit einem veränderten Verständnis von Personalführung einher. Annahme ist, dass eine auf Autorität und Weisungsbefugnis ausgelegte Personalführung kaum einer wissensintensiven Zusammenarbeit gerecht wird, die für die öffentliche Verwaltung bedeutsamer wird. So sind Führungskräfte auf einen engen Austausch mit selbstständig handelnden, zufriedenen und motivierten Mitarbeiter\*innen angewiesen, um fundierte und nachvollziehbare Entscheidungen angesichts komplexer und dynamischer Entwicklungen und unklarer Anforderungen oder Erwartungen treffen zu können. Nicht zuletzt relativiert der breite und leicht verfügbare Quellenzugang im *Internet* sowie eine veränderte Kommunikation in den sozialen Medien die Ansicht, dass Personalverantwortliche über einen mutmaßlichen Informationsvorsprung gegenüber den IT-affinen Mitarbeiter\*innen oder informierten Bürger\*innen verfügen. In einem veränderten Führungsverständnis geht es darum, in wechselseitiger Anerkennung, vertrauens- und respektvoll zusammenzuarbeiten und zu kooperieren, damit sich im gegenseitigen Lernen die unterschiedlichen Fähigkeiten und Wissenshintergründe (so zwischen den tendenziell älteren Führungskräften und den jüngeren *Digital Natives*) bereichern können. Daran ist allerdings eine wissensbezogene (kognitive) Distanz hinderlich, die auf unterschiedliche berufliche Hintergründe und soziale Prägungen zurückzuführen ist, insbesondere dann, wenn sich diese in interdisziplinären Arbeitsgruppen oder in organisations- oder sektorenübergreifender Zusammenarbeit zeigt. Zugleich vermag sich die soziale, emotionale und räumliche (Organisations-)Bindung der Beschäftigten aufzulösen. Soziales Kapital, etwa das gegenseitige Vertrauen sowie enge Kontakte und Beziehungsnetzwerke, drohen darunter zu leiden – mit der Folge geringerer Motivation und schwierigerer Arbeitskoordination. Diese Distanz und organisatorische Entfremdung ist entsprechend zu verringern: Führungskräfte können die Kommunikation anregen oder moderieren, Präsenzzeiten vorsehen oder die Zusammenarbeit durch geteilte, selbstorganisierte Aufgaben verstärken. Entsprechend baut *E-Leadership* überwiegend auf eine transformationale Führung,

welche Beschäftigten zusätzliche Freiräume dabei gibt, ihre Arbeitsprozesse zu gestalten und die benötigten methodischen, fachlichen und sozialen Kompetenzen zu erweitern und zu intensivieren. Ziel ist, die Mitglieder insbesondere von virtuellen Arbeitsgruppen darin zu unterstützen, soziale Netzwerke zu pflegen sowie neue Medien effektiv einzusetzen. Entsprechend dieser transformationalen Perspektive von *E-Leadership* ist einer Distanz von Führungskraft und Mitarbeiter\*innen entgegenzuwirken, indem eine offene Kommunikation auch über neue Medien erfolgt und dabei nicht nur die Kontrolle von Leistungszielen entscheidend ist. Die transformationale Führungskraft nimmt in ihrer modellhaften Ausformung vielmehr die Rolle eines Vorbilds und Mentors ein: Sie ist offen, empathisch und wertschätzend für die Perspektiven und Bedürfnisse der Beschäftigten, unterstützt diese beziehungsorientiert und individuell, vermag zu inspirieren und zu motivieren. Dabei gilt es zugleich, die mit der Digitalisierung einhergehenden Arbeitsbelastungen zu berücksichtigen: Neue Anforderungen, veränderte Prozesse, anwachsende Informationsströme und ein ständiger Kompetenzerwerb („lebenslanges Lernen“) drohen Mitarbeiter\*innen zu überfordern. Hinzu kommt, dass ständige Erreichbarkeiten („*always on*“) und zeitlich wie örtlich flexible Arbeitszeitmodelle sich negativ auf Erholungs- und Ruhephasen auswirken können und die Grenze zwischen beruflicher und privater Sphäre verwischen. Auch hier setzen praktische Empfehlungen in der *E-Leadership*-Literatur an, wonach Führungskräfte etwa Zeiten der Nichterreichbarkeit einführen und vorleben, für eine Ausstattung an Arbeitsmitteln oder möglichen Fortbildungsmaßnahmen sorgen und einen aktiven wie gezielten Umgang mit IT fördern (Boos et al. 2017; Wald 2014; skeptischer sind Hoch et al. 2007, die eine transaktionale Führung bevorzugen).

In der *gesellschaftlichen* und *organisatorischen* Perspektive schließlich wird deutlich, dass scheiternde, langwierige und kostenintensive *E-Government*-Projekte mit einer defizitären *E-Leadership* zusammenhängen. Dies lässt sich einerseits auf unklare oder nicht vorhandene Entscheidungsstrukturen zurückführen, über welche die Arbeit zwischen den Ministerien, Behörden und relevanten Stellen (vertikal) sowie den staatlichen Ebenen (horizontal) zu koordinieren ist. Wie eine Personalführung die erforderlichen Veränderungen fördert und begleitet, die mit einheitlichen Zugang zu allen Verwaltungsdienstleistungen über ein Bürgerportal einhergehen, bleibt eine offene und angesichts der im internationalen Vergleich defizitären Ausgestaltung des *E-Government* dringliche Frage. So erfordert ein vernetztes *E-Government* nicht nur neue Kompetenzen im Umgang mit IT, etwa um effizient und zielgerichtet digitale Medien zu verwenden. Um diese sich anzueignen und zielgerichtet anzuwenden, ist von Mitarbeiter\*innen (aber auch Führungskräften) eine hohe Veränderungsbereitschaft verlangt. Auch zeigt sich, dass eine über die eigene Organisationseinheit hinausgehende Zusammenarbeit allgemein erforderlich ist und angesichts eines vernetzten *E-Government* umso wichtiger erscheint. Die dabei entstehenden, notwendigerweise (physisch und organisationsübergreifend) verteilten, virtuellen Arbeitsgruppen agieren in komplexen und verschiedenartigen Umfeldern. Um sowohl Mitarbeiter\*innen vor Ort als auch auf Distanz mit jeweils unterschiedlichen Bedürfnissen angemessen zu leiten, wird von Führungskräften mitunter erwartet, multiple Verhaltensmuster anzuwenden und diese situationsgebunden oder phasenweise zu wechseln. Solch eine wechselnde beziehungsweise

„ambidextre“ (beidhändige) Führung ist entscheidend, da eine organisationskulturelle Bindung der Gruppenmitglieder unterschiedlich stark oder inhaltlich verschiedenartig ausgeprägt ist (Hill 2016; Petry 2016). Insbesondere in der Anfangsphase sollten Führungskräfte dafür sorgen, dass gemeinsame Vorstellungen dazu entstehen, welche Ziele anzustreben sind, damit sich die Mitglieder mit diesen identifizieren können. Auch ist zu klären, ob die Ziele mit denen anderer Organisation (seinheit)en kompatibel sind, wie diese verfolgt und umgesetzt und welche Arbeitsleistungen von den Mitarbeiter\*innen erwartet werden können. Dies kann dazu beitragen, die eigene Arbeit als sinnhaft und motivationsförderlich zu erachten. Entsprechend können Führungskräfte rollenklärend sowie vertrauensfördernd und beziehungsorientiert agieren, um Tätigkeiten zu koordinieren, Wissen zu teilen, ein gemeinsames Zielverständnis zu entwickeln und somit in der Verwaltung kooperatives Handeln zu ermöglichen. Dies gilt insbesondere dann, wenn Mitarbeiter\*innen längerfristig mit komplexen und unstrukturierten Aufgaben in einem dynamischen Umfeld betraut sind und ihre Arbeitsleistungen ineinander greifen und voneinander abhängig sind. Wenn sich im weiteren Verlauf eine engere Zusammenarbeit herausgebildet hat oder diese nur anlassbezogen und kurzfristig notwendig ist sowie einfachere Aufgaben repetitiv zu erledigen und Entscheidungen rasch zu treffen sind, erscheint ein transaktionales Führen als angemessen, indem Ziele vermittelt, Leistungen bewertet und entsprechende Anerkennung oder Kritik geäußert werden (Parry 2011, S. 56–57).

Der in dieser dritten Perspektive von *E-Leadership* häufig angeführte Ansatz der agilen Führung gilt als hilfreich, eine digital affine Organisationskultur zu fördern. Ein Ziel ist dabei, veränderungsresistente, auf bekannte Verhaltensmuster und Regeln ausgerichtete Einstellungen zu hinterfragen und zugunsten einer partizipativen Entscheidungsfindung abzulösen. Dies ist etwa über flexible Arbeitsstrukturen und eine Feedback- und Fehlerkultur möglich, in denen Mitarbeiter\*innen Führungsaufgaben übernehmen, Ideen einbringen sowie diese eigenverantwortlich und experimentell umsetzen.

---

## 4 Umsetzungsstand und Auswirkungen

In der jüngeren Forschungsliteratur zum Thema *E-Leadership* hat sich noch keine einheitliche Auffassung entwickelt, wie Personalführung und Digitalisierung aufeinander wirken oder wirken sollten. Zudem ist die Literatur stark von praxisbezogenen Konzeptionen, beratungsorientierten Gestaltungsempfehlungen und einer mit dem Führungsbegriff einhergehenden Theorienvielfalt geprägt. Dabei lässt sich ein normativ aufgeladenes Führungsverständnis ausmachen, das aber auf einer immer noch unzureichenden empirischen Grundlage fußt. Verwaltungswissenschaftliche, empirische Untersuchungen zur *E-Leadership* in Deutschland sind bislang nicht durchgeführt worden. So hat zwar Vogel (2016) eine umfängliche Studie der Personalführung im öffentlichen Sektor veröffentlicht. Darin finden sich jedoch keine Bezüge zu IT und ihrer besonderen Rolle. Dagegen ist im Schweizer Kontext untersucht worden, wie *E-Leadership* als Instrument genutzt wird, was sich jedoch nur auf die Privatwirtschaft

erstreckt (Müller 2008). Der englischsprachigen Literatur wiederum ist eine Vielzahl von (insbesondere experimentell angelegten) Studien zu entnehmen, die sich wiederum nicht auf Staat und Verwaltung beziehen (Wald 2014). Hierin zeigt sich etwa, dass ein gezielt eingesetztes Führungsverhalten dazu beiträgt, das geringere Zusammengehörigkeitsgefühl und gegenseitige Vertrauen in virtuellen, divers zusammengesetzten Teams zu stärken, was zur erfolgreichen Zusammenarbeit beiträgt (Avolio et al. 2014).

Im Gegensatz zu den mit Studierenden experimentell durchgeführten Untersuchungen sind bisher vorliegende Befunde für den öffentlichen Sektor jedoch nicht auf *E-Leadership* bezogen oder eher narrativer Natur und nicht systematisch-wissenschaftlich erarbeitet. Außerdem stellen sich allgemein Fragen der Übertragbarkeit aus dem Privatsektor, insofern als Brüche bei Werten, Selbstverständnis und prinzipiengeleiteten Anforderungen an Staat und Verwaltung absehbar sind. Zwar gibt es etliche Beispiele, in denen z. B. virtuelle Teams vorzufinden sind. Bereits seit Längerem ist ein räumlich verteiltes Arbeiten im Informationsverbund Bonn-Berlin möglich. Auch sind Mitarbeiter\*innen im Außendienst, Home-Office oder mobiles Arbeiten bekannt, wenngleich dies für agile Methoden noch nicht der Fall ist (Hill 2015). Hinzu kommen Experimentierräume wie jüngst im Rahmen des von der Bundesregierung betriebenen Dialogprozesses Arbeiten 4.0 (Bundesministerium für Arbeit und Soziales 2018). Dennoch sind die hierbei gewonnenen Erkenntnisse und Anwendungsfelder aus Sicht einer (digitalen) Personalführung nicht systematisch analysiert worden. *E-Leadership* ist damit im öffentlichen Sektor empirisch nicht erschlossen; Anwendungsbeispiele sind vorhanden, aber noch nicht erforscht.

Eine Ausnahme stellt die auf eine moderne Personalpolitik gerichtete, vom Bundesministerium für Arbeit und Soziales geförderte „Initiative Neue Qualität in der Arbeit“ dar: Das in diesem Rahmen geförderte Projekt „Führung im digitalisierten öffentlichen Dienst – FührDiv“ richtet sich auf die Herausforderungen und Anforderungen durch virtuelles Führen und eine digitalisierte Arbeitsorganisation. Auch behandelt das Projekt partizipative Aushandlungsprozesse und IT-Kompetenzen. In sechs Pilotorganisationen der öffentlichen Verwaltung sollen praktische Lösungen und Instrumente erarbeitet werden. Diese reichen von Führungskultur und -rollen in virtuellen Teams über Leitfäden für gute digitale Führung bis hin zu geänderten Dienstvereinbarungen und Stellenbeschreibungen (wmp consult 2018). Über die einzelnen Beschreibungen hinausgehende Ergebnisse stehen jedoch noch aus.

---

## 5 Perspektiven für Staat und Verwaltung

Angesichts einer tatsächlichen oder eingeforderten vernetzten Verwaltungsorganisation ist zu erwarten, dass die Bedeutung von *E-Leadership* für die Verwaltungsarbeit steigt. Nahe liegt zumindest, dass eine transformationale oder eine agile Führung hilfreich ist, *E-Government*-Projekte zu begünstigen. Analysen sind erforderlich, die kritisch untersuchen, wie IT die Personalführung im öffentlichen Sektor verändern kann, welche Folgen hieraus für Motivation und Vertrauen im öffentlichen Dienst erwachsen und wie sich Informationsflüsse qualitativ und quantitativ ändern, wenn sich neue Arbeitsformen (Telearbeit, virtuelle Teams) ausprägen. Dies gilt auch dahingehend, dass IT standardi-

sierbare Tätigkeiten zunehmend (teil)automatisiert und zugleich die Wissensarbeit bedeutsamer werden lässt. Erhebliche Auswirkungen auf den öffentlichen Dienst sind zwar noch nicht genau vorherzusehen aber durchaus wahrscheinlich. Veränderte Stellenanzahl und -profile, Prozesse und Abläufe sowie neue Anforderungen an Aus- und Fortbildung fordern dann nach einer digitalen Personalführung.

Ohne kritisch analysierte Anwendungsbeispiele bleibt es im Wesentlichen bei einem Empfehlungscharakter von *E-Leadership*. Allein Erkenntnisse aus privaten Unternehmen oder aus experimentellen Untersuchungen stützen das Leitbild der *E-Leadership*. Dementsprechend sind eine transformationale oder agile Führung nicht vorbehaltlos für den öffentlichen Sektor zu empfehlen. Sie eignen sich allenfalls für komplexe Arbeitskontakte und dynamische Umfelder, in denen ein hoher Grad an selbstorganisierten Arbeiten und kurzfristig, mitunter eigenverantwortlich getroffenen Entscheidungen erwartet werden kann. Welchen Einfluss eine veränderte Personalführung in einem solchen Kontext haben kann, in dem Personalverantwortliche dadurch führen, dass sie Ziele überzeugend vermitteln, als Mentoren fungieren und die Mitarbeiter\*innen individuell unterstützen, ist für den öffentlichen Sektor noch zu belegen. Auch ist fraglich, inwieweit Personalverantwortliche über gegebene charakterliche Eigenschaften oder mittels eines angeeigneten Führungsverhaltens dafür sorgen können, dass ein vernetztes *E-Government* über eine vertrauensvolle, engagierte und innovationsorientierte Zusammenarbeit gefördert wird.

Zu klären ist zudem, inwiefern Führungskräfte authentisch und ethisch konsistent handeln, wenn sie unterschiedliche Rollen einnehmen. Problematisch erscheinen damit einhergehende, unklare oder überbordende Anforderungen. Diese entsprechen einem geradezu heroisch-charismatischen Bild einer Führungskraft, was sich letztendlich als trügerisch und für eine geteilte oder partizipative Führung kontraproduktiv herausstellen muss. Eine *E-Leadership* ist somit verhaltensorientiert darauf zu überprüfen, wie sich eine „beidhändige“, situative bzw. kontextabhängige Personalführung auszuwirken vermag. Ethisch zu hinterfragen ist eine IT-Nutzung, die nur oder vorrangig dazu dient, Leistungs- und Verhaltensdaten zu sammeln und auszuwerten, um den Arbeitsdruck zu erhöhen. Dies entspricht einem hierarchischen, direktiven Führungsverständnis, das als wenig vertrauensfördernd und mitarbeiter\*innenbezogen gilt und somit zu unerwünschtem Leistungsverhalten und Demotivation führen kann. Angesichts der fortschreitend digitalen Verwaltungsarbeit und des defizitär ausgestalteten *E-Governments* bleibt somit die Frage, welchen praktischen Beitrag das Konzept der *E-Leadership* für die Gestaltung einer digitalisierten Verwaltung in nächster Zukunft leisten kann.

---

## Literatur

- Avolio, Bruce J., Surinder Kahai, und George E. Dodge. 2000. E-leadership. Implications for theory, research, and practice. *Leadership Quarterly* 11(4): 615–668.  
Avolio, Bruce J., John J. Sosik, Surinder S. Kahai, und Bradford Baker. 2014. E-leadership. Re-examining transformations in leadership source and transmission. *The Leadership Quarterly* 25(1): 105–131.

- Boos, Margarete, Thomas Hardwig, und Martin Riethmüller. 2017. *Führung und Zusammenarbeit in verteilten Teams*. Göttingen: Hogrefe.
- Bundesministerium für Arbeit und Soziales. 2018. Praxisbeispiele. Arbeiten 4.0 Experimentierräume. <https://www.experimentieraeume.de/experimentieraeume/>. Zugriffen am 19.03.2020.
- Hill, Hermann. 2015. Wirksam verwalten. Agilität als Paradigma der Veränderung. *Verwaltungarchiv. Zeitschrift für Verwaltungslehre, Verwaltungsrecht und Verwaltungspolitik* 106(4): 397–416.
- Hill, Hermann. 2016. Führung in digitalisierten Arbeitswelten. *Verwaltung & Management* 22(5): 241–249.
- Hoch, Julia E., Panja Andreßen, und Udo Konradt. 2007. E-Leadership und die Bedeutung Verteilter Führung. *Wirtschaftspsychologie* 9(3): 50–57.
- Lee, Margaret R. 2009. E-ethical leadership for virtual project teams. *International Journal of Project Management* 27(5): 456–463.
- Lilian, Snellman C. 2014. Virtual teams. Opportunities and challenges for E-leaders. *Procedia. Social and Behavioral Sciences* 110:1251–1261.
- Misgeld, Manuel, und Markus Wojtczak. 2018. Führung in der Netzwerkverwaltung. In *Digitalisierte Verwaltung. Vernetztes E-Government*, Hrsg. Margrit Seckelmann, 633–654. Berlin: Erich Schmidt.
- Müller, Renato C. 2008. *E-Leadership. Neue Medien in der Personalführung*. Norderstedt: Books on Demand.
- Parry, Ken W. 2011. Leadership and organization theory. In *The Sage handbook of leadership*, Hrsg. Alan Bryman, David Collinson, Keith Grint, Mary Uhl-Biel und Brad Jackson, 53–70. London: Sage.
- Petry, Thorsten. 2016. Digital Leadership. Unternehmens- und Personalführung in der Digital Economy. In *Digital Leadership. Erfolgreiches Führen in Zeiten der Digital Economy*, Hrsg. Thorsten Petry, 21–82. Freiburg: Haufe.
- Vogel, Dominik. 2016. *Führung im öffentlichen Sektor. Eine empirische Untersuchung von Einflussfaktoren auf das Führungsverhalten*. Potsdam: Universitätsverlag Potsdam.
- Wald, Peter M. 2014. Virtuelle Führung. In *Aktuelle Führungstheorien und -konzepte*, Hrsg. Rainhart Lang und Irma Rybníkova, 355–386. Wiesbaden: Springer Gabler.
- wmp consult. 2018. Projekt FührDiv. Führung in der digitalisierten öffentlichen Verwaltung. <https://fuehrdiv.org/projekt-fuehrdiv.h.html>. Zugriffen am 19.03.2020.



---

# E-Kompetenzen

Nadine Ogonek, Michael Räckers, Steffen Gilge und Sara Hofmann

## Inhalt

1 Einleitung .....	612
2 Klärung des Begriffs .....	612
3 Theoretische/Analytische Grundlagen .....	614
4 Praktische Anwendungsfelder .....	615
5 Umsetzungsstand und Auswirkungen .....	619
6 Ausblick/Perspektiven .....	619
Literatur .....	622

---

## Zusammenfassung

Die Digitalisierung der öffentlichen Verwaltung bedarf einer adäquaten Vorbereitung aller Beteiligten, denn sie setzt einen kompetenten Umgang mit IT auf allen Ebenen innerhalb der Verwaltungen und allen föderalen Ebenen voraus. Dieses Kapitel beschäftigt sich mit der Kategorisierung, dem Erwerb und der Vermittlung der benötigten E-Government-Kompetenzen, kurz: „E-Kompetenzen“. Nach einer einführenden Klärung des Begriffes E-Kompetenz und theoretischer Fundierung

---

N. Ogonek (✉)

Westfälische Wilhelms-Universität Münster, Münster, Deutschland

E-Mail: [nadine.ogonek@uni-muenster.de](mailto:nadine.ogonek@uni-muenster.de)

M. Räckers

European Research Center for Information Systems, Westfälische Wilhelms-Universität Münster, Münster, Deutschland

E-Mail: [michael.raeckers@ercis.uni-muenster.de](mailto:michael.raeckers@ercis.uni-muenster.de)

S. Gilge

Sächsische Staatskanzlei, Dresden, Deutschland

E-Mail: [steffen.gilge@sk.sachsen.de](mailto:steffen.gilge@sk.sachsen.de)

S. Hofmann

Department of Information Systems, University of Agder, Kristiansand, Norwegen

E-Mail: [sara.hofmann@uia.no](mailto:sara.hofmann@uia.no)

werden zwei Werkzeuge zur E-Kompetenz-Erfassung und -Evaluation vorgestellt sowie Einsatzmöglichkeiten skizziert. Ein Ausblick auf mögliche Weiterentwicklungen der Werkzeuge rundet das Kapitel ab.

### Schlüsselwörter

E-Government-Kompetenzen · Digitale Transformation des öffentlichen Sektors · Digitaler Wandel · Kompetenzsteckbrief · Referenzrolle · Öffentlicher Dienst

---

## 1 Einleitung

Die Digitalisierung wirkt sich stark auf das Arbeitsumfeld im öffentlichen Dienst aus: Die Potenziale der Informationstechnologie (IT) werden genutzt, um Bürger\*innen Nähe, Effizienz und Effektivität staatlichen Handelns zu verbessern. Normen, Strukturen, Abläufe, Führung, Arbeitsinstrumente und auch die Art und Weise der Kommunikation zwischen Beschäftigten, Behörden und in der Interaktion mit Bürger\*innen und Unternehmen verändern sich. Gleichzeitig bestehen rechtsstaatliche Prinzipien und damit Anforderungen wie Rechtmäßigkeit, Gleichbehandlung und Nachvollziehbarkeit fort.

Die Vielzahl und Vehemenz der Veränderungen, die durch den IT-Einsatz in Staat und Verwaltung verursacht oder begünstigt werden, erfordern neue Kompetenzen bei allen Beschäftigten, gleich ob Fach- oder Führungskraft, IT-Personal oder IT-Nutzer\*in. Um auf die Fähigkeiten und Fertigkeiten zu fokussieren, mit denen diese verschiedenen Personen spezifische Probleme im Arbeitsumfeld des öffentlichen Dienstes erfolgreich und verantwortungsvoll lösen können, wird hier, wie mittlerweile auch an vielen anderen Stellen, der Kompetenzansatz gewählt. Im Unterschied zum Qualifikationsansatz werden dadurch auch Fähigkeiten und Fertigkeiten erfasst, die in nicht-formalen Bildungsprozessen, also etwa in der praktischen Tätigkeit, ausgeprägt bzw. erworben wurden.

---

## 2 Klärung des Begriffs

Das Bündel an erforderlichen neuen Kompetenzen, welches für die Digitalisierung der öffentlichen Verwaltungen benötigt wird, kann mit Begriffen wie Medienkompetenz oder IT-Kompetenz nicht umfassend bezeichnet werden. Denn zusätzlich zur persönlich-instrumentellen Dimension des Umgangs mit IT bzw. elektronischen Inhalten ist auch die integrierte Gestaltung von Recht, Organisation und Technik sowie die Anpassung der Führungstätigkeit zu betrachten. Um diesem höheren Anspruch Ausdruck zu verleihen, wird hier – aufbauend auf Schuppan (2009) und Hill (2011) – der Begriff „E-Kompetenz“ genutzt. Kernelemente einer Kompetenz sind Wissen, Fähigkeiten, Fertigkeiten und Persönlichkeitseigenschaften. Dabei lassen sich Kompetenzen in fachliche, soziale und personale Kompetenzen unterscheiden (Schuppan 2009).

Nach Hill können E-Kompetenzen „[...] als die Fähigkeit verstanden werden, sich [...] innerhalb von durch moderne Techniken erweiterten Informationsräumen und mit technikunterstützten Methoden kreativ und selbstorganisiert zurecht zu finden.“ Aufbauend auf diesem Verständnis geht es bei den für die Digitalisierung nötigen Kompetenzen daher darum, in (einfachen und komplexen) Arbeitssituationen der Verwaltung durch das Verstehen, Anwenden und Gestalten digitaler Systeme zur Verbesserung der Aufgabenerledigung beizutragen.

Die Überlegungen von Schuppan und Hill sind für den Organisationstypus der öffentlichen Verwaltung besonders passfähig, vor allem im Vergleich zum ‚fließenden Konzept‘ der individuellen „digitalen Souveränität“ (vgl. etwa Goldacker 2017 oder Gräf et al. 2018).

Der Begriff „E-Kompetenz“ soll, diesem Prinzip folgend, hier wie folgt verstanden werden:

E-Kompetenzen bezeichnen verschiedene Bündel an kognitiven Fähigkeiten und Fertigkeiten, mit denen

- spezifische Aufgaben in einer Organisation durch die zielgerichtete, verantwortungsvolle Nutzung von Informations- und Kommunikationstechnik unter Berücksichtigung einschlägiger Normen erfolgreich erfüllt (Fähigkeit, *operativ* und konkret IT bei der Aufgabenerfüllung zu nutzen und zielgerichtet einzusetzen) und
- die Rahmenbedingungen für den Einsatz der Informations- und Kommunikationstechnik, insbesondere in rechtlicher, organisatorischer, technischer und/oder personeller Hinsicht adäquat gestaltet und gesteuert werden können (Fähigkeit, die IT-Landschaft einer öffentlichen Verwaltung *strategisch* zu gestalten, zielgerichtet die richtige IT auszuwählen und in die Prozesse und Abläufe einzubinden usw.)

sowie soziale Fähigkeiten und weitere Persönlichkeitsmerkmale, um diese Bündel an Fähigkeiten und Fertigkeiten in variablen Situationen wirksam nutzen zu können.

Dass sich der Begriff E-Kompetenz nicht allein auf das Beherrschung von Programm- und Gerätefunktionen beziehen kann, wird schon beim Blick auf den Arbeitsalltag der Beschäftigten im öffentlichen Dienst offenbar. Elektronische Nachrichten erhöhen die Geschwindigkeit der Kommunikation und die Erwartung an eine Reaktion. Die örtliche Flexibilität steigt z. B. durch Telearbeit. Der Austausch von Angesicht zu Angesicht und die Zusammenarbeit im Team verändern sich. Das Internet ermöglicht es, bei der Vorbereitung von Entscheidungen und der Lösung von Problemen erweiterte Wissensbestände einzubeziehen. Die steigende Menge an zu verarbeitenden Informationen wird für manchen zur unbeherrschbaren Flut. Die Vernetzung der Technik erfordert von jedem Einzelnen eine erhöhte Aufmerksamkeit zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit der Informationen. Insgesamt müssen die Beschäftigten mit gleichermaßen breiten wie tiefgreifenden Konsequenzen des Einsatzes der IT und deren ständiger Weiterentwicklung Schritt halten. Hierfür ist ein Grundverständnis für die Prinzipien der Informationsverarbeitung

nötig. Jede\*r Beschäftigte muss die Potenziale der IT für seine/ihre Tätigkeit im vernetzten Prozess der Leistungserstellung erkennen und nutzen können.

Für eine Führungskraft gilt das Vorgenannte gleichermaßen. Zusätzlich ist sie dafür verantwortlich, dass die Beschäftigten in ihrem Bereich mit adäquater IT ausgestattet sind, diese ordnungsgemäß bedienen können und Anforderungen z. B. des Datenschutzes und der Informationssicherheit erfüllen. Zudem muss eine Führungskraft dafür Sorge tragen, dass neue Potenziale der Technik genutzt werden, um ihren Bereich zu modernisieren, z. B. in organisatorischer oder rechtlicher Hinsicht. Dafür sind fachliche Erfordernisse mit technischen Möglichkeiten abzustimmen und Schnittstellen jenseits des eigenen Fachbereichs mitzudenken und zu definieren. Nicht zuletzt ist die Führungstätigkeit selbst auf neue Gegebenheiten einzustellen, wie z. B. das Führen auf Distanz im Falle von bereits genannter Telearbeit. Insgesamt müssen Führungskräfte die IT als wesentliches Element der Gestaltung und Steuerung ihres Bereichs berücksichtigen. Hierfür ist Überblickswissen zu den Möglichkeiten, die der Einsatz der IT bietet, nötig.

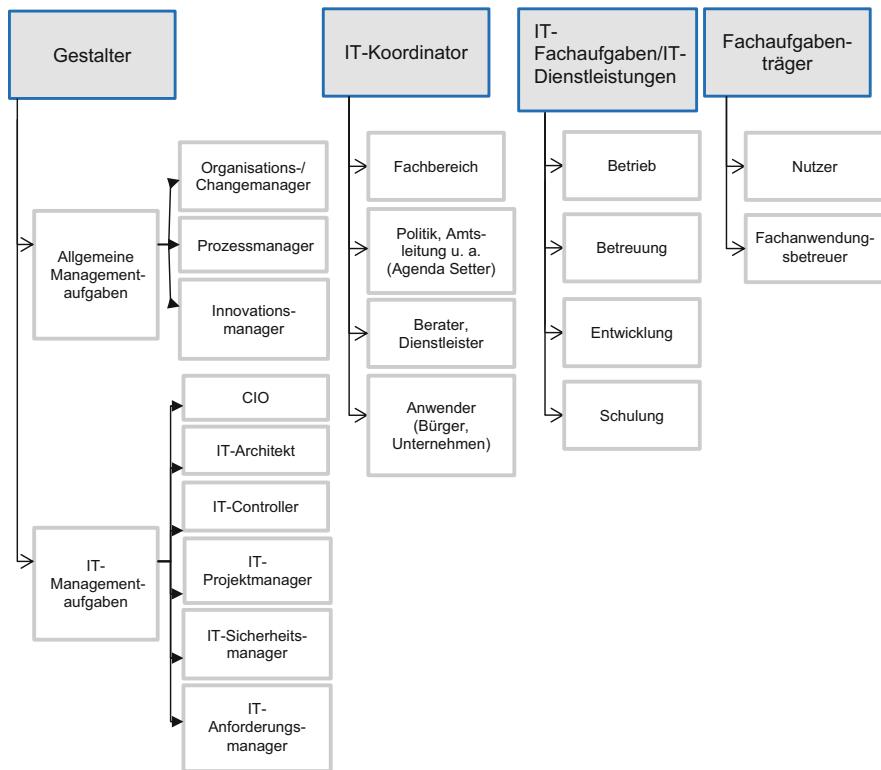
Im hier vorgeschlagenen Verständnis des Begriffs E-Kompetenz bleibt die konkrete Ausgestaltung und der Betrieb der IT der Zuständigkeit des IT-Personals vorbehalten. Dieses muss nicht nur den Einsatz der IT entsprechend den fachlichen Anforderungen des jeweiligen Bereichs und bestehender Festlegungen in der Organisation vorbereiten und begleiten, sondern angesichts zunehmenden Outsourcings vermehrt auch IT-Dienstleister steuern können. Dabei macht die Geschwindigkeit des technischen Fortschritts beständiges Lernen und Anpassungen notwendig. Wichtig ist hier festzuhalten, dass dieses spezifische IT-Personal nicht im engeren Sinne unter die Kategorisierung der Rollen und der zugeordneten E-Kompetenzen fällt, sondern hier im besonderen Maße auf die Bediensteten mit fachlich-inhaltlichem Fokus geschaut wird.

---

### 3 Theoretische/Analytische Grundlagen

Das theoretische Grundgerüst zum Begriff E-Kompetenz ist noch lückenhaft und weiter auszuarbeiten. Auch wenn die allgemeine Diskussion um Kompetenzen und Fähigkeiten in der Organisationslehre breit verankert ist, ist die spezielle Fokussierung auf E- bzw. E-Government-Kompetenzen bisher nicht in der Breite diskutiert, was sicher auch dem vergleichsweise neuen und insbesondere sich dynamisch entwickelndem Anwendungsfeld geschuldet ist. Die nachfolgend dargestellten Aktivitäten und Überlegungen beschreiben erste Schritte auf dem Weg zu diesem Ziel.

Die konkrete Ausprägung der E-Kompetenzen für Staat und Verwaltung wurde in der Studie von Becker et al. (2016), aufbauend auf der Studie von Schuppan et al. (2014), im Auftrag des IT-Planungsrats entwickelt. Im Rahmen der Studie wurden insgesamt 19 Referenzrollen der öffentlichen Verwaltung mit IT-Bezug identifiziert und kategorisiert. Die Orientierung und Strukturierung anhand von Rollen folgte dem Gedanken, dass sich so enger an dem Konzept von Stellen orientiert werden konnte, einem in der öffentlichen Verwaltung dominierenden Ansatz. Dabei kann



**Abb. 1** Referenzrollen der Verwaltung

eine Rolle einer Stelle entsprechen; gerade bei kleineren Verwaltungseinheiten können aber auch mehrere Rollen von einer einzigen Stelle bekleidet werden. Rollen bieten auf diese Weise die Möglichkeit, Aufgaben und Tätigkeiten zu bündeln und im Weiteren mit entsprechenden IT-Kompetenzen in Bezug zu setzen. Dies ermöglicht es, einen strukturierenden Rahmen um gleichartige oder miteinander in Bezug stehende Aufgaben und Tätigkeiten sowie hierfür nötige IT-bezogene Fähigkeiten zu ziehen und diesem Rahmen einen Namen, die Rollenbezeichnung, zu geben, der in der weiteren Verwendung und Anwendung hilft, ein allgemeineres Verständnis zu definieren (Abb. 1).

## 4 Praktische Anwendungsfelder

Für die heute in der Verwaltung benötigten Berufsbilder bedarf es einer strukturierteren Einordnung der vorhandenen Rollen, um einerseits eine bessere Orientierung auf Seiten der Personalabteilung zu schaffen und andererseits auch eine bessere Ausstattung mit benötigten Kompetenzen zu garantieren. Eine Rolle im öffentlichen

Dienst – gleich welcher Natur – ist mit einem speziellen Bündel Kompetenzen ausgestattet. Klar ist, dass Digitalisierung ein zentrales Thema ist, das alle Beschäftigten betrifft und somit davon auszugehen ist, dass alle Beschäftigen ein gewisses Maß an E-Kompetenzen haben müssen, um ihren Aufgaben im Sinne der Aufgabenerfüllung ihrer Einrichtung nachgehen zu können.

Die oben genannten identifizierten Rollen wurden zusätzlich in Form von „Steckbriefen“, in denen ihre Aufgaben, Verantwortlichkeiten und Kompetenzen beschrieben sind, dokumentiert. Diese Steckbriefe ermöglichen eine strukturierte Darstellung und auf allen Ebenen vergleichbare Beschreibung der Kompetenzen. Im jeweiligen Steckbrief werden Aufgaben und Verantwortlichkeiten kurz dargestellt und die benötigten Kompetenzen kategorisiert. Der Aufbau eines solchen Steckbriefs inklusive einer beispielhaften Andeutung von möglichen Ausprägungen der Kategorien ist in Abb. 2 wiedergegeben. Die Kompetenzen sind dabei in vier weitere Kategorien unterteilt: Technische, fachliche, soziale Kompetenzen und Persönlichkeitsmerkmale. Im Folgenden wird kurz auf die Charakteristika der einzelnen Kompetenzbereiche eingegangen:

Technische Kompetenzen bezeichnen Kenntnisse der IT oder Kenntnisse in der Planung und Gestaltung der IT. Diese Kenntnisse reichen von allgemeinen IT-Kenntnissen bis zu tiefergehenden Programmierkenntnissen.

Fachliche Kompetenzen unterteilen sich in sozio-technische, die Organisation betreffende, Management- und politisch-administrative Kompetenzen.

#### **Steckbriefnummer: Rollename**

*fortlaufende Steckbriefnummer und eindeutiger Rollename, z. B. Nr. 1: Organisations- / Changemanager*

#### **Zuordnung der Rolle zu einer Oberkategorie (Gestalter, Koordinator, Dienstleistungen, Fachaufgabenträger)**

#### **Beschreibung der Rolle**

*Kurze allgemeine Beschreibung mit Zusammenfassung der wichtigsten Aufgaben und Verantwortlichkeiten*

#### **Aufgaben und Verantwortlichkeiten**

*Stichpunktartige Vorstellung der Aufgaben und Verantwortlichkeiten*

#### **Kompetenzen**

*Detaillierte Beschreibung der Kompetenzen*

#### **Technische Kompetenzen (z. B. Kenntnisse der IT oder Planung/Gestaltung von IT, u. a. allgemeine IT-Kenntnisse, Programmierkenntnisse)**

##### **1. Fachliche Kompetenzen**

- a. Sozio-technische Kompetenzen (z. B. Kenntnisse der Auswirkungen/Akzeptanz von E-Government)
- b. Die Organisation betreffende Kompetenzen (z. B. Prozessmanagement, Organisationsgestaltung)
- c. Managementkompetenzen (z. B. Changemanagement)
- d. Politisch-administrative Kompetenzen (z. B. rechtliche Rahmenbedingungen, administrative Abläufe)

##### **2. Soziale Kompetenzen (z. B. Führungs- und Kommunikationskompetenz)**

##### **3. Persönlichkeitsmerkmale (z. B. Kreativität, Selbstmanagement)**

**Abb. 2** Aufbau eines Steckbriefs

Als soziale Kompetenzen werden Kompetenzen im Umgang mit anderen Menschen, z. B. Beschäftigten oder Bürger\*innen, bezeichnet. Beispiele hierfür sind Führungs-, Kommunikations- und Konfliktmanagement-Kompetenzen oder Verhandlungsgeschick.

Persönlichkeitsmerkmale wurden explizit mitaufgenommen, um in Stellenbeschreibungen häufig erwähnte gewünschte Charakteristika oder Verhaltensweisen einer Person zu benennen. Diese Persönlichkeitsmerkmale trägt eine Person in sich bzw. nimmt diese ein, ohne sie explizit, d. h. in Form von Schulungen etc., erlernt zu haben.

Die in den jeweiligen Rollensteckbriefen identifizierten Kompetenzen werden nicht bei jeder Rolle in der gleichen Tiefe benötigt. So mag es bei einer bestimmten Rolle ausreichen, nur theoretisches Wissen in einer Kategorie zu besitzen, wohingegen es in einer anderen Rolle zwingend notwendig sein kann, dieses Wissen auch zur praktischen Anwendung zu bringen bzw. mit diesem Wissen Sachverhalte zu hinterfragen oder weiterzuentwickeln. Da sowohl die Steckbriefe als auch die Kompetenzen konkret auf die jeweiligen Aufgabenbereiche zugeschnitten sein sollten, hat sich eine Matrix als geeignete Darstellungsform herauskristallisiert, in der die Gesamtheit an Kompetenzen zu unterschiedlichen Beherrschungsniveaus in Bezug gesetzt werden kann. Dabei werden die drei folgenden Kompetenzniveaus herausgestellt:

Wissen: Kenntnisse werden erworben und verstanden, jedoch nicht angewendet. Sie liegen passiv vor, wobei ein Transfer auf andere Anwendungskontexte nicht erforderlich ist. Beispielsweise ist jemand in der Lage, ein Prozessmodell zu lesen, ohne die konkrete Modellierungsmethode selbst nutzen oder anwenden zu können.

Anwenden: Neben dem theoretischen Wissen über einen spezifischen Bereich kann das Wissen in neuen Kontexten zur Anwendung kommen. Jemand ist nicht nur in der Lage, beispielsweise ein Prozessmodell zu lesen, sondern kann die Modellierungsmethode selbst anwenden und Prozessmodelle erstellen.

Gestalten: Wissen und Anwenden als Vorstufen sind die Voraussetzung für dieses Niveau. Denn hier muss darüber hinaus die analytische Fähigkeit, Probleme zu erkennen, als auch die Fähigkeit, Lösungen zu erarbeiten und umzusetzen, eingesetzt werden. Jemand ist nicht nur in der Lage, Prozessmodelle zu lesen bzw. selbst zu erstellen, sondern kann die Modelle interpretieren, Schwachstellen und Handlungsempfehlungen über einzelne Modelle hinweg analysieren, zusammentragen und organisatorische Abläufe auf dieser Basis (neu) gestalten.

Die Matrix enthält jeweils Rollennamen sowie alle zuvor identifizierten Kompetenzen, die der Beschreibung in den Rollensteckbriefen folgend dargestellt werden. Zusätzlich helfen entsprechende Kennzeichnungen bei der weiteren Spezifizierung der Kompetenzen.

Die Aufteilung in die unterschiedlichen Kompetenzstufen kommt für die Persönlichkeitsmerkmale nicht in Frage, da diese Eigenschaften entweder vorhanden sein müssen oder nicht. So kann es sein, dass eine bestimmte Rolle ein hohes Maß an Eigeninitiative voraussetzt. Die Person, die jene Rolle verkörpert, hat diese Fähigkeit automatisch in allen Kompetenzstufen und kann sie nicht „ausschalten“, wenn es z. B. um das Anwenden oder Gestalten geht. Auch wenn soziale Kompetenzen

gelehrt und gelernt werden können, wurde aus vergleichbaren Gründen auf eine Beschreibung von Kompetenzstufen verzichtet. Das Raster „verstehen – anwenden – gestalten“ lässt sich nicht in gleicher Weise wie bei technischen oder fachlichen Kompetenzen anwenden, die Kompetenzmatrix eignet sich daher nur für die technischen und fachlichen Kompetenzen. Bei den sozialen Kompetenzen und Persönlichkeitsmerkmalen kann an dieser Stelle nur gekennzeichnet werden, ob eine Rolle eine soziale Kompetenz oder ein Persönlichkeitsmerkmal in ihrer Ausführung benötigt oder nicht.

Die Steckbriefe zeigen das Potpourri an benötigten Kompetenzen auf und gehen vor allem bei den technischen bzw. IT-Kompetenzen etwas mehr in die Tiefe. Durch die weiterführenden Beschreibungen können diese genauer an den jeweiligen Bedarf angepasst werden. Diese ganzheitliche Übersicht der Steckbriefe kann nun für neue Stellenausschreibungen oder als Orientierungshilfe für Arbeitsplatzbeschreibungen verwendet werden. Die Kompetenzmatrizen im Gegenzug vermitteln ein konkreteres Bild über die benötigte Kompetenztiefe, die vorhanden sein sollte bzw. muss. Ferner zeigen sie wünschenswerte weiterführende Kompetenzen im Unterschied zu den zwingend nötigen Kompetenzen auf.

Diese Werkzeuge richten sich primär an Sachbearbeiter\*innen im Personalfachbereich, aber können natürlich auch von Führungskräften in Fach- oder IT-Bereichen genutzt werden:

1. Die Bausteine der Rollensteckbriefe können eingesetzt werden, um bei bestehendem Personal die Fortbildungsbedarfe zu eruieren und ggf. Fortbildungen zu planen. Ein Abgleich des Soll-/Ist-Zustands wird durch den strukturierten Aufbau der Steckbriefe vereinfacht.
2. Die Matrizen helfen dabei, für neu zu generierende Stellen die jeweiligen Kompetenztiefen zu bestimmen, indem mit der Fachabteilung die einzeln aufgeführten Kompetenzen besprochen und zunächst nach „notwendig/wünschenswert“ eingruppiert werden, um dann in einem zweiten Schritt das Kompetenzniveau festzulegen.
3. Sowohl Rollensteckbriefe als auch Matrizen helfen dabei, mögliche Kompetenzprofile mit der jeweiligen Fachabteilung durchzusprechen und im weiteren Verlauf neue Stellenausschreibungen zu generieren.

Mit diesen zwei Werkzeugen können die folgenden Ziele unterstützt werden:

*Eindeutige Abgrenzung und Vergleichbarkeit:* Rollenbeschreibungen können untereinander eindeutig abgegrenzt und so miteinander verglichen werden. Führungskräfte können die Steckbriefe dazu nutzen, um abzugleichen, welche Rollen und Kompetenzen in ihrem Bereich vorhanden sind und so einen möglichen (Schulungs-)Bedarf besser abschätzen. Es kann auf Basis der Rollensteckbriefe und Kompetenzprofile bewertet werden, welche Kompetenzen benötigt werden und welche Kompetenzen vorhanden sind. Auf dieser Basis kann dann entschieden werden, ob fehlende Kompetenzen durch Fort- und Weiterbildung erworben oder durch Beauftragung von externen Dienstleistern gewonnen werden sollten.

*Standardisierung:* Die einheitliche Verwendung von Kategorien und Kompetenzen könnte den Koordinations-, Abstimmungs- und Kommunikationsaufwand bei der Stellenbeschreibung und letztendlich auch der Stellenbewertung reduzieren. Bisher gibt es in dieser Hinsicht immer wieder Konflikte zwischen den Personal- und Fachbereichen.

*Grundlage für Schulungen/Qualifizierung:* Anhand der modularisierten Anforderungen an eine Rolle kann der Qualifizierungs- und Schulungsbedarf einfacher ermittelt und mit dem Angebot des Bildungsträgers abgeglichen werden.

---

## 5 Umsetzungsstand und Auswirkungen

Mit den vorgestellten Werkzeugen *Rollensteckbrief* und *Kompetenzmatrix* kann die Personalentwicklung öffentlicher Verwaltungen in den Stufen *Personalgewinnung* und *Personalentwicklung* unterstützt werden. Die gezielte Beschreibung der benötigten Kompetenzen sowie die strukturierte Definition von zu erwerbenden Kompetenzen lassen sich mit den Steckbriefen und Matrizen abbilden. Der in der öffentlichen Verwaltung bestehende Handlungsbedarf hierfür ist durch die zunehmenden und sich ständig fortentwickelnden IT-Anforderungen dringender denn je. Vordringliches Ziel aus Sicht der Autor\*innen ist es zunächst, das Thema *E-Kompetenzmanagement* in der Verwaltung zu verankern. Personalmanagement und Personalentwicklung müssen sich den neuen Kompetenzanforderungen widmen und sie zum elementaren Bestandteil der eigenen Arbeit machen. Erste Evaluationen des Konzepts wurden unmittelbar nach Entwicklung der Werkzeuge durchgeführt (Zimmerling et al. 2017). In einzelnen Bundesländern lassen sich erste Maßnahmen beobachten, die das Themenfeld aufgreifen. So hat sich konkret ein Bundesland zum Ziel gesetzt, bis Ende des Jahres 2019 für den eigenen Bereich IT-orientierte Rollen anhand der hier vorgestellten Referenzrollen zu definieren und landesweit einheitlich in den IT-Grundsätzen zu verankern. Dies wird verschiedene Implikationen haben. So werden der Sprachgebrauch und das Verständnis der künftigen Rollen vereinheitlicht und Gleches wird gleich bezeichnet werden. Die Bemessung der Rollen und damit verbundenen Stellenanteile wird so harmonisiert werden. Ebenso hat sich das Bundesland zum Ziel gesetzt, im Anschluss an die Vereinheitlichung der Rollenprofile das landeseigene Weiterbildungs- und Schulungsangebot auf die neuen Profile anzupassen. Auch wenn sich erste konkrete Initiativen wie diese formieren, so muss doch konstatiert werden, dass der Bedarf für ein einheitliches Verständnis IT-orientierter Rollendefinitionen und entsprechender (Weiter-)Bildungsbedarfe zwar erkannt ist und diskutiert wird, die Umsetzung entsprechender Maßnahmen aber noch in den Anfängen ist.

---

## 6 Ausblick/Perspektiven

Verbunden mit der Erkenntnis, dass E-Kompetenzen in der öffentlichen Verwaltung ausgebildet und erworben werden müssen, ergeben sich verschiedene Herausforderungen, die es zu adressieren gilt (vgl. u. a. auch Räckers et al. (2017)):

*Entwicklung einer E-Kompetenz-Strategie:* Wie bereits angedeutet, muss das Management der E-Kompetenzen in den Verwaltungen fest verankert werden. IT-/E-Government-Bildungsmaßnahmen müssen von Führungskräften aus „nicht-technischen“ Bereichen ebenso als fachlich und strategisch relevant angesehen werden. Dies ist verbunden mit der Definition der Personalentwicklung im Sinne von E-Kompetenzen als strategische Führungsaufgabe. Die Führungskräfte müssen sich dies bewusst machen. Für die Verwaltungen als Ganzes sollten die hiermit verbundenen Maßnahmen in die strategischen Überlegungen der Organisationsentwicklung einbezogen werden.

Hiermit verbunden ist die Voraussetzung, dass auch und im besonderen Maße die Führungskräfte in der öffentlichen Verwaltung bereit sind, die Weiterentwicklung des eigenen Personals im Bereich der E-Kompetenzen anzuerkennen und zu fördern. Die Beschäftigten müssen Schulungsangebote nutzen dürfen, entsprechende Fort- und Weiterbildungen müssen honoriert werden. Hier gilt es, die Führungskräfte zu sensibilisieren, dass eine solche Fort- oder Weiterbildungsmaßnahme einen langfristigen Nutzen für den Bereich hat. Bei der Gewinnung neuen Personals ist ebenso darauf zu achten, dass die relevanten und nötigen E-Kompetenzen in den Ausschreibungen und Arbeitsplatzbeschreibungen berücksichtigt werden und bei der Auswahl des Personals beachtet werden oder unmittelbar auf eine Einstellung entsprechende Qualifizierungsmaßnahmen folgen.

*Ableitung bzw. Schaffung von adäquaten Angeboten:* Die weitere Ausdifferenzierung der Rollen mit E-Kompetenzen macht deutlich, dass die bisherigen Angebote, insbesondere für die Ausbildung im Bereich Organisationsgestaltung mit IT, nicht ausreichend sind. Die Angebote der Bildungsanbieter müssen daher weiterentwickelt und ausgeweitet werden. Es muss deutlich werden, dass die Angebote über eine reine Vermittlung von IT-Basiskompetenzen hinausgehen muss. Die Nutzung und die Gestaltung einer digitalisierten Organisation bedingt deutlich weitergehende Fähigkeiten, exemplarisch seien Projekt-, Architektur- oder Prozessmanagementfähigkeiten genannt, die es aktuellen und zukünftigen Führungskräften zu vermitteln gilt. Dies sollte bei der künftigen Entwicklung der Aus-, Fort- und Weiterbildung in diesem Bereich beachtet werden. Auch hier zeichnen sich erste Maßnahmen, u. a. unter erneuter Förderung des IT-Planungsrats ab und sollen in den Jahren 2020/2021 erste, konkrete Angebote liefern.

Allein mit klassischen, auf Präsenzseminaren und Literaturstudium basierenden Aus- oder Fortbildungsveranstaltungen können schon rein kapazitätsmäßig nur Teile des Personals erreicht werden (Skalierungsproblem). Darüber hinaus gewinnt das Lernen im unmittelbaren Arbeitsumfeld, z. B. in Form einer In-House-Schulung oder direkt am Arbeitsplatz, an Stellenwert, um die aufgabenkonkrete Anwendung des Gelernten sicherzustellen (Transferproblem). Schließlich ist die Ausdifferenzierung der Lernenden, z. B. aufgrund des Vorwissens, der gewünschten Kompetenztiefe oder der zur Verfügung stehenden Zeit, zu berücksichtigen (Bedarfsproblem).

*Bündelung bzw. Koordinierung der Angebote:* Den Rahmen für all dies kann eine Lern- und Wissensplattform bieten, die von allen Bildungsanbieter\*innen und -nachfrager\*innen, Praktiker\*innen und Fachexpert\*innen aus dem öffentlichen Sektor Deutschlands genutzt werden kann. Damit kann dem Fokus auf Fachsilos, dem auf

die eigene Organisation beschränktem Denken und mangelnden Modernisierungserfahrungen in einzelnen Behörden und Einrichtungen entgegengewirkt werden. Insbesondere Inhalte, die für die derzeitige Modernisierung von Staat und Verwaltung wichtig und über eine mittlere Zeitspanne gleichbleibend sind, dazu zählen u. a. IT-Grundlagen, elektronische Vorgangsbearbeitung und Aktenführung, Informationssicherheit, Prozessmanagement, Projektmanagement sowie Kommunikations- und Methodenkompetenz, könnten so auf breiter Front angeboten werden.

*Kontinuierliche Evaluation und Weiterentwicklung:* Kaum ein Handlungsfeld entwickelt sich so rasant und dynamisch wie das der Digitalisierung bzw. der digitalen Transformation. Durch den Wandel der Lebens- und Arbeitswelt verändern sich auch die Anforderungen regelmäßig und schnell. Daher müssen die Steckbriefe und Kompetenzmatrizen bzw. die damit verbundenen Rollenprofile im aktiven Einsatz kontinuierlich evaluiert und weiterentwickelt werden, sich an wandelnde Schwerpunkte und Bedürfnisse anpassen. Die Erwartung kann also nicht sein, den aktuell gegebenen Stand an Struktur als finales Ergebnis zu nehmen, sondern als Vorlage im Wandel.

*Bereitschaft zur Annahme von „Bottom-Up-Innovationen“ schaffen:* Bei der Fokussierung auf die Vermittlung von E-Kompetenzen sollte nicht vergessen werden, dass die Bediensteten auch aus ihrem Privatleben bzw. täglichen Leben immer mehr verschiedene E-Kompetenzen mitbringen. Im Zuge der zunehmenden Digitalisierung sind wir mehr und mehr vertraut mit Technologien, die speziell für den Endkund\*innenmarkt entwickelt wurden, und nutzen diese zu jeder Zeit. Auf der einen Seite wird in den Basiskompetenzen so die Kompetenzlücke geringer, da die Kompetenzen und das Verständnis für die Nutzung von digitalen Technologien im Alltag erworben werden, auf der anderen Seite aber wächst auch die Erwartung dieser Beschäftigten, dass sie vergleichbare (Arbeits-)Bedingungen am Arbeitsplatz vorfinden. Dies bedeutet in der zukünftigen Entwicklung, dass sich die Grundeinstellung zur Veränderungsfähigkeit und Veränderungsbereitschaft der öffentlichen Organisationen wandeln und öffnen muss.

Gerade der letztgenannte Aspekt führt zu einer dritten Säule im Personalmanagement, die für die öffentliche Hand, besonders im Bereich von IT-Fachkräften, von erheblicher Bedeutung ist. Die *Bindung von geeignetem Personal* stellt in Zeiten des Fachkräftemangels allerorts eine große Herausforderung dar. Neben finanziellen Anreizen, die durch Tarifverträge und Laufbahnverordnungen eingegrenzt werden, spielen andere Faktoren der Mitarbeiter\*innenbindung eine große Rolle. Die Verwaltungen stehen im harten Wettbewerb mit der Privatwirtschaft um die besten IT-Talente. Hier gilt es, sich selbst ins „rechte Licht“ zu rücken, sowohl bei den künftigen Beschäftigten, aber auch und vor allem bei den aktuell Beschäftigten.

Um Image, Werte oder Normen überhaupt nach außen zu transportieren, darf der Schritt der eigentlichen Entwicklung und Gestaltung, ergo der Identitätsbildung, nicht vernachlässigt werden. Die Schaffung einer Identität, einer gelebten und damit greifbaren Organisationskultur hat jedoch nicht nur eine Wirkung nach außen: Identifiziert sich der Personalstamm mit den definierten und gelebten Werten, erhöhen sich die Zufriedenheit, die Motivation und Loyalität. Je höher die Identifikation und die Bindung zum Arbeitgeber, auch und gerade über eher weiche Faktoren wie

der viel zitierten Work-Life-Balance oder weiteren Faktoren ist, desto weniger besteht bei den Beschäftigten die Bereitschaft, die Organisation kurzfristig zu verlassen. Beispielsweise die Entwicklung einer Arbeitgebermarke (sog. *Employer Branding*) kann hierbei helfen.

---

## Literatur

- Becker, Jörg, Vanessa Greger, Oliver Heger, Katharina Jahn, Helmut Kremer, Heidrun Müller, Björn Niehaves, Nadine Ogonek, Michael Räckers, Tino Schuppan, und Robert Zepic. 2016. *E-Government-Kompetenz*. Studie im Auftrag des IT-Planungsrats. Berlin: Nationales E-Government Kompetenzzentrum e.V.
- Goldacker, Gabriele. 2017. *Digitale Souveränität*. Berlin: Kompetenzzentrum Öffentliche IT/Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS.
- Gräf, Eike, Henning Lahmann, und Philipp Otto. 2018. *Die Stärkung der digitalen Souveränität. Wege der Annäherung an ein Ideal im Wandel*. Diskussionspapier von iRights.Lab und DIVSI. Berlin/Hamburg: iRights.Lab/DIVSI.
- Hill, Hermann. 2011. E-Kompetenzen. In *Handbuch zur Verwaltungsreform*, Hrsg. Bernhard Blanke, Frank Nullmeier, Christoph Reichard und Göttrik Wewer, 4., Ak. u. erg. Aufl., 385–392. Wiesbaden: VS.
- Räckers, Michael, Astrid Nelke, und Steffen Gilge. 2017. *E-Kompetenz im öffentlichen Sektor. Eine Positionsbestimmung*. Ergebnisse des Workshops „E-Kompetenz in der Aus- und Fortbildung“. Berlin: Gesellschaft für Informatik/Nationales E-Government-Kompetenzzentrum (NEGZ).
- Schuppan, Tino. 2009. Kompetenzen für vernetztes E-Government. *eGov Präsenz* 9(1): 62–65.
- Schuppan, Tino, Hunnius, Sirkо, und Paulowitzsch, Benedikt. 2014. *Aktuelle Ausprägung sowie Gestaltungsmöglichkeiten der E-Government-Aus- und Fortbildung von Fach- und Führungskräften der Verwaltung*. Studie im Auftrag des IT-Planungsrats. Potsdam: IfG.CC. The Institute for eGovernment.
- Zimmerling, Emanuel, Steffen Gilge, Eric, Schoop, und Michael Breidung. 2017. Transformationsbedarf in der öffentlichen Verwaltung. Kompetenzorientiert den demografischen Wandel gestalten. In *Tagungsband der 9. Konferenz Professionelles Wissensmanagement (Professional Knowledge Management), Karlsruhe, Germany, April 5–7, 2017. CEUR Workshop Proceedings 1821*, Hrsg. York Sure-Vetter, Stefan Zander und Andreas Harth, 186–197. Aachen: CEUR Workshop Proceedings (CEUR-WS.org).



---

# Folgen der Digitalisierung auf öffentliche Dienstleistungen

Matthias Döring und Stephan Löbel

## Inhalt

1 Klärung der Begriffe .....	624
2 Konzeptionelle Grundlagen .....	624
3 Praktische Einsatzfelder .....	626
4 Verbreitungsgrad und Auswirkungen .....	627
5 Perspektiven für Staat und Verwaltung .....	629
Literatur .....	630

---

## Zusammenfassung

Die Digitalisierung von Dienstleistungen ist ein erklärtes Ziel von Politik und Verwaltung. Neben der Hebung von Effizienzpotenzialen und einer beschleunigten Leistungserbringung soll sie auch Lösungsansätze für Probleme in ländlichen Räumen liefern. Die Effekte fallen jedoch durchaus ambivalent aus. Die Standardisierung von Verwaltungsprozessen im Zuge der Digitalisierung kann zu vergleichbaren Entscheidungen und damit zu mehr Gerechtigkeit führen, Fehler minimieren, aber auch Diskriminierung verfestigen, Kontextinformationen vernachlässigen und das Ermessen der Mitarbeiter\*innen unnötig einschränken. Eine Standardisierung von Interaktionen kann von Routinefällen entlasten und Freiraum schaffen für die komplizierten Prüffälle. Die Effekte der Digitalisierung sind umso vielschichtiger, je näher man der unmittelbaren Interaktionsebene zwischen Verwaltung und Bürger\*innen kommt. Besondere Herausforderungen müssen die Mitarbeiter\*innen bewältigen, die in direktem Kund\*innenkontakt

---

M. Döring (✉)

Department of Political Science and Public Management, University of Southern Denmark,  
Odense, Dänemark

E-Mail: [mdoering@sam.sdu.dk](mailto:mdoering@sam.sdu.dk)

S. Löbel

SHI Stein-Hardenberg Institut GmbH, Berlin, Dänemark  
E-Mail: [loebel@shi-institut.de](mailto:loebel@shi-institut.de)

stehen. Digitalisierung verändert sowohl die Interaktionsprozesse mit den Verwaltungskund\*innen als auch die anschließende Bearbeitung von Anträgen.

---

### Schlüsselwörter

Interaktion mit Kunden · Street-level bureaucrats · Vorgangsbearbeitungssysteme · Curtailment-Theorie · Enablement-Theorie

---

## 1 Klärung der Begriffe

Ein erheblicher Teil der öffentlichen Leistungserbringung ist durch den interaktiven Charakter von Dienstleistungen geprägt. Unterrichtende Lehrer\*innen, beratende Sozialarbeiter\*innen, Mitarbeiter\*innen in Ämtern und Behörden, die Anträge gewähren oder ablehnen, all diese Leistungen sind ohne Interaktion mit den Kund\*innen bzw. Klient\*innen schwer vorstellbar. Dabei wird die Dienstleistung nicht nur durch den Verwaltungsmitarbeiter\*innen geprägt, sondern auch durch die Kund\*innen selbst. Erkenntnisse der Organisationsforschung verdeutlichen, dass die menschliche Komponente bei Dienstleistungen eine zentrale Rolle einnimmt. Gerade bei komplexeren Dienstleistungen oder Problemen ist die Gefahr von Überforderung und Unzufriedenheit bei fehlender Interaktion mit den Mitarbeiter\*innen besonders hoch.

Auf Seiten der Verwaltung finden diese Interaktionen durch sogenannte *street-level bureaucrats* (SLB) statt. So wird eine Gruppe von Mitarbeiter\*innen in Verwaltungen bezeichnet, die direkten Klient\*innenkontakt haben sowie über einen gewissen Entscheidungsspielraum bei der Erbringung der Dienstleistung verfügen (Lipsky 2010). Sie sind nicht nur die eigentlichen Erbringer\*innen öffentlicher Dienstleistungen, sondern auch die Instanzen der *Verwirklichung von Politik*.

---

## 2 Konzeptionelle Grundlagen

Die Digitalisierung der Verwaltungsarbeit kann sich auf zwei Phasen ihrer Leistungserbringung auswirken: Erstens kann sich die Natur der Interaktion mit den „Kund\*innen“ grundlegend verändern, wenn beispielsweise persönlicher Kontakt durch digitale Plattformen oder aber Intermediäre ersetzt wird. Zweitens kann sich die Arbeitsweise der *street-level bureaucrats* durch die Einführung von E-Akten und Vorgangsbearbeitungssystemen verändern – mit eher ambivalenten Effekten.

Durch die Einführung elektronischer Hilfsmittel erhoffen sich Verwaltungen, die Geschwindigkeit und Effizienz ihrer Arbeit zu erhöhen und Fehlerraten zu senken. Der Abbau von Medienbrüchen, der Verzicht auf Papierakten, die aufwendig zu transportieren und zu archivieren sind, sowie die Verknüpfung mit anderen Fachanwendungen sind ebenso wie eine höhere Transparenz der Entscheidungen Argumente für die Optimierung von Prozessen innerhalb der Verwaltung. Gleichzeitig führen solche Systeme häufig zu einer stärkeren Standardisierung von Verwaltungsprozessen. Diese Standardisierung kann jedoch nicht nur für die Bürger\*innen ein

zweischneidiges Schwert werden: Welche Effekte die Einführung von *E-Government*-Instrumenten auf die Arbeitsweise von Mitarbeiter\*innen hat, die unmittelbare Bürger\*innenkontakte haben, ist nicht abschließend geklärt (Buffat 2014). Zwei grundlegende Thesen werden derzeit diskutiert: die *Curtailment*-These und die *Enablement*-These.

Die *Curtailment*-These geht davon aus, dass die zunehmende Strukturierung der Arbeitsprozesse durch technische Systeme die Entscheidungsspielräume der Mitarbeiter\*innen verringert. Standardisierte Eingabeformulare mit Prüfalgorithmen sowie klar definierten Sequenzen von Arbeitsschritten schränken die Flexibilität in einzelnen Verfahren ein. Informelle Absprachen und Kompromisse werden hierdurch häufig systematisch erschwert. Dies kann einerseits vorteilhaft sein, da der Gleichheitsgrundsatz der öffentlichen Verwaltung gestärkt wird. Andererseits können gerade solche Entscheidungsspielräume und informelle Übereinkünfte die Effizienz und Legitimität von Verfahren erhöhen – und nicht selten die Akzeptanz einer ganzen Organisation sicherstellen.

Auch für die unmittelbare Interaktion mit den Klienten der Verwaltung kann die operative Digitalisierung weitreichende Folgen haben. Die Bürger\*innen sollen ihre Behördengänge möglichst „vom Sofa aus“ erledigen können, ohne in den jeweiligen Ämtern vorstellig werden zu müssen. Der offensichtliche Vorteil aus ihrer Sicht sind hierbei die sinkenden Transaktionskosten. Ein solches Prozedere setzt jedoch ein entsprechendes Angebot der Behörden sowie eine intuitive Führung durch dieses Angebot voraus, damit die passenden Formulare, Informationen sowie Rahmenregelungen rasch gefunden werden können. Da das nicht immer gegeben ist, müssen Verwaltungskund\*innen ein gewisses Kompetenzniveau bei der Suche mitbringen. Ist eine Dienstleistung vollständig elektronisch abbildbar, kommt es zu keiner unmittelbaren Kommunikation zwischen beiden Seiten mehr, die Verwaltung wird weniger spürbar. Im Falle von reinen Routineätigkeiten wie etwa der Aktualisierung von Anschriften ist dies denkbar unproblematisch. Die meisten Interaktionen sind jedoch weniger eindeutig, sondern erfordern häufig Entscheidungen, bei denen ein Ermessen ausgeübt werden kann. Die zunehmende Anonymisierung durch die Digitalisierung kann dabei unterschiedliche Effekte haben: Einerseits kann sie Antragsteller vor expliziter und impliziter Diskriminierung schützen, da nicht selten kulturelle und sozio-demografische Faktoren die Entscheidungen von Mitarbeiter\*innen der Verwaltung beeinflussen, die nicht immer sichtbar werden (Hemker und Rink 2017). Andererseits haben Antragsteller in einem rein digitalen Kanal nur geringe Möglichkeiten für Nachfragen, Erläuterungen und Hinweisen auf Besonderheiten ihres individuellen Falls.

Ein unpersönlicher Kontakt erschwert zudem das Sammeln von Kontextinformationen, die die Abwägung normalerweise beeinflussen. Dass solche Entscheidungen nicht ausschließlich auf Aktenlage basieren, kann ebenfalls als ambivalent gedeutet werden: Zusätzliche Informationen, gerade wenn sie nur auf verbaler Kommunikation beruhen, können einerseits eine strikte Umsetzung von geltendem Recht einschränken, ohne dass dies immer den Akten zu entnehmen ist. Fehlendes Kontextwissen erschwert es andererseits den Bearbeiter\*innen von Anträgen, Empathie aufzubauen, was zu Entscheidungen führen kann, die als unverständlich wahrgenommen werden.

nommen werden. Die Zufriedenheit mit einer staatlichen oder kommunalen Dienstleistung hängt nicht nur vom Ergebnis ab, sondern in besonderem Maße auch von der zwischenmenschlichen Interaktion mit den Mitarbeiter\*innen der Verwaltung. Bei vollständig digitalisierten Verfahren kommen diese Aspekte, die häufig durch kommunikative Signale vermittelt werden, nicht mehr zum Tragen.

Die *Enablement*-These widerspricht dem unterstellten Determinismus, dass Technik die Rolle des Menschen verdrängt und die Interaktion mit den Klienten marginalisiert. Durch die Standardisierung würde lediglich Routinearbeit automatisiert, was die Mitarbeiter\*innen in den Behörden entlaste. Dadurch könnten Ressourcen für prüfintensivere Fälle eingesetzt werden. Als positives Beispiel dienen Finanzämter, die zunehmend Routinefälle automatisiert abwickeln und nur noch prüfintensive Fälle persönlich kontrollieren. Die Mitarbeiter\*innen könnten dennoch eine *ultima ratio* sicherstellen, wenn sie mit ihrem Kontextwissen Vorentscheidungen von automatisierten Systemen kritisch überprüfen und korrigieren. Gleichzeitig könnten computergestützte Entscheidungen die Legitimation des Verwaltungshandelns erhöhen, was zu größerer Akzeptanz führen dürfte.

Durch die größere Transparenz, die mit einer digitalisierten Abbildung von Arbeitsprozessen einhergehen kann, können Kolleg\*innen und die Führungskräfte Arbeitsschritte genauer nachvollziehen. Bei paralleler Bearbeitung von Fällen durch mehrere Mitarbeiter\*innen sind Entscheidungen für andere unmittelbarer nachvollziehbar. Prüfalgorithmen können widersprüchliche Daten leichter offenlegen, was wiederum das Verhalten der Bearbeiter\*innen beeinflusst. Eine gesteigerte Fehlerempfindlichkeit kann zunächst von Vorteil sein und den Gleichheitsgrundsatz stärken. Wenn jedoch eine konstruktive Behördenkultur fehlt, kann diese Fokussierung allerdings auch dazu führen, dass vermehrt „Angstbescheide“ ausgestellt werden, in denen Spielräume ungenutzt bleiben, um das Risiko von Fehlern zu verringern.

Für beide Thesen lassen sich in der raren empirischen Forschung Belege finden. Welche These jedoch den Narrativ eines Digitalisierungsprojekts dominiert, scheint von einer Reihe von Faktoren abzuhängen, darunter der Einsatzbereich, die Bereitschaft der Belegschaft und deren professionelles Selbstbild.

---

### 3 Praktische Einsatzfelder

Die Annahme, dass es in naher Zukunft zu einer kompletten Automatisierung der Verwaltung kommen wird, ist wenig realistisch. Auch wenn in den letzten Jahren neue Möglichkeiten von IT-Potenzialen aufgekommen sind, die sich unter „neue Digitalisierung“ zusammenfassen lassen. Dazu zählen Entwicklungen im Bereich der Künstlichen Intelligenz oder erweiterte Datenauswertung im Zusammenhang von *Big Data*. Diese Entwicklungen werden gegenwärtig in Deutschland in Analogie zur Wirtschaft unter dem Begriff Verwaltung 4,0 diskutiert. Es geht um weitergehende Vernetzung, Sensorik, z. B. für die Steuerung öffentlicher Infrastrukturen, bis hin zu Vorstellungen eines voll automatisierten Verwaltungsaktes aufgrund umfassender Datenauswertung. Es ist davon auszugehen, dass menschliche Handlungsträger im Zusammenhang mit der Digitalisierung weiterhin erforderlich sind,

weil es vielfach um die Verarbeitung von zum Teil anspruchsvollem Wissen und komplexem Kontextwissen geht sowie um interaktionsintensive Prozesse zu den Bürger\*innen, wie auch innerhalb der Verwaltung. Das zeigen zum großen Teil auch Studien, die davon ausgehen, dass es zu einer Verschiebung und inhaltlichen tätigkeitsbezogenen Änderung bei Berufen kommt und weniger zu deren kompletten Abschaffung (Zika et al. 2018). Generell wird davon ausgegangen, dass Tätigkeiten mit Kontextwissen, analytischen Fähigkeiten oder häufiger Interaktion weniger für eine Automatisierung geeignet sind. Hinzukommt die Notwendigkeit der Interpretation von Daten, die weiterhin menschliches Tun erfordert, so dass auch bei Entscheidungen auf Datenbasis eine gänzliche Automatisierung weder machbar noch wünschenswert erscheint. So wurde mit der Einführung des § 35a VwVfG zwar explizit der voll automatisierte Verwaltungsakt erlaubt. Als Einschränkung führt der Gesetzgeber jedoch solche Prozesse auf, die Entscheidungsspielraum enthalten (Martini und Nink 2017). Diese Entscheidungen müssen also final durch Menschen getroffen werden.

Trotz dieser generellen Einschränkung sind der Phantasie der möglichen Einsatzfelder kaum Grenzen gesetzt. Neben Bereichen, die hierbei bereits erste gute Beispiele liefern wie die Steuerverwaltung, sind vollständig digitalisiert unterstützte Prozesse und Dienstleistungen auch im Bereich Ordnungsverwaltung (z. B. Kfz-An- und Ummeldung), Gewerbeverwaltung (z. B. Ausstellung von Gewerbescheinen) oder auch der Sozialverwaltung (z. B. Ausstellung von Wohngeldanträgen) denkbar. Für die Seite der Antragssteller wird hierbei eine intelligente und nutzerfreundliche Navigation durch diese Prozesse essenziell sein.

Um die Navigation durch ihre Dienstleistungen zu erleichtern, werden im Privatsektor zunehmend *Chatbots* eingesetzt. Auch im öffentlichen Kontext ist eine solche automatisierte Steuerung durch einfache Ja-Nein-Fragen vorstellbar. Zu nennen wären etwa die Prototypen für den „Botty Bonn“ und den „Kumpel Krefeld“, die sich aktuell in der Testphase befinden. Mit zunehmender Komplexität kann ein solches Verfahren jedoch schnell langwierig und unpräzise werden. Der Entpersonalisierung der Interaktionen könnte jedoch durch Echtzeitchats mit Mitarbeiter\*innen der Verwaltung vorgebeugt werden, die bei Fragen und Problemen unmittelbar auf die Klienten eingehen und Hinweise sowie Empfehlungen aussprechen. *Chats* können zwar nicht die nonverbale Kommunikation einer „echten“ Interaktion ersetzen, aber ein Gefühl der Hilflosigkeit verhindern, wenn Bürger\*innen überfordert sind. Derartige *Service-Chats* werden nicht nur in privaten Unternehmen genutzt, sondern teilweise auch schon im öffentlichen Sektor (die US-amerikanische Behörde zur Vergabe von Studentenkrediten – *Federal Student Aid* – nutzt dieses Instrument bereits seit Jahren).

---

## 4 Verbreitungsgrad und Auswirkungen

Während die deutsche Praxis und Forschung zur Wirkung solcher digitalisierten Dienstleistungen noch weitestgehend in den Kinderschuhen steckt, lassen sich international erste Erfahrungen und Analysen finden. Die Arbeitsweisen von Mitar-

beiter\*innen der Verwaltung mit Kundenkontakt und die Einführung von IT-Systemen beeinflussen sich dabei häufig wechselseitig. Bruhn und Ekström (2017) haben am Beispiel der schwedischen Vergabebehörde für Studienkredite aufgezeigt, dass die Einführung eines Systems zur strukturierten Begleitung von Anrufen im *front-office* die Art und Weise maßgeblich beeinflusst, wie dort gearbeitet wird. Die Arbeitsprozesse wurden in den vergangenen Jahren sukzessive hin zu mehr Standardisierung, Transparenz und Effizienz umgebaut. Dennoch blieben aber Spielräume bei Entscheidungen für rechtlich spezifische Einzelfälle erhalten. Der vermehrte Fokus auf Standardisierung, Monitoring und Entpersonalisierung von Dienstleistungen minimiert die emotionale Interaktion zwischen Mitarbeiter\*innen und Bürger\*innen. Ausnahmen werden von den Mitarbeiter\*innen nur gewährt, wenn die Klient\*innen in der Interaktion lösungsorientiert auftreten und eine entsprechende Bereitschaft signalisieren. Für Klient\*innen, denen diese Arbeitsmodi, die zugrunde liegenden Spielregeln und die erwarteten Verhaltensweisen nicht bekannt sind, stellt dies jedoch eine Hürde dar.

Auch beim Pilotprojekt einer schwedischen Kommune, die ihr Bürgerbüro durch ein umfassendes Onlineangebot ersetzen wollte, spielten Argumente der *Curtailment*-These eine Rolle (Jansson und Erlingsson 2014). Deutlich wurde auch in diesem Fall der Zwiespalt zwischen einer Einschränkung des Ermessens, um den Gleichheitsgrundsatz zu stärken, und der notwendigen Flexibilität der Entscheider\*innen, um dem Einzelfall gerecht zu werden. Der Rückgang von direkten Interaktionen beschnitt außerdem die Möglichkeiten der Mitarbeiter\*innen, als „Übersetzungsinstanz“ zwischen Politik und Bürger\*innen aktiv zu werden. Eine besondere Relevanz hat hier der „*digital divide*“: Bei einer Auslagerung des Verwaltungshandelns ins *Internet* benötigen Bürger\*innen nicht nur technische Kompetenzen, um sich im Dienstleistungsangebot zurechtzufinden und den Überfluss an Informationen zu bewältigen, sondern auch Wissen über die Strukturen der Verwaltung und über die Regeln, nach denen sie arbeitet. Um negative Effekte auffangen zu können, bedarf es daher bei Verwaltungsleistungen eines Multikanalansatzes.

Einen vermittelnden Ansatz verfolgt die norwegische Arbeits- und Wohlfahrtsbehörde (Hansen et al. 2018). Über viele Jahre wurde hier die *Homepage* als zentrale Informationsquelle aufgebaut und explizit beworben. Mit der Überarbeitung der *Homepage* und der elektronischen Abbildung einiger Dienstleistungen wurde diese Strategie weiter fortgesetzt. Einige Bevölkerungsgruppen haben ihre Interaktionen mit der Behörde zunehmend in den digitalen Raum verlagert und damit immer mehr den persönlichen Kontakt verringert. Die meisten jedoch kombinieren *Online*-Anträge mit *face-to-face*-Kontakten, weil sich komplexe individuelle Sachverhalte technisch häufig nicht angemessen abbilden lassen. Ein Wandel von der *street-level bureaucracy* hin zur *system-level bureaucracy*, also eine vollständige Verlagerung auf automatisierte Dienstleistungen, findet also nicht statt. Die Veränderungen sind tendenziell marginal, die klassische persönliche Interaktion wurde nicht durchweg ersetzt. Die zunehmende Standardisierung ermöglicht nicht nur neue Online-Dienstleistungen, sondern auch einen besseren Erfahrungsaustausch innerhalb der Behörde und eine Konzentration auf schwierigere Fälle, was der *Enablement*-These entspricht. Ein umfassender Zugriff auf Daten der Klienten aus öffentlichen Regis-

tern, der technisch möglich geworden ist, verringert die Fehleranfälligkeit und verbessert die Leistungen.

Gerade öffentliche Organisationen, deren Mitarbeiter\*innen durch ein professionsgetriebenes Selbstbild charakterisiert werden (z. B. Lehrer, Ärzte etc.), können ein sehr ambivalentes Verhältnis zur digitalen Unterstützung der Dienstleistungen entwickeln. Die Studie von Petrakaki et al. (2016) zum Verhältnis von Ärzt\*innen in britischen Krankenhäusern zu elektronischen Patientenakten zeigt den Konflikt der Curtailment-These zwischen professioneller Autonomie und Standardisierung auf. Jedoch zeigt sich auch in dieser Studie, dass es sich keineswegs um einen Determinismus handeln muss, dass die Einführung von Vorgangsbearbeitungssystemen zu einer Verschiebung von Entscheidungshoheit, Macht oder Verantwortung führen muss. Die Einbeziehung des Personals, deren professionelle Identität und Wandlungsbereitschaft spielen hierbei eine wichtige Rolle.

---

## 5 Perspektiven für Staat und Verwaltung

Auch wenn in einigen Fachkreisen die Vorstellung existieren mag, dass der öffentliche Sektor mit seinen Prozessen gut automatisierbar wäre, lassen heutige Studien kaum den Schluss zu, dass die zukünftige Verwaltung von menschlicher Tätigkeit entleert wird. Sicherlich heißt digitalisierte Arbeitsweise auch, den Umgang mit verringerten Entscheidungsspielräumen durch die zunehmende Strukturierung im Zuge der IT-Nutzung, die eingeschränkte Flexibilität in einzelnen Verfahren durch standardisierte Eingabeformulare mit Prüfalgorithmen sowie klar definierten Sequenzen von Arbeitsschritten und dadurch eher erschwerten informellen Absprachen und Kompromissen einzuüben. Um den digitalen Wandel zu bewältigen, müssen öffentliche Verwaltungen die dafür erforderlichen Kompetenzen (Fähigkeiten, Fertigkeiten und Wissen) aufbauen. Zukünftige Kundenberater\*innen, gerade in Kernverwaltungen, werden zunehmend die Rolle von Lotsen einnehmen, die Bürger\*innen bei ihren Anliegen und Anträgen unterstützen. Kommunikations- und Sozialkompetenzen werden im Qualifikationsprofil eine dominierende Rolle einnehmen. Der Gedanke einer *service-dominant logic*, wie sie im privaten Dienstleistungssektor seit Jahren vorherrscht, rückt somit auch im öffentlichen Sektor zunehmend in den Fokus. Gleichzeitig ist diese Zielgruppe bei Einführungsprozessen von Vorgangsbearbeitungssystemen besonders zu beachten. Nicht nur bringen diese Kundenbetreuer\*innen notwendige Expertise und die Alltagserfahrung mit, um Spezifikationen für etwaige Systeme zu formulieren. Sie können außerdem am besten Schwächen und Restriktionen benennen, die die tägliche Arbeit erschweren (oder erleichtern). Für die erfolgreiche Implementation entsprechender IT-Systeme ist ihre Rolle somit unerlässlich. Die Programme müssen hierbei den Spagat zwischen Standardisierung und Sicherung notwendiger Flexibilität bewältigen. Nicht zuletzt ist eine solche partizipative Einbindung in einem *Change-Prozess* auch akzeptanz- und motivationsfördernd.

Es ist daher essenziell, Digitalisierung als ganzheitlichen Veränderungsprozess einer Organisation zu verstehen, damit Verwaltungsmitarbeiter\*innen durch die

Standardisierung tatsächlich von ihrer Routinearbeit entlastet und dadurch Ressourcen für prüfintensivere Fälle frei werden. Mit ganzheitlichem Veränderungsprozess ist allerdings nicht nur die Einführung technischer Systeme gemeint. Diese müssen nämlich wiederum systematisch in die Prozessorganisation der Verwaltung eingebettet werden. Hierbei werden sich jedoch Routinen und Arbeitsweisen verändern (was durchaus gewollt und wünschenswert ist). Bei arbeitsplatznahen Untersuchungen, wie z. B. bei den *Service Centern* der einheitlichen Behördenrufnummer 115 oder auch der EAkte, ist vielfach aufgezeigt worden, dass in Praxisprojekten die bewusste Gestaltung der Arbeitsorganisation bisher kaum eingeplant wird bzw. kaum vorkommt. Allenfalls wird der Fokus auf Technikgestaltung und -akzeptanz gelegt. Das heißt, die Arbeitsorganisation wird in vielen Digitalisierungsprojekten zur unbestimmten Restgröße reduziert, die sich mehr oder weniger als Zufallsprodukt ergibt. Ein reiner Technikfokus stößt hierbei an seine Grenzen: Letztendlich sind gerade Dienstleistungen hochgradig von Menschen als sozialen Wesen charakterisiert. Dies gilt nicht nur für die Kundenorientierung, sondern auch für die ausführenden Mitarbeiter\*innen. Hier kann die Digitalisierung Probleme verursachen, die auf den ersten Blick leicht übersehen werden. Auftretende Widerstände sollten hierbei nicht als bloße „Technikintoleranz“ abgetan werden. Sie betrifft den Kern der Arbeit einer der wichtigsten Mitarbeiter\*innengruppen der öffentlichen Verwaltung. Bei der digitalen Abbildung und Unterstützung von Dienstleistungen sollte also bewusst eruiert werden, welche Konsequenzen eine digitale Dienstleistung ohne persönliche Interaktionen und ohne Entscheidungsspielräume hat. Sind tatsächlich alle Fälle standardisiert abbildbar? Könnte die Legitimität eines solchen Prozesses gefährdet sein? Haben alle relevanten Bevölkerungsgruppen die gleichen Möglichkeiten, eine solche Dienstleistung abzurufen? Sind diesen Fragen nicht eindeutig mit Ja zu beantworten, werden *street-level bureaucrats* weiterhin eine zentrale Rolle spielen. Die zuständigen Führungskräfte wären in diesen Fällen gut beraten, die Rolle dieser Akteursgruppe in solchen Prozessen zu würdigen und nicht in die „*curtailment-Falle*“ zu tappen.

Ob Spielräume bei Entscheidungen bestehen bleiben, verschoben oder sogar eingeschränkt werden, ist letztlich eine offene Frage. Schon die denkbare Einschränkung dieser Spielräume kann zu erheblichen Widerständen und zu Demotivation führen. Gerade in Berufsfeldern mit einem ausgeprägten professionellen Selbstverständnis sind Entscheidungsspielräume häufig identitätsstiftend.

---

## Literatur

- Bruhn, Anders, und Mats Ekström. 2017. Towards a multi-level approach on frontline interactions in the public sector. Institutional transformations and the dynamics of real-time interactions. *Social Policy and Administration* 51(1): 195–215.
- Buffat, Aurélien. 2014. Street-level bureaucracy and E-government. *Public Management Review* 17(1): 149–161.
- Hansen, Hans-Tore, Kjetil Lundberg, und Liv Johanne Syltevik. 2018. Digitalization, street-level bureaucracy and welfare users' experiences. *Social Policy and Administration* 52(1): 67–90.

- Hemker, Johannes, und Anselm Rink. 2017. Multiple dimensions of bureaucratic discrimination. Evidence from German welfare offices. *American Journal of Political Science* 61(4): 786–803.
- Jansson, Gabriella, und Gissur Ó. Erlingsson. 2014. More E-government, less street-level bureaucracy? On legitimacy and the human side of public administration. *Journal of Information Technology & Politics* 11(3): 291–308.
- Lipsky, Michael. 2010. *Street-level bureaucracy. dilemmas of the individual in public services. 30th anniversary expanded edition.* New York: Russell Sage Foundation.
- Martini, Mario, und David Nink. 2017. Wenn Maschinen entscheiden ... voll automatisierte Verwaltungsverfahren und der Persönlichkeitsschutz. *Neue Zeitschrift für Verwaltungsrecht – Extra* 36(10): 1–14.
- Petrakaki, Dimitra, Ela Klecun, und Tony Cornford. 2016. Changes in healthcare professional work afforded by technology. The introduction of a national electronic patient record in an english hospital. *Organization* 23(2): 206–226.
- Zika, Gerd, Robert Helmrich, Tobias Maier, Enzo Weber, und Marc I. Wollte. 2018. *Arbeitsmarkteffekte der Digitalisierung bis 2035. Regionale Branchenstruktur spielt eine wichtige Rolle.* IAB Kurzbericht. Aktuelle Analysen aus dem Institut für Arbeitsmarkt- und Berufsforschung. Nr. 9, 10.04.2018. Nürnberg: Institut für Arbeitsmarkt- und Berufsforschung. <http://doku.iab.de/kurzber/2018/kb0918.pdf>. Zugriffen am 18.03.2020.



---

# Standardisierter Datenaustausch

Matthias Döring und Sebastian Noack

## Inhalt

1 Begriffsbestimmung .....	634
2 Konzeptionelle Grundlagen .....	634
3 Praktische Einsatzfelder .....	635
4 Umsetzungsstand, Auswirkungen und Problemfelder .....	638
5 Perspektiven für Staat und Verwaltung .....	641
Literatur .....	642

---

## Zusammenfassung

Zur Erfüllung des *Once-only*-Prinzips zwischen Bürger\*innen und Verwaltung ist der reibungslose Austausch von Daten zwischen verschiedenen Behörden auf unterschiedlichen Ebenen unabdingbar. Die Interoperabilität der Daten spielt dabei eine zentrale Rolle. Mit zentralen Datenregistern und den sogenannten XÖV-Standards soll ein moderner digitaler Datenaustausch ermöglicht werden. Neben erfolgreichen Projekten gibt es dabei noch zahlreiche Probleme. Das Online-Zugangsgesetz von 2017, wonach alle Dienstleistungen von Bund, Ländern und Gemeinden bis 2022 auch elektronisch angeboten werden sollen, stellt einerseits einen potenziellen Treiber für die Digitalisierung in Deutschland dar, andererseits aber auch eine besondere Herausforderung, da der standardisierte Datenaustausch aufgrund von föderalen Strukturen und von Ressortgrenzen noch nicht selbstverständlich ist.

---

M. Döring (✉)

Department of Political Science and Public Management, University of Southern Denmark,  
Odense, Dänemark

E-Mail: [mdoering@sam.sdu.dk](mailto:mdoering@sam.sdu.dk)

S. Noack

Init[ Aktiengesellschaft für digitale Kommunikation, Berlin, Deutschland  
E-Mail: [Sebastian.Noack@init.de](mailto:Sebastian.Noack@init.de)

**Schlüsselwörter**

Zentrale Register · Online-Zugangsgesetz · *Once-only*-Prinzip · XÖV-Standards · *Open Source*

---

## 1 Begriffsbestimmung

Standardisierter Datenaustausch bezieht sich auf die elektronische, regelmäßige und wechselseitige Übermittlung von Daten zwischen verschiedenen IT-Systemen in verschiedenen Verwaltungsorganisationen. Bei der Interoperabilität von Datenbeständen können *vier Ebenen* unterschieden werden: die *rechtliche*, die *organisationale*, die *semantische* und die *technische* Ebene.

Für den Austausch von Daten brauchen Behörden eine *rechtliche* Grundlage. Neben der Zulässigkeit des Datenverkehrs geht es insbesondere um Themen wie Umfang und Detailierunggrad der Übermittlung. Sind in Gesetzen spezifische Standards explizit vorgegeben, so sind technische oder inhaltliche Anpassungen nur begrenzt zulässig oder verursachen einen höheren Änderungsaufwand.

Der Austausch von Daten muss zudem mit den vorhandenen *Organisationsstrukturen* und Geschäftsprozessen vereinbar sein. Ähnliche Prozesse sind in verschiedenen Verwaltungen häufig unterschiedlich organisiert (etwa im Vergleich der Länder). Nichtsdestotrotz müssen Daten ausgetauscht und verarbeitet werden können.

Kulturelle Unterschiede, die den Kontext berühren, in dem Daten vorliegen, können die praktischen Probleme auf der *semantischen* Ebene vertiefen. Unterschiedliche Sprachen können insofern eine Herausforderung für den Datenaustausch darstellen. Die unterschiedliche Schreibweise von Namen (je nach Sprache) sind ein Beispiel dafür, warum Standards erforderlich sind, damit die Daten an verschiedenen Stellen richtig interpretiert werden können. Die unterschiedliche Auslegung von Begriffen wie „Adresse“ wäre ein anderes Beispiel.

Auf der *technischen* Ebene schließlich stellen sich Fragen bezüglich der Datenformate (.xml, .csv usw.) und der Zeichencodierung (ASCII, UTF-8 usw.). Ohne technische Standards könnten Daten im schlimmsten Fall nicht an anderen Stellen maschinell weiterbearbeitet oder ausgewertet werden.

Nur wenn diese vier Ebenen in Einklang gebracht werden können, kann ein standardisierter Datenaustausch problemlos vonstattengehen. Die Interoperabilität der Daten und IT-Systeme ist insofern die maßgebliche Voraussetzung für ein funktionierendes *E-Government*, gerade in föderalen Regierungssystemen.

---

## 2 Konzeptionelle Grundlagen

Die Digitalisierung erfordert ein hohes Maß an Verfügbarkeit und Integrität von Daten, ein Ziel, das häufig durch Zentralisierung erreicht werden soll. Zentrale Rechenzentren, zentrale Register und die IT-Konsolidierung des Bundes sind Beispiele, die diese Tendenz illustrieren. Jedoch liegen diese Zentralisierungstendenzen

im Konflikt mit dem föderalen Staatsaufbau Deutschlands. Dies führt dazu, dass Daten auf allen Verwaltungsebenen und in allen Gebietskörperschaften mehrfach erhoben werden, von jeweils unterschiedlichen Ebenen benötigt und verarbeitet werden. Das sogenannte „*Once-only-Prinzip*“ (NEGZ 2017) setzt an dieser Stelle mit dem Ziel an, dass Bürger\*innen und Unternehmen bestimmte Standardinformationen den Verwaltungen nur noch einmal mitteilen müssen und die Verwaltungen die Informationen untereinander austauschen. 2017 wurde das *Online-Zugangsge-setz* beschlossen, wonach alle Dienstleistungen von Bund, Ländern und Gemeinden bis 2022 auch elektronisch angeboten werden sollen. Dies soll im Wesentlichen über den sogenannten *Portalverbund* realisiert werden, über den die häufig dezentralen Verwaltungsleistungen gebündelt digital angeboten werden sollen (BMI 2017). Die Anforderungen an eine enge Kooperation zwischen Verwaltungen werden damit komplexer. Prinzipien wie die Ressorthoheit und die Eigenständigkeit von Ländern und Kommunen sind dabei allerdings häufig Reibungspunkte, die eine solche Kooperation erschweren und sogar verhindern.

Zentrale Datenregister bieten für dieses Problem einen Ausweg, da sie einerseits die Hoheit der Gebietskörperschaften unberührt lassen und gleichzeitig eine zentrale Quelle für Daten zur Verfügung stellen. Diese Register ermöglichen den Spagat zwischen einem dezentralen, ebenen-übergreifenden Datenzugriff, einheitlichen digitalen Prozessen in Behörden und hohen Anforderungen an den Datenschutz. Elementar für das Funktionieren solcher Register ist jedoch die Standardisierung des Datenaustauschs, um die Vergleichbarkeit und Wiederverwendbarkeit sowie die Kompatibilität der jeweiligen Verwaltungsprozesse sicherstellen zu können.

Der standardisierte Datenaustausch und der Zugriff auf zentrale Datenregister erfolgt i. d. R. durch Fachanwendungen in den einzelnen Behörden. Die *Software* dazu wird in vielen Fällen durch private Softwarehersteller, aber manchmal auch durch die Verwaltung selbst entwickelt und zur Verfügung gestellt. Fachanwendungen bieten die Nutzeroberfläche und damit den Zugang des Verwaltungsmitarbeiters zu den Daten. Sie müssen in der Lage sein, die erforderlichen Daten in dem vorgegebenen Format austauschen zu können. Offene und frei zugängliche Datenaustauschstandards ermöglichen jedem Softwarehersteller die eigenen Anwendungen entsprechend anzupassen. Ein anderer Ansatz ist ein proprietärer, nicht-offener Standard, der den Kreis möglicher Softwarehersteller stark einschränkt. Die Entscheidung welcher dieser Ansätze für den jeweiligen Anwendungsfall besser ist, zieht in erster Linie organisatorische und erst in zweiter Linie technische Fragestellungen nach sich.

---

### 3 Praktische Einsatzfelder

Aus diesem Grund wurden in Deutschland unter anderem die sogenannten *XÖV-Standards* (XML in der Öffentlichen Verwaltung; <https://www.xoev.de/>) entwickelt, die als methodische Grundlage für den maschinenlesbaren und standardisierten Austausch von Daten zwischen Behörden dienen sollen. Sie setzen vor allem an der technischen und semantischen Interoperabilitätsebene an, bieten jedoch auch Ansätze für die organisationale Ebene, wie beispielsweise das Änderungsmanagement.

Das XÖV-Rahmenwerk setzt dabei auf die Wiederverwendung von Methoden und Werkzeugen, um Synergieeffekte und Erfahrungen anderer *E-Government*-Projekte nutzbar zu machen, und schafft eine einheitliche Entwicklungsumgebung. Mithilfe einer transparenten Zertifizierung wird die notwendige Investitionssicherheit gewährleistet.

Als „Mutter aller XÖV-Standards“ gilt *XMeld*, das den standardisierten Austausch von Meldedaten von Bürger\*innen möglich macht und seit 2007 als verbindliche bundesweite Regelung im Einsatz ist. Die rechtliche und organisatorische Grundlage bildete die Neufassung des Melderechtsrahmengesetzes (MRRG) im Jahre 2002. Darin wurden neben den Anwendungsfällen der Datenübermittlung zwischen den ca. 5400 Meldebehörden auch die für diesen Zweck zu übermittelnden Daten festgelegt (z. B. Familienname, Vorname, Geschlecht, Geburtsdatum, Staatsangehörigkeiten). Organisatorische Herausforderungen ergaben sich für die Meldebehörden insbesondere durch angepasste und neu hinzugekommene Geschäftsprozesse, die es zu implementieren galt (bspw. Melderegisterauskunft für Bürger\*innen).

Die semantische Ebene wird bei XMeld, wie auch bei allen anderen XÖV-Standards, im Rahmen einer Spezifikation festgelegt. Darin wird beispielsweise bestimmt, dass die Übermittlung unvollständiger Geburtsdaten von Personen möglich ist und die fehlenden Daten mit Nullen bezeichnet werden. Für eine Person, die im Januar 1980 geboren wurde, der genaue Tag jedoch unbekannt ist, wird also 1980-01-00 übermittelt. Des Weiteren werden in der Spezifikation Festlegungen getroffen, wie Namen mit Buchstaben aus anderen Alphabeten (z. B. kyrillisch) zu übermitteln sind.

Die technische Ebene des XMeld-Standards umfasst u. a. die Festlegung auf ein einheitliches Übermittlungsprotokoll für den Datenaustausch. Damit wird unter anderem festgelegt, wie viele Parteien an der Kommunikation teilnehmen und wie genau das Anfrage- und Antwortverhalten abzulaufen hat. Darüber hinaus wurde eine einheitliche, hersteller- und produktneutrale Schnittstelle für alle Fachverfahren der Meldebehörden entwickelt. Die Nutzung des Standards mit der Schnittstelle wurde durch einen Grundsatzbeschluss der Innenministerkonferenz für alle Meldebehörden verbindlich. Demnach darf im Einwohnermeldebewesen keine Software eingesetzt werden, die nicht diese Standards implementiert hat.

Die Einführung von XMeld führte zu einer erheblichen Senkung des Aufwands für Bürger\*innen, Unternehmen und Verwaltungen. Schätzungen aus dem Jahr 2007 sahen allein durch den Wegfall von Portokosten eine jährliche Einsparung von ca. 5,5 Millionen Euro (OSCI-Leitstelle 2008). Das früher mühselige Abmelden des alten Wohnsitzes im Falle eines Umzugs entfiel hierdurch vollständig. XMeld wird fortlaufend unter Federführung der Koordinierungsstelle für IT-Standards (KoSIT) weiterentwickelt und gepflegt. Schwerpunkte sind dabei die Optimierung von Meldeprozessen sowie die Ausarbeitung weiterer möglicher Anwendungsfälle zur Datenübermittlung an andere Behörden in bestimmten Anwendungsfällen (KoSIT 2014a).

Am Beispiel XMeld wird deutlich, dass Standardisierung dann erfolgreich ist, wenn alle vier Ebenen (rechtlich/organisatorisch/semantisch/technisch) berücksichtigt werden und ineinander greifen. Noch während der Entwicklung dieses Standards

führte die Föderalismusreform I zu einer Kompetenzverlagerung des Meldewesens von den Ländern auf die Bundesebene. Das Melderechtsrahmengesetz wurde durch das Bundesmeldegesetz ersetzt, welches regelmäßig um weitere Anwendungsfälle für den Datenaustausch im Meldewesen ergänzt wird (z. B. Datenübermittlung an die Landesrundfunkanstalten).

Die Einführung von XÖV-Standards kann jedoch nur ein Baustein hin zur bundesweiten Digitalisierung von Verwaltungsleistungen sein, denn die Problematik dezentraler Datenhaltung und der mehrfachen Abfrage von Daten durch Behörden lässt sich damit nicht vollständig lösen. Ein weiterer Ansatz ist daher seit einigen Jahren die Einführung zentraler Register für eine einheitliche und zuverlässige Datenhaltung. Beispielsweise wurde 2013 das Nationale Waffenregister (NWR) mit Hilfe des Standards XWaffe entwickelt. Dieses Register ermöglicht es u. a. den Landespolizeien, unmittelbar auf Waffenregistrierungen aus allen Bundesländern zuzugreifen, was vor der Einführung ein mühseliger Prozess war, da die Länder, wenn überhaupt, eigene Register vorhielten, auf die man von anderen Gebietskörperschaften aus nicht zugreifen konnte. Ein weiteres Beispiel ist das elektronische Personenstandsregister (XPersonenstand), das 2009 eingeführt wurde, wodurch ein zentrales Verzeichnis für Ehe-, Lebenspartnerschafts-, Geburts- und Sterbedaten aufgebaut wurde, auf das insbesondere Standesämter zugreifen. Seit 2019 soll ein bundesweites „Bewacherregister“ den zuständigen Behörden dabei helfen, die fachliche Eignung und Zuverlässigkeit von Wachpersonal schnell und verlässlich festzustellen. Damit soll auch die Kontrolle am Einsatzort einer Wachperson (etwa bei Fußballspielen oder vor Flüchtlingsheimen) durch eine mobile Abfrage im Register erleichtert werden. Im Falle des Bewachungsgewerbes liegt die Vollzugsverantwortung bei den Ländern. Ein zentrales Register ermöglicht jedoch erstmals, dass Informationen zum Wachpersonal einmalig zentral und nicht – wie bisher – bei Mehrfachbeschäftigung des Personals mit sich teilweise widersprechenden Daten gespeichert werden.

Ein international vergleichender Blick in der EU zeigt weitere Potenziale auf (NKR 2017b). Gerade unitaristisch organisierte Staaten wie Estland, Schweden und Dänemark sind Vorreiter beim Aufbau und der Integration von Datenregistern. Estland schuf 2011 mit der zentralen Informationsbehörde (RIA) eine Behörde mit weitgehenden Steuerungs- und Harmonisierungskompetenzen. Durch ein Verzeichnis aller IT-Systeme und Datenbanken, die in der Verwaltung genutzt werden, verfügt RIA über ein essenzielles Steuerungsinstrument, ohne dabei selbst Daten zu speichern. Hierdurch kann die Integrität und Aktualität der Daten sichergestellt werden und Datenredundanzen aufgrund verschiedener Register verhindert werden. Des Weiteren stellen individuelle Identifikationsnummern sicher, dass alle Informationsobjekte (Personen, Kraftfahrzeuge etc.) eindeutig identifizierbar sind. Bürger\*innen haben mittels der *X-Road*-Plattform einen transparenten Überblick über die gespeicherten Daten und können Zugriffe auf diese Daten nachvollziehen.

In Dänemark wurde 2012 mit der Modernisierung der Registerdaten begonnen und eine zentrale Verknüpfungsstelle zu den sechs Fachregistern erstellt, in denen Basisdaten von Bürger\*innen und Unternehmen aus verschiedenen Domänen gesammelt werden. Durch die Verknüpfung der Schnittstelle mit den nationalen

Verwaltungsportalen sind diese Basisdaten bereits in entsprechenden Formularen vorausgefüllt.

Das SSBTEK (Gemeinsamer Service für Transferleistungen) in Schweden dient als Plattform für den standardisierten Datenaustausch von Sozialhilfeanträgen und verknüpft die Register verschiedener Institutionen, die hierfür relevante Daten erheben (bspw. Steuerverwaltung oder Sozialversicherung). Kommunen, die für die Bearbeitung von Sozialhilfeanträgen zuständig sind, können diese Daten auf Antrag anfordern. Hierdurch wird die Effizienz des Verfahrens erhöht und die Fehleranfälligkeit gesenkt. Die Infrastruktur soll in den kommenden Jahren weiter ausgebaut und um andere Anwendungsfälle erweitert werden.

Jedoch gibt es auch unter den Bundesstaaten einige, die Vorreiterrollen einnehmen und wegweisende Lösungen gefunden haben. Österreich praktiziert ein innovatives Verfahren zur Sammlung und Verschlüsselung von persönlichen Stammdaten. Diese Stammdaten werden mit einer geheimen Stammzahl zur eindeutigen Identifikation der Person bei der nationalen Datenschutzbehörde hinterlegt. In einem sogenannten *Hash*-Verfahren (ähnlich den Verfahren einer *Blockchain*) werden Teile dieser Daten verschlüsselt an andere Behörden weitergeleitet. Der Datensatz wird dabei jeweils mit einer aus der Stammzahl abgeleiteten neuen bereichsspezifischen Personenkennzahl (bPK) versehen. Den Behörden ist es nicht möglich, von dieser Kennzahl auf die originäre Stammzahl zu schließen. Ein unmittelbarer Datenaustausch zwischen den Behörden wird somit bewusst verhindert, er kann nur anlassbezogen im konkreten Fall über die Datenschutzbehörde erfolgen.

Die Schweiz wiederum setzt auf dezentrale Register, die jedoch bundesweit festgelegte Standards einhalten müssen. Für den landesweiten Austausch von Daten wurde eine Plattform geschaffen, die über verschiedene zertifizierte private Anbieter betrieben wird. Dieses Vorgehen zeigt recht eindrücklich, wie ein Zusammenspiel unter Vorhaltung von dezentralen Registern und zentralen Vorgaben zur Sicherstellung der Interoperabilität funktionieren kann.

Viele dieser Beispiele sind wenig öffentlichkeitswirksam, führen in den betroffenen Fachbereichen jedoch zu erheblichen Aufwandsersparnissen. Nichtsdestotrotz sind derartige Register-Projekte, die durch ihren Mehrebenencharakter eine erhebliche Komplexität mit sich bringen, in jedem Fall eine große Aufgabe. Der Normenkontrollrat hat in seinem Jahresbericht 2017 die Modernisierung der Registerlandschaft als ein zentrales Element der Digitalisierung der deutschen Verwaltung hervorgehoben, um das *Once-Only*-Prinzip effektiv verfolgen zu können (NKR 2017a).

---

## 4 Umsetzungsstand, Auswirkungen und Problemfelder

Um den standardisierten Datenaustausch der deutschen föderalen Verwaltung systematisch voranzutreiben, sind verschiedene Probleme in naher Zukunft zu lösen. Die praktischen Herausforderungen können insbesondere durch Maßnahmen auf der semantischen und technischen Ebene gelöst werden, da diese den Kern eines standardisierten Datenaustauschs bilden. Dennoch müssen auf der organisationalen

und politischen Ebene die Grundlage geschaffen werden, denn die Ursachen für bestehende Umsetzungshemmnisse sind nicht selten politischer Natur und weniger technische Restriktionen.

An IT-Standards mangelt es in Deutschland nicht. Ganz im Gegenteil ist die Landschaft der verwendeten IT-Standards sehr umfassend. Diese Diversität spiegelt die vielfältige Realität von Verwaltungshandeln wider (Sozialverwaltung, Grünflächenverwaltung, Schulverwaltung etc.). Für ein übergreifendes Datenmanagement kann diese Vielfalt jedoch zur Herausforderung werden, wenn die entsprechenden Fachanwendungen keine offenen Schnittstellen enthalten, um eine semantische und technische Interoperabilität zu gewährleisten. Diese Problematik wird zusätzlich verstärkt, wenn innerhalb eines Bereichs eine Vielzahl an Standards existiert und im Extremfall „jeder sein eigenes Süppchen kocht“. Beispielhaft wäre die Festlegung der Zeichensätze in Datenbanken. Hier unterstützen derzeit verschiedene Datenbanklösungen unterschiedliche Standards und schränken die zu verwendenden Zeichen unterschiedlich ein (ASCII, ALN, String Latin etc.). Der IT-Planungsrat gibt daher den an Unicode angelehnten Zeichensatz *String Latin* vor, was bisher jedoch nicht flächendeckend umgesetzt wurde (KoSIT 2014b). Die standardsetzenden Institutionen sind entsprechend vielfältig und reichen von internationalen Organisationen wie der ISO (Internationale Organisation für Standardisierung), supranationalen Institutionen wie der CEN (Europäisches Komitee für Normung) bis zu privaten Softwareherstellern, die eigene Standards setzen (z. B. ooxml von Microsoft). Manche fordern daher, dieser Vielfalt Einhalt zu gebieten, um einen problemlosen Datenaustausch in der öffentlichen Verwaltung ermöglichen zu können: Standards sollten standardisiert werden. Darüber hinaus müssen Standards frei verfügbar und möglichst quelloffen sein, um eine anpassbare Umsetzung zu ermöglichen und Investitionssicherheit zu garantieren. Der IT-Planungsrat hat hierfür erste Ansätze mit den XÖV-Standards angestoßen. Die einzelnen Verwaltungen wiederum können diese geforderten Standards an die Softwareentwickler weitergeben oder zu Bedingungen von Ausschreibungsverfahren machen. Bei nachfolgenden IT-Projekten, die die Vernetzung von Fachsoftware und Vorgangsbearbeitungssystemen anstreben, oder auch bei Registerprojekten kann hierdurch Zeit und Geld eingespart werden. Davon betroffen sind somit alle Verwaltungsebenen von der Kommune bis zum Bund.

Bei technischen Standards stellt sich zudem die Frage nach der Abhängigkeit der Verwaltung von Produkten bestimmter IT-Firmen, beispielsweise *Microsoft*. Die eigene Entwicklung von Standards ist nur ein Ansatz, um Interoperabilität in der Kommunikation zwischen und mit Behörden zu erreichen. Demgegenüber steht der Ansatz, dass alle Kommunikationspartner das gleiche Produkt bzw. die gleiche Software implementieren, um den reibungslosen Datenaustausch zu ermöglichen. Dieser „One-For-All-Ansatz“ (OFA) lässt sich an der Dominanz von *Microsoft-Office*-Produkten in der deutschen Verwaltung veranschaulichen. Allen Behörden, die diese Produkte einsetzen, ist es so möglich, die darin erstellten Dokumente zu öffnen und zu bearbeiten. Die Interoperabilität wird somit gewährleistet. Viele Verwaltungsmitarbeiter sind zudem mit der Nutzung dieser Produkte aus dem Privatbereich vertraut, was die Akzeptanz für diese Lösung erhöht.

Kommerzielle Einheitslösungen haben jedoch entscheidende Nachteile. Zwar basieren neue *Office*-Dokumente auf der plattform- und implementierungsunabhängigen Auszeichnungssprache XML. Die Struktur ist jedoch proprietär geschützt und nicht einsehbar oder für andere Hersteller aufgrund der Komplexität nicht vollständig umsetzbar. Dies führt zu einer starken Abhängigkeit der Behörden von einem Hersteller, denn Supportleistungen und die Umsetzung behördenspezifischer Anforderungen müssen immer mit diesem Hersteller oder dessen Subunternehmern vereinbart und bezahlt werden. Darüber hinaus führt die einheitliche Festlegung auf einen Hersteller zu einer Monopolbildung, was wiederum zu höheren Lizenzkosten für diese Produkte und somit zu höheren Kosten für die Verwaltung führen kann. Abgesehen davon wird durch Einheitslösungen der Wettbewerb von Softwareherstellern eingeschränkt oder gar vollständig verhindert, da die Abhängigkeit der Nutzer von den *Microsoft*-Produkten zu groß ist. Dies kann wiederum zu einer Verhinderung von Innovationen in diesem Bereich führen.

Die Diskussion zur Abkehr von *Microsoft*-Produkten wird daher in der deutschen Verwaltungslandschaft seit Jahren lebhaft geführt. Ein prominentes Beispiel ist die Stadt München, die 2006 damit begonnen hatte, die *Windows*-Arbeitsplätze der Kernverwaltung durch angepasste *Linux*-Systeme (LiMux) und *OpenOffice*-Anwendungen zu ersetzen. Nach einem Machtwechsel in der Stadtführung 2014 wurde jedoch zunehmend Widerstand mobilisiert. 2017 schließlich wurde der Beschluss gefasst, zu einer *Windows*-Lösung zurückzukehren. Welche Kosteneffekte eine solche Umstellung auf Monopolanbieter haben kann, zeigt allein schon der Umstand, dass *Microsoft* vor der Einführung von LiMux ein Serviceangebot abgab, das um rund ein Drittel unter dem ursprünglichen Angebot lag. Ein weiteres Beispiel ist eine Entscheidung der niedersächsischen Landesregierung, die Rechner ihrer Steuerverwaltung wieder auf *Windows* umzustellen, nachdem diese seit 2012 über eine *Linux*-Version genutzt wurden. Die Rückmigration wurde im Koalitionsvertrag von SPD und CDU im Jahre 2017 beschlossen. Grund hierfür sei u. a. der Mehraufwand in der länderübergreifenden Zusammenarbeit, da andere Bundesländer häufig auf *Windows*-Standards zurückgreifen. Wie groß dieser Mehraufwand tatsächlich ist, blieb ungeklärt. Hingegen entschied die Landesregierung Schleswig-Holstein 2018, perspektivisch große Teile der Landes-IT durch *Open-Source*-Software zu ersetzen. Ein konkreter Zeitplan dafür existiert noch nicht. Journalisten haben in diesem Zusammenhang herausgefunden, dass öffentliche Verwaltungen bei der Vergabe öffentlicher Aufträge an *Microsoft* gegen das europäische Vergaberecht verstießen und sich durch den Einsatz von *Microsoft*-Produkten angreifbar für Hacker und Spione machten (Barczok 2018).

Verwaltungen, die vor der Entscheidung stehen, bei digitalen Projekten entweder auf eine OFA-Lösung oder doch auf einen offenen Standard zu setzen, benötigen klare und einheitliche Entscheidungskriterien. Dazu gehören Faktoren wie Interoperabilität, Investitionssicherheit, Wirtschaftlichkeit, Sicherheit, Wiederverwendbarkeit und vieles mehr. Die Bundesregierung gibt dafür eine Zusammenstellung von Referenzen auf Spezifikationen und Methoden für Softwaresysteme der öffentlichen Verwaltung heraus, um den Entscheidern ein Werkzeug an die Hand zu geben. Diese Zusammenstellung heißt SAGA und ist für die Bundesverwaltung bei der

Auswahl ihrer Informationstechnologien verbindlich anzuwenden (Rat der IT-Beauftragten 2011). Problematisch ist jedoch, dass SAGA seit 2011 faktisch nicht aktualisiert wurde und die darin aufgeführten Standards nicht mehr aktuell sind. Jüngste Bemühungen, wie die Architekturrichtlinie für die IT des Bundes, die im Rahmen der IT-Konsolidierung des Bundes entstand, greifen den Ansatz von SAGA auf. Ziel der Verwaltung muss es hier sein, dass eine einheitliche, konsistente und regelmäßig aktualisierte Zusammenstellung von Standards zur Verfügung gestellt wird, die für alle IT-Projekte der Verwaltung verbindlich gilt.

Eine dritte Baustelle für den ebenen-übergreifenden Datenaustausch ist die Entwicklung einer *einheitlichen Behördenkennung*. Gerade bei Registern, die auch von kommunalen Stellen mit Daten gefüllt werden, ist die eineindeutige Identifizierung dieser Verwaltungen absolut notwendig. Für die differenzierte Rechtevergabe bei der Dateneingabe, Datenausgabe und Datenänderung sowie bei der Zuordnung von Daten und Zuständigkeiten wären solche Behörden-Identitäten grundlegend. Ein einheitlicher Standard würde dafür sorgen, dass diese ID nicht in jeder Anwendung und jedem Register unterschiedlich ausfällt und nicht in jedem dieser Projekte mühsam neu erarbeitet werden muss. Eine entsprechende deutschlandweite Kenntnis gibt es in dieser Form noch nicht, wäre allerdings für die elektronische Kommunikation im föderalen System ein wichtiger Entwicklungsschritt hin zu semantischer und technischer Interoperabilität von Daten. Die Forderung nach einem solchen „X-Behörde“-Standard ist schon über zehn Jahre alt (von Lucke und Viola 2008) und mündete bisher in dem Ansatz eines standardisierten Zuständigkeitsfinders (XZuFi). Mit XZuFi wird der Austausch von Daten zu Verwaltungsleistungen und zuständigen Stellen sowie hierzu erforderlichen Metadaten standardisiert. Dadurch werden Anwendungen wie ein deutschlandweiter Behördenfinder möglich ([www.behoerdenfinder.de](http://www.behoerdenfinder.de)). Die Zuständigkeit ist ein zentraler Aspekt, um Behörden eindeutig identifizieren zu können. Dennoch ist damit noch keine einheitliche Behörden-ID geschaffen, die verfahrensunabhängig und fachübergreifend eingesetzt werden kann. Hierfür wird es einen organisatorischen Unterbau geben müssen, um die Behördenliste zu pflegen und die Aktualität zu gewährleisten. Das Deutsche Verwaltungsdiensteverzeichnis (DVDV) des zentralen IT-Dienstleisters des Bundes (ITZ Bund) könnte zum Beispiel in Richtung eines Behördenverzeichnisses weiterentwickelt werden.

---

## 5 Perspektiven für Staat und Verwaltung

Der Föderalismus gilt als deutliches Hindernis für die konsequente Digitalisierung der deutschen Verwaltungslandschaft. Die Weiterentwicklung digitaler Services und Datenbanken ermöglicht jedoch den Spagat zwischen föderaler Selbstständigkeit und effizienten Prozessen wie erste Beispiele in Deutschland, aber auch im internationalen Vergleich zeigen. Die Weiterentwicklung der Registerlandschaft wäre ein Mammutprojekt, da allein die Grundlagen hierfür schätzungsweise 600 bis 800 Millionen Euro kosten würden (NKR 2017b). Hinzu kämen jährliche Kosten für den Betrieb und die sich anschließenden konkreten Registerprojekte.

Der standardisierte Datenaustausch wird durch den angestrebten Portalverbund, der nach dem Online-Zugangsgesetz aufgebaut werden soll, weiter vorangetrieben. Der Nutzen zeigt sich hierbei meist unmittelbar für Bürger\*innen und Unternehmen (siehe XMeld und Bewacherregister). Zugleich sind zunehmende Veränderungen in den öffentlichen Verwaltungen notwendig, da Geschäftsprozesse elektronifiziert und teils neue Fachanwendungen eingeführt werden. Doch dadurch sind auf Dauer Kosteneinsparungen und Effizienzsteigerungen möglich. Das *Once-Only-Prinzip* kann hierbei im Einklang mit dem Datenschutz verwirklicht werden, was den Verwaltungsaufwand aller Beteiligten nachhaltig senkt und die Arbeit der deutschen Verwaltungen selbst effektiver und fehlerärmer gestaltet.

Digitalisierung bedingt immer auch Standardisierung. Im Spannungsfeld des Föderalismus ist dieser Punkt besonders brisant, da Länder und Kommunen dabei um ihre Souveränität fürchten. Jedes ebenen-übergreifende IT-Vorhaben steht somit im Konflikt zwischen der Suche nach einheitlichen Prozessen, in denen standardisierte Daten gesammelt und kommuniziert werden können, und der eigenständigen Aufgabengestaltung unterschiedlicher Gebietskörperschaften. Dieser Konflikt lässt sich nicht ohne weiteres auflösen. Die Digitalisierung favorisiert dabei zentrale Lösungen. Nichtsdestotrotz ermöglicht sie im Gegensatz zu einer reinen organisatorischen oder aufgabenbezogenen Zentralisierung ein großes Maß an Eigenständigkeit dezentraler Einheiten. Zwar müssen zentrale Standards bestimmt und vereinbart werden, die letztliche Einbettung kann sich dennoch zu einem gewissen Grad unterscheiden und mehr oder minder an die örtlichen Gegebenheiten angepasst werden. Kompromisse bieten insofern Vorteile für alle Seiten. Das gilt nicht nur für eine effizientere Aufgabenerledigung, sondern vermeidet bei zunehmendem Problemdruck auch den Anschein, nur eine echte Zentralisierung könne Abhilfe schaffen.

---

## Literatur

- Barczok, Achim. 2018. ARD-Doku. Einsatz von Microsoft-Produkten in Behörden problematisch. *Heise Online*, 19. Februar. <https://www.heise.de/newsticker/meldung/ARD-Doku-Einsatz-von-Microsoft-Produkten-in-Behoerden-problematisch-3973448.h.html>. Zugegriffen am 18.03.2020.
- BMI (Bundesministerium des Innern). 2017. Grundprinzipien der Architektur des künftigen Portalverbundes. [https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/24\\_Sitzung/B31\\_Portalverbund\\_Anlage1.pdf?\\_\\_blob=publicationFile&v=4](https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/24_Sitzung/B31_Portalverbund_Anlage1.pdf?__blob=publicationFile&v=4). Zugegriffen am 18.03.2020.
- KoSIT. 2014a. Pflege des Standard OSCi-XMeld in 2014. Bremen: Koordinierungsstelle IT-Standards. <https://www.transparenz.bremen.de/dokument/bremen76.c.12997.de>. Zugegriffen am 18.03.2020.
- KoSIT. 2014b. Festlegung eines einheitlichen Zeichensatzes. Bericht zum Sachstand und Vorschlag zum weiteren Verfahren. Bremen: Koordinierungsstelle IT-Standards. <https://www.xoev.de/sixcms/media.php/13/Festlegung%20Zeichensatz.pdf>. Zugegriffen am 18.03.2020.
- Lucke, Jörn von, und Gerhard Viola. 2008. Ein Zuständigkeitsfinder für Deutschland. *E-Government-Computing*, 07. Januar. <https://www.egovement-computing.de/ein-zustaendigkeitsfinder-fuer-deutschland-a-148026/index2.h.html>. Zugegriffen am 18.03.2020.
- Nationaler Normenkontrollrat (NKR). 2017a. *Bürokratieabbau, Rechtsetzung, Digitalisierung. Erfolge ausbauen – Rückstand aufholen. Jahresbericht 2017 des NKR*. Berlin: Nationaler Normenkontrollrat.

- Nationaler Normenkontrollrat (NKR). 2017b. *Mehr Leistung für Bürger und Unternehmen. Verwaltung digitalisieren. Register modernisieren.* Berlin: Nationaler Normenkontrollrat.
- NEGZ e.V. 2017. Das Once-Only Prinzip. Potenziale für Bürger, Unternehmen und die Verwaltung. Berlin: Nationales E-Government Kompetenzzentrum. [https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Fachkongress/5FK2017/26April\\_II\\_once-only-prinzip.pdf?\\_\\_blob=publicationFile&v=3](https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Fachkongress/5FK2017/26April_II_once-only-prinzip.pdf?__blob=publicationFile&v=3). Zugegriffen am 18.03.2020.
- OSCI-Leitstelle. 2008. Automatisierte Datenübermittlungen im Meldewesen. Sachstandsbericht zur Frühjahrssitzung 2008 des AK I der IMK. <https://www1.osci.de/sixcms/media.php/13/2008-03-13-Sachstandsbericht%20der%20OSCI-Leitstelle..df>. Zugegriffen am 18.03.2020.
- Rat der IT-Beauftragten. 2011. Beschluss des Rates der IT-Beauftragten, Gegenstand: SAGA 5.0, 03.11.2011. Beschluss 71/2011. [https://www.cio.bund.de/SharedDocs/Publikationen/DE/Bundesbeauftragter-fuer-Informationstechnik/IT\\_Rat\\_Beschluesse/beschluss\\_71\\_2011\\_download.pdf?\\_\\_blob=publicationFile](https://www.cio.bund.de/SharedDocs/Publikationen/DE/Bundesbeauftragter-fuer-Informationstechnik/IT_Rat_Beschluesse/beschluss_71_2011_download.pdf?__blob=publicationFile). Zugegriffen am 18.03.2020.



---

# Digitale Archivpolitik

Catharina Wasner und Niklaus Stettler

## Inhalt

1 Klärung des Begriffs .....	645
2 Theoretische Grundlagen .....	646
3 Praktische Anwendung .....	649
4 Künftige Entwicklung .....	654
Literatur .....	655

---

## Zusammenfassung

Ebenso wie andere Institutionen in Politik und Verwaltung sind Staatsarchive vom Prozess der digitalen Transformation betroffen. Die Einführung der E-Akte sowie veränderte Nutzererwartungen stellen die Archive vor zahlreiche Herausforderungen. Wie Archive auf diese Wandlungsprozesse reagieren und inwiefern digitale Archivpolitik die Archive bei der Umsetzung ihrer neuen Aufgaben gestaltend unterstützen kann, wird in diesem Beitrag vorgestellt.

---

## Schlüsselwörter

Staatsarchiv · Langzeitarchivierung · E-Akte · Online-Portale · Archivpolitik

---

## 1 Klärung des Begriffs

Archive sichern das Gedächtnis einer Gesellschaft. Sie dokumentieren und bewahren Entscheidungen und Erinnerungen. Archive stellen ein einzigartiges, unersetzliches kulturelles Erbe dar, wie der Internationale Archivrat in seiner „Universal Declaration on Archives“ betont (International Council on Archives 2011). Dieses

C. Wasner (✉) · N. Stettler

Hochschule für Technik und Wirtschaft HTW Chur, Chur, Schweiz  
E-Mail: [catharina.wasner@htwchur.ch](mailto:catharina.wasner@htwchur.ch); [niklaus.stettler@htwchur.ch](mailto:niklaus.stettler@htwchur.ch)

kulturelle Erbe werde durch die Arbeit der Archive für zukünftige Generationen erhalten und verständlich. Weiterhin hebt der Archivrat die wichtige Funktion des Archivguts hervor, das als zuverlässige und frei zugängliche Informationsquelle transparentes Verwaltungshandeln und somit Demokratie und Bürgerrechte stärke.

Dienten Archive in früheren Jahrhunderten der Machtsicherung der jeweiligen Machthaber, verstehen sie sich heute als moderne und offene Informationsdienstleister, die mit verschiedenen Serviceangeboten das Archivgut für ihre Nutzenden u. a. aus Forschung und Zivilgesellschaft, aber auch für Privatpersonen zugänglich machen wollen (Gillner 2018). Auch wenn der Internationale Archivrat mit seiner Erklärung hauptsächlich auf die Archive der staatlichen Verwaltung fokussiert, gibt es Archive in großer Zahl und Vielfalt. Über die Staats-, Landes-, Kreis- und Kommunalarchive hinaus gibt es Wirtschafts-, Rundfunk-, Privatarchive sowie Archive von Forschungseinrichtungen oder Parteien, außerdem weitere auf bestimmte Themen, Medien oder Kulturgüter spezialisierte Archive. Privatarchive sind kaum Gegenstand der Diskussion um Archivpolitik, obwohl sie eine nicht zu unterschätzende Informationsquelle darstellen können. Um Archive von anderen Gedächtnisinstitutionen abgrenzen zu können, wird oftmals der Unikat-Charakter, also die Einzigartigkeit, des Archivguts betont. Archive müssen an Schriftgut übernehmen, was in ihrem Auftrag vorgesehen ist. Bibliotheken hingegen betreiben eine aktive Sammlungspolitik von i. d. R. Duplikaten. Museen wiederum bewahren auch Unikate, jedoch liegt der Fokus hier auf Objekten. In der Realität sind die Grenzen zwischen den Institutionen fließend.

Unter Archivpolitik wird die Planung und Steuerung der Tätigkeit der staatlichen Archive verstanden. Digitale Archivpolitik befasst sich mit dem Wandel dieser Institutionen und der aktiven Steuerung dieses Wandels im Zuge der Digitalisierung. *Staatsarchive* sind öffentlich-rechtlich verfasste Archive, denen die gesetzliche Aufgabe zugewiesen ist, das staatliche Verwaltungshandeln zu dokumentieren. Es gibt sie – zumindest im deutschsprachigen Raum (andere politische Systeme, in denen der Föderalismus weniger ausgeprägt ist, organisieren die Archivierung z. T. anders) – auf allen Ebenen des staatlichen Handelns. Unter digitalem Kulturerbe im Zusammenhang mit Staat und Verwaltung ist das Archivgut staatlicher Archive zu verstehen, das als offene und transparente Dokumentation von Verwaltungs- und Regierungshandeln im Dienste von Demokratie und Rechtsstaatlichkeit steht (vgl. Lepper und Rauff 2016).

---

## 2 Theoretische Grundlagen

Das digitale Zeitalter hat die jüngsten Wandlungsprozesse für die *Staatsarchive* mit sich gebracht. Von den Archiven selbst wird und wurde der digitale Transformationsprozess angesichts knapper finanzieller Mittel und oftmals fehlender technischer Ressourcen als Herausforderung, zunehmend aber auch als Chance, vor allem bezüglich einer größeren Wahrnehmung in der Öffentlichkeit und erweiterter Kundenbeziehungen, betrachtet. Mittlerweile versteht sich das traditionell eher in analogen Denk- und Organisationsstrukturen verhaftete Archivwesen als digitale

Dienstleistungs- und Informationsinfrastruktur. Gründe für diesen Wandel waren und sind zum einen der Anpassungsdruck an die virtuelle Lebensrealität der Nutzenden und die damit verbundene Erwartungshaltung und zum anderen die Umstellung der Verwaltung auf digitale und datengetriebene Prozesse in der Aktenführung. Diese Gründe sollen im Folgenden näher ausgeführt werden.

Die Lebenswelt der Menschen hat sich im digitalen Zeitalter stark virtualisiert. Damit verbunden ist eine gewisse Erwartungshaltung an die bereitgestellten Dienste der verschiedensten Akteure der Gesellschaft. Wirtschaftsunternehmen, Zivilgesellschaft und Private sind genauso betroffenen wie die Akteure aus Staat und Verwaltung. Als selbstverständlich gelten heute die Nutzung von Smartphones und Tablets, das Lesen von E-Books und E-Papers sowie Online-Shopping und -Banking. Insbesondere aber das Auffinden von Information im Internet über Online-Suchmaschinen und deren permanente Verfügbarkeit von jedem Ort und zu jeder Zeit, lassen auch die Nutzenden von Archiven immer mehr digitale Dienstleistungen einfordern. Es geht nicht mehr nur um die Bereitstellung von Online-Findmitteln und bequemen Recherche-Portalen der Metadaten. Es wird geradezu selbstverständlich angenommen, dass alle Archivbestände, also Bilder, Filme, Plakate, Archivakten, etc. digital vorliegen und mit wenigen Mausklicks auf den eigenen PC geladen werden können. Argumente wie Urheberrechte, große analoge Bestände und wenig Ressourcen, die die Online-Findbarkeit des Archivguts behindern, mindern den Erwartungsdruck nicht.

In den ersten Kontakt mit der neuen digitalen Lebensrealität kamen die Archive durch die Einführung der elektronischen Aktenführung im Verwaltungsprozess um die Jahrtausendwende. In allen deutschsprachigen Ländern wurden nahezu gleichzeitig Konzepte und Standards vorgelegt, wie die Akte in digitaler Form nachgebildet werden könnte. Demnach sollte – so das Postulat – in der Verwaltung kein Papier mehr genutzt werden müssen, vielmehr der gesamte Verwaltungsprozess in Form von digitalen Ordnern abgebildet werden können. Lange begegneten die meisten Archive dieser Veränderung mit größter Zurückhaltung. Wo die Herausforderung angenommen wurde, geschah dies in erster Linie auf der technischen Ebene: Die Archive suchten Wege, wie digitale Files in eine noch unbekannte Zukunft transportiert werden könnten. Das digitale Archiv schien insbesondere eine technische Herausforderung darzustellen, die jedoch mit geeigneten Modellen und Verfahren – zumindest im Verbund verschiedener Akteure – bewältigt werden konnte. Erst in jüngster Zeit wurde deutlich, dass die Digitalisierung der Verwaltung wesentlich größere Implikationen für die Archive hat. Allein schon der Umstand, dass die digitalen Akten besser durchsuchbar sind als ihre analogen Vorgänger, zwingt die Archive aufgrund des Datenschutzes dazu, viele Dokumente unter Verschluss zu halten.

Ungleicher größer sind die Auswirkungen der datengetriebenen Verwaltung. Unmengen an Daten werden zwischen den verschiedenen staatlichen Organen ausgetauscht, ein nicht unbedeutender Teil davon auch in Open-Data-Portalen zur Verfügung gestellt. Die Archive verlieren – so machte es zuerst den Anschein – hier ihre Funktion als Institution, die je gesondert die Daten der einzelnen Organe aufzubewahren und zur Verfügung stellen, während diejenigen staatlichen Stellen,

die die Daten zusammenführen, in gewisser Weise auch Archivfunktionen übernehmen, indem sie beispielsweise Zeitreihen zusammenstellen. Bereits 1996 hat der australische Archivwissenschaftler Frank Upward darauf hingewiesen, dass die traditionelle Arbeitsteilung zwischen verschiedenen staatlichen Organen und insbesondere zwischen den Verwaltungseinheiten und dem Archiv im Zuge der Digitalisierung nicht mehr sinnvoll ist. Unter dem Begriff des „Records Continuum Concept“ wird eine Neupositionierung der Archive postuliert, die sich demnach nicht mehr allein darauf konzentrieren können, Unterlagen der sog. stabilen Phase zu archivieren. Vielmehr müssten die Archive bereits in der Phase der Aktenproduktion eingreifen und zugleich spezialisierten Verwaltungseinheiten die Archivierung ihrer Unterlagen überantworten (Upward 1996). Im deutschsprachigen Raum stoßen solche Gedanken bislang noch kaum auf größeres Interesse.

Das Archivwesen ist durch Archivgesetze geregelt. Dabei ist sowohl in Deutschland, Österreich als auch der Schweiz aufgrund des föderalen Staatsaufbaus eine dreigeteilte Verwaltungsstruktur vorzufinden: Bund, Länder/Kantone und Städte/Gemeinden. Auf allen diesen Ebenen gibt es Archive. Gesetzlich geregelt sind die Archive auf Bundes- und Landesebene. In der Regel gibt es ein Archivgesetz des Bundes und jeweilige Landesarchivgesetze für die Länder. Die Archivgesetze sind eine junge Rechtsmaterie. Entstanden sind sie in Deutschland seit den 1980er-Jahren, in Österreich und der Schweiz erst seit Ende der 1990er-Jahre. Die Gesetze regeln Abgabepflichten aller staatlichen Stellen, die rechtliche Stellung der Archive, ihre Aufgaben und Kompetenzen, den Schutz des Archivguts, Sperrfristen sowie Zugangs- und Nutzungsrechte. Das Archivrecht in Deutschland ist als Teilbereich des öffentlichen Informationsrechts Bestandteil des Besonderen Verwaltungsrechts. Es befindet sich als solches im Spannungsverhältnis zwischen den Rechtsgütern des Informationsrechts des Bürgers bzw. der historischen Forschung und Wissenschaftsfreiheit einerseits und staatlicher Sicherheits- und Geheimhaltungsinteressen sowie Persönlichkeitsrechte Dritter andererseits (vgl. Berger 2016; Lepper und Raulff 2016).

Archive sind Kulturerbe-Institutionen. Aus diesem Grund stehen sie auch im Kontext der Bemühungen der UNESCO, das kulturelle Erbe der Menschheit zu erhalten und schützen. Im digitalen Zeitalter hat die UNESCO ihren Begriff von Kulturerbe erweitert, welcher nun auch das digitale Kulturerbe umfasst. Die „Charter on the Preservation of the Digital Heritage“ aus dem Jahre 2003 (UNESCO 2003) oder die „Vancouver-Deklaration – The Memory of the World in the Digital Age: Digitization and Preservation“ aus dem Jahre 2012 (UNESCO/UNC 2012) sind Ausdruck dieses neuen Verständnisses. Hintergrund ist die auch von vielen anderen Stellen geäußerte Befürchtung, das digitale Erbe gehe der Nachwelt verloren. Es bestehe die Gefahr, dass die Anfänge des digitalen Zeitalters für zukünftige Generationen einen weißen Fleck darstellen könnten, ähnlich der schlechten Dokumentationslage über das europäische Mittelalter. Digitale Inhalte sind fragil und unterliegen einer rasanten technischen Entwicklung. Dazu tragen laut Charter verschiedene Faktoren bei, wie das schnelle Veralten von Hard- und Software, welche die Daten erst lesbar macht, weiterhin die Ungewissheit über die Ressourcen, die Verantwortung und die Methoden für Wartung und Erhalt sowie das Fehlen unterstützender

Rechtsvorschriften. Die UNESCO ruft mit ihren Erklärungen Regierungen und Gedächtnisorganisationen zum Handeln und zur Entwicklung von Politiken und Strategien auf. Aus der Vancouver-Erklärung ging das UNESCO PERSIST Programme hervor, das eine Roadmap für Lösungen und Policies für die vertrauenswürdige *Langzeitarchivierung* entwickeln will (UNESCO 2019).

Heute, mehr als fünfzehn Jahre, nachdem die „Charter on the Preservation of the Digital Heritage“ verabschiedet wurde, sind die Dinge langsam ins Rollen gekommen. Von einer digitalen Archivpolitik im Sinne eines Politikfeldes kann jedoch bis heute nur in Ansätzen gesprochen werden. Dies zeigt sich zum Beispiel auch daran, dass nationale digitale Strategien zum einen, wie von vielen Seiten bemängelt, viel zu spät entwickelt wurden und zum anderen vorerst eher Absichtserklärungen als Strategien zum digitalen Kulturgut geschweige denn zur Steuerung von *Staatsarchiven* beinhalteten. 2010 erschien die „Digitale Agenda für Europa“ der Europäischen Union (Europäische Kommission 2010), die sich im Schwerpunkt eher der Frage widmet, wie man einen digitalen Binnenmarkt schaffen kann, um so wirtschaftliche Vorteile zu erzielen. Unter dem Punkt „Förderung von kultureller Vielfalt und kreativen Inhalten“ wird als Förderschwerpunkt im kulturellen Bereich immerhin der Ausbau der europäischen digitalen Bibliothek „Europeana“ beschrieben. Erst 2014 erschien die „Digitale Agenda 2014–2017“ der Bundesregierung, welche den Begriff „Archiv“ allerdings nur zwei Mal und den Begriff „Kulturgut“ drei Mal aufführt (Bundesregierung 2014). Geäußert wird die Absicht, den Zugang zu letzterem zu verbessern und dessen Digitalisierung vorantreiben zu wollen. Für die meisten *Staatsarchive* relevanter als die Bundespolitik sind jedoch aufgrund der föderalen Zuständigkeiten den Kulturbereich betreffende Digital-Strategien auf Landesebene. Der Stand der digitalen Transformation ist in den *Staatsarchiven* dabei höchst heterogen und abhängig von dem Zeitpunkt der Einführung der *E-Akte* sowie weiterhin von Know-how, politischem Willen und den zur Schaffung notwendiger Infrastrukturen finanziellen Mittel. So verfügt beispielsweise Baden-Württemberg bereits seit 2006 über Infrastrukturen zur Archivierung digitaler Unterlagen, während sich der Aufbau des Digitalen Archiv Nord, ein Zusammenschluss der Länder Bremen, Hamburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und Schleswig-Holstein, bis heute verzögert.

Wie aber begegnen nun die Archive den Herausforderungen des digitalen Zeitalters? Wie setzen sie die digitale Archivierung um und wie reagieren sie auf die neuen Erwartungshaltungen der Nutzenden? Dies soll im nächsten Abschnitt geklärt werden.

---

### 3 Praktische Anwendung

Staatliche Archive haben seit jeher die Aufgabe, Archivgut, das im Rahmen des staatlichen Handelns entstanden ist, zu verwahren. Die gesetzlichen Bestimmungen bilden den Rahmen der archivarischen Tätigkeit, die traditionell die Aufgaben der Übernahme und Bewertung, der Erschließung, der Sicherung und Erhaltung sowie der Bereitstellung und Auswertung des Archivguts umfassen. Diese Bestimmungen

und Aufgaben haben auch im digitalen Zeitalter nicht ihre Gültigkeit verloren und stehen nach wie vor im Mittelpunkt der Archivarbeit.

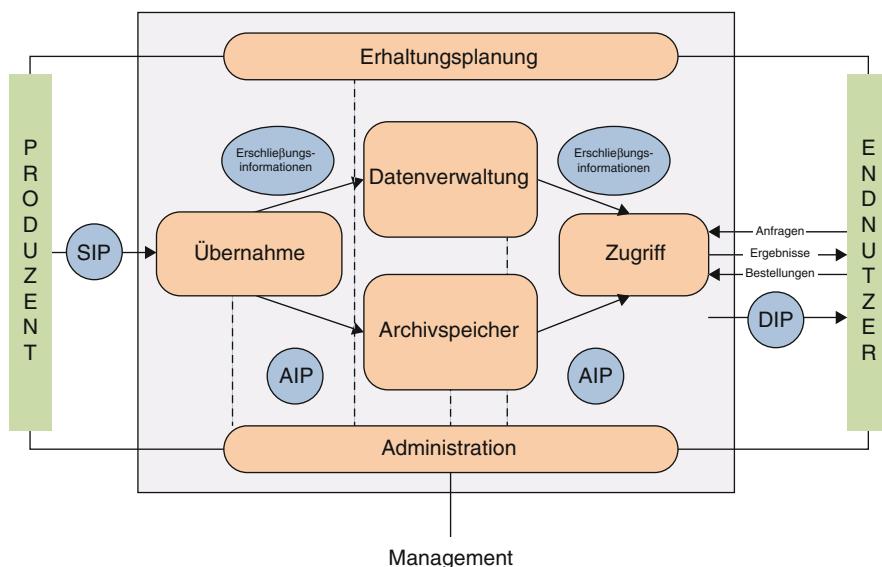
Die erste archivarische Aufgabe besteht darin, das Verwaltungsschriftgut zu sichten. Dem Archivar obliegt die verantwortungsvolle Aufgabe, zu entscheiden, welches Schriftgut ins Archiv zur dauernden Aufbewahrung übernommen wird und welches „kassiert“, also vernichtet wird. Dieser Vorgang heißt „Bewertung“, durch welchen das Verwaltungsschriftgut zum Archivgut wird. Die Schwierigkeit des Vorgangs wird deutlich, wenn man sich vor Augen führt, dass die zukünftige Quellenlage und das spätere Geschichtsbild einer Gesellschaft vom Bewertungsentscheid des Archivars abhängen, jedoch jeder Entscheid zur Übernahme Kosten und zu leistenden Arbeitsaufwand steigen lässt. Vom modernen Verwaltungsschriftgut werden etwa 5 Prozent übernommen. Eine vollständige Archivierung allen Schriftguts kommt aus Platz- und Ressourcengründen nicht infrage. Das Platzproblem scheint sich zwar durch die digitale Schriftgutverwaltung zu vermindern, jedoch bleibt das Ressourcenproblem bei der Erschließung, dem nächsten Schritt im Archiv. Unter Erschließung sind Ordnungs- und Verzeichnisarbeiten zu verstehen, die die Auffindbarkeit und Nutzbarkeit des Archivguts durch Einträge und Dokumentationen in den archiveigenen Findbüchern gewährleisten. Diese Arbeiten erfolgen nach fachspezifischen Regeln. Um das Archivgut zu gliedern, ist das Archiv in verschiedene Bestände unterteilt. Diese stellen die Zwischenstufe zwischen dem Archiv als Ganzem und den einzelnen Archivalien dar und sind somit zentrale Gliederungseinheiten. Bestände sind auf bestimmte Art strukturiert und enthalten wiederum Archivalien-Einheiten, meistens in Form von Akten. Ein Bestand stammt in der Regel von einer bestimmten Organisation, z. B. von einem Ministerium, einem Verein, einem Unternehmen, oder aber von natürlichen Personen. Dieses Provenienzprinzip, das verlangt, Bestände im Archiv nach ihrer Herkunft als Einheit zu behandeln und die Zusammenhänge der Unterlagen aus ihrer Entstehungszeit zu erhalten, hat sich als Grundsatz der Strukturierung von Archiven durchgesetzt. Zu einem Bestand gehört außerdem ein Findmittel, das den Inhalt eines Bestandes wiedergibt. Die Bestandssicherung eines analogen Archivs erfordert vielfältige konservatorische und restauratorische Maßnahmen, vorbeugende Maßnahmen in Bezug auf die Lagerung sowie regelmäßige Kontrollen. Die Bereitstellung des Archivguts ist das Ziel des Archivs (Burkhardt 2006).

Diese beschriebenen Aufgaben sind auch im digitalen Zeitalter nach wie vor zentrale Tätigkeiten des Archivs. Allerdings erweist es sich als unumgänglich, dass auch die Archive schneller reagieren müssen, wenn sie Unterlagen von der Zerstörung retten wollen. Sowohl die organisatorischen wie auch die technischen Veränderungen in der digitalen Verwaltung bringen die Gefahr mit sich, dass Unterlagen verloren gehen. Um dem vorzubeugen, haben Archive und Verwaltungseinheiten begonnen, den Bewertungsprozess zu verändern, sodass bereits im Vorfeld der Aktenproduktion klar definiert werden kann, welche Unterlagen am Schluss archiviert werden sollen. Diese „prospektive Bewertung“ hat die Archivarbeit wesentlich umgestaltet.

Seit Einführung der *E-Akte* und digitalen Verwaltung bauen die bisher analog betriebenen Archive digitale Strukturen zur *Langzeitarchivierung* auf. Dieser Pro-

zess ist noch nicht abgeschlossen. Gerade kleine Archive mit wenig Ressourcen können diese Aufgabe allein nicht meistern, weshalb vermehrt Verbundprojekte und Kooperationen ins Leben gerufen werden, die der gemeinsamen Erarbeitung von Standards und Best-Practices dienen. So wurde beispielsweise die Norm ISO 14721 „Open Archival Information System – OAIS“, welche zuerst 2002 von der Data Archiving and Ingest Working Group des Consultative Committee for Space Data Systems (CCSDS) unter Federführung der NASA veröffentlicht wurde (nestor 2003), das gängige Referenzmodell beim Aufbau eines digitalen Langzeitarchivs, das bis heute Gültigkeit hat. Es beschreibt ein digitales Langzeitarchiv als eine Organisation, in dem Personen und technische Systeme zusammenwirken, um digitale Daten langfristig zu erhalten und verfügbar zu machen. Es diente insbesondere der Etablierung einer einheitlichen Fachterminologie im Bereich der digitalen *Langzeitarchivierung* und ist weniger als detaillierte Anleitung zur technischen Implementierung gedacht. Die unten stehende Abbildung illustriert das Konzept des Modells (Abb. 1).

Das OAIS unterscheidet zwischen drei so genannten Informationspaketen sowie zwischen sechs Aufgabenbereichen. Die Informationspakete stehen für die digitalen Unterlagen, die an ein Archiv abgegeben, dort weiterverarbeitet und zur Nutzung bereitgestellt werden. In der OAIS-Terminologie steht das Submission Information Package (SIP) für die vom Produzenten an das Archiv übergebenen Unterlagen. Im Archiv selbst werden die SIP durch Metadaten und Dokumentationen ergänzt, in archivtaugliche Formate gebracht und somit zur langfristigen Aufbewahrung zu einem Archival Information Package (AIP) umgeformt. Damit die Bestände eines Archivs aber auch genutzt werden können, ist es erforderlich, verschiedene Dis-



**Abb. 1** OAIS-Funktionseinheiten (nestor 2013, S. 33)

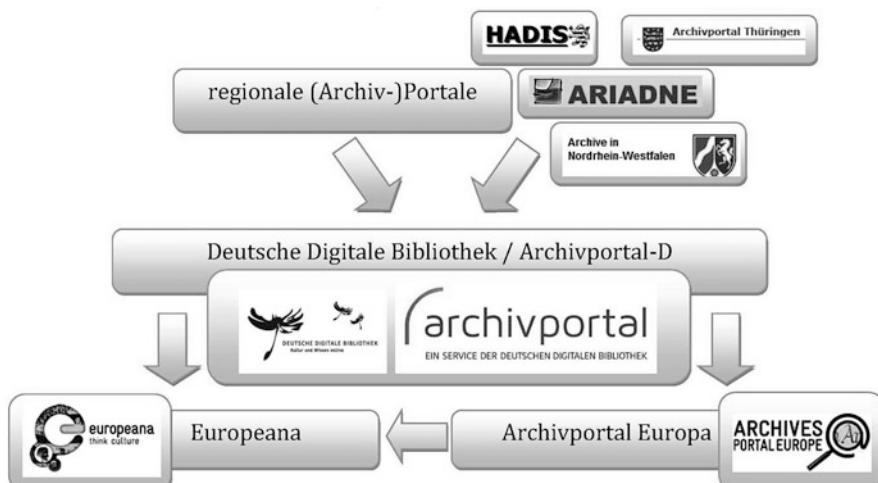
semination Information Packages (DIP) zu erzeugen, die für bestimmte Nutzergruppen je nach rechtlicher Situation zielgruppenorientiert über *Online-Portale* und andere Kanäle zur Verfügung gestellt werden. Form und Inhalt der einzelnen Pakete können sich dann durchaus unterscheiden. Der Anspruch von digitaler *Langzeitarchivierung* ist es, den Erhalt der Daten auf unbegrenzte Zeit über Veränderungen in der Technik, also Soft- und Hardware, und in der Zielgruppe, also auch künftige Generationen, sicherzustellen. Diese besonders herausfordernde Aufgabe erfordert, einen permanenten Zielgruppen- und Technology-Watch zu betreiben, damit das digitale Archivgut für die jeweilige vorgesehene Zielgruppe langfristig verfügbar und verstehbar bleibt, auch wenn Technologien und Nutzungsgewohnheiten sich längst verändert haben. Diese Aufgabe ist am ehesten in Netzwerken und Communities zu bewältigen, welche sich für diese Zwecke in der Zwischenzeit gebildet haben, wie z. B. das nestor-Netzwerk, das 2009 als Kooperationsverbund aus einem vom BMBF geförderten Projekt hervorging.

Die zunehmend virtuelle Lebenswirklichkeit machte auch vor den Archiven nicht halt. Waren es zu Beginn des Internets vorerst nur einfache Webseiten, auf denen die Archive mit allgemeinen Informationen Präsenz zeigten, so wurden diese Internet-präsenzen nach und nach immer weiter ausdifferenziert, um den Nutzerinteressen entgegen zu kommen (Gillner 2018). Das umfasste zunächst die Veröffentlichung von Bestände-Übersichten und Findmitteln im Netz, für welche manchmal erst eine Digitalisierung derselben stattfinden musste. Inzwischen sind auch vor dem Hintergrund der Open-Access- und der späteren Open-Data-Bewegung Archivalien in digitaler Form hinzugekommen. Umfangreiche Bemühungen zur Digitalisierung der analogen Bestände finden bis heute statt. Trotz großer Anstrengungen ist jedoch erst ein kleiner Teil der Archivbestände digitalisiert. Das deutsche Bundesarchiv verfügt z. B. über 330 laufende Kilometer Akten, welche aufgrund der Masse auch noch in den nächsten Jahren nicht digital zur Verfügung stehen werden. Herausfordernd ist abgesehen von der großen Menge an Beständen auch deren Heterogenität an Quellengattungen, wie Fotos, Mikrofilme/Makrofiches, Urkunden, Akten, Karten/Pläne und Amtsbücher, für die jeweils eigene Strategien und Workflows zur qualitativ hochwertigen und kostengünstigen Digitalisierung entwickelt werden müssen.

Diese Entwicklung hatte zur Folge, dass *Online-Portale* in großer Vielzahl mit unterschiedlichen Schwerpunkten und in der Regel medien- oder projektbasiert und ohne Absprache voneinander entwickelt wurden. Diese Vielzahl ist für den Nutzenden, der Recherche und Forschung betreiben möchte, kaum zu überschauen. Darüber hinaus prägt die „Google-Suche“ das heutige Suchverhalten, mit der Folge, dass für den Suchenden komfortable und möglichst alle globalen Bestände erfassende Suchmöglichkeiten erwartet werden. Die utopische Vorstellung, dass alles globale Wissen zukünftig für alle erreichbar sei, fängt an in der Realität Gestalt anzunehmen durch den Aufbau von integrierten Meta-Portal-Lösungen, die eine über Organisations- und Ländergrenzen hinweg übergreifende Suche ermöglichen sollen. Für das einzelne Archiv eröffnet sich so eine weltweite Nutzungsperspektive zum Beispiel durch den Aufbau des von der EU ins Leben gerufenen Meta-Portals „Europeana“, dessen Ziel es ist, das Kulturgut Europas an einem Ort für jedermann

zugänglich zu machen (Europeana 2019). Integriert werden hier die Metadaten aus ganz unterschiedlichen Gedächtnisorganisationen. Um die Digitalisate selbst zu konsultieren, wird der Suchende auf das jeweilige Portal der bereitstellenden Institution weitergeleitet. Damit jedoch die europäische Datenintegration gelingen kann, sind wiederum Anstrengungen auf nationaler Ebene notwendig, welche die stark ausdifferenzierte Portal-Landschaft auf nationaler Ebene zusammenführen. So entstand unter Förderung der Deutschen Forschungsgemeinschaft 2014 ein Archivportal für Deutschland, das aus regionalen Archivportalen gespeist wird und seine Daten weiter an die Europeana leitet. Die unten stehende Abbildung illustriert die Datenweitergabe innerhalb der Archiv-Portal-Landschaft in Deutschland (Abb. 2).

Standen die Archive anfangs den Entwicklung rund um das Web 2.0 eher skeptisch gegenüber, werden mittlerweile zahlreiche Versuche gestartet, digitale Kommunikation, Partizipation und Community-Building aktiv voranzutreiben. Bei sinkenden Vor-Ort-Besucher- und steigenden Online-Nutzer-Zahlen rückt der digitale Nutzerkontakt zunehmend in den Fokus. Wenn auch spät, so sind doch viele Archive mittlerweile auf Social-Media-Kanälen zu finden oder betreiben eigene Blogs. Beratungen von Archivnutzenden müssen jedoch in der Regel individualisiert angeboten werden. Aus diesem Grund hat das Schweizerische Bundesarchiv beispielsweise einen virtuellen Beratungs-Chat eingeführt, in welchen Nutzende und Archivmitarbeitende direkt und darüber hinaus über eine geteilte Bildschirmansicht kommunizieren können. Welche Möglichkeiten die digitale Vernetzung für das Archivwesen weiterhin bietet, zeigt sich z. B. auch bei der Nutzung von Crowd-sourcing. Diverse archivische Erschließungs-Projekte versuchen durch die Einbindung von Freiwilligen bisher nicht dokumentierte Bestände zu erschließen. Die Vorteile von Crowdsourcing gehen aber über Kosteneinsparung und schnelle Pro-



**Abb. 2** Schaubild der deutschen Archiv-Portal-Landschaft aus dem DFG-Projekt „Aufbau eines Archivportals-D“ (Quelle: Wolf 2016, S. 63)

jeckdurchführung hinaus. Zum Beispiel gelingt es mit Hilfe von kollektivem Wissen, unbekannte Personen, Orte oder Gegenstände auf Bildern nachträglich zu identifizieren und somit dem Archivgut seinen Kontext zurückzugeben.

---

## 4 Künftige Entwicklung

Auch künftig werden die *Staatsarchive* die digitale Transformation weiter vorantreiben müssen, wenn sie nicht Gefahr laufen wollen, an der Lebensrealität ihrer Nutzenden vorbei zu agieren. Es ist davon auszugehen, dass zukünftig der Fokus stärker auf die Erweiterung des digitalen Dienstleistungsangebots gelegt werden wird als bisher geschehen. Grenzen bei dieser Ausrichtung werden bestehende gesetzliche Regelungen zu Datenschutz und bestimmten Schutzfristen sein, an denen aber weiterhin festgehalten werden wird. Leidenschaftlich diskutiert wird allerdings über das Thema des Urheberrechts, das in Bezug auf die Digitalisierung und digitale Bereitstellung von Kulturgut ein großes Hindernis darstellt und das eine umfassende Digitalisierung des kulturellen Erbes auf Jahrzehnte verhindern wird. Hier ist damit zu rechnen, dass Kultureinrichtungen weiterhin auf eine Verbesserung der rechtlichen Situation hinwirken werden.

Die immer stärkere Ausrichtung der Verwaltungen auf Daten und digitale Prozesse erfordert es, die digitalen Strategien der Archive noch mehr auf die Automatisierung der Archiv-Prozesse auszurichten, um die über die Archive einbrechende Datenflut überhaupt handhaben zu können. Damit die Archive diese Herausforderungen meistern können, wird nach wie vor eine verstärkte Vernetzung und Zusammenarbeit zwischen den Archiven notwendig sein sowie eine Neuausrichtung des Berufsbildes des Archivars. Weiterhin gilt es innovative Verfahren zur Bewertung der Archivwürdigkeit zu entwickeln, um möglichst ressourcenschonend, aber ausgewogen, gesellschaftlich auch zukünftig relevante Unterlagen ins Archiv zu bringen. Ein Beispiel dafür ist die „partizipative Bewertung“ des Schweizerischen Bundesarchivs, in deren Rahmen über verschiedene Kanäle die Zivilgesellschaft, Experten und Laien, in den Bewertungsprozess miteinbezogen werden sollen. Es ist damit zu rechnen, dass kooperative und kollektive Beteiligung an Aufgaben des Archivs zukünftig größere Bedeutung erfahren werden.

Doch wie wird es zukünftig um die digitale Archivpolitik bestellt sein? Wie gezeigt, gibt es nicht einen bestimmten Akteur, der die Tätigkeit der staatlichen Archive plant und steuert. Archivpolitik scheint im Gegenteil in Ermangelung wirklicher politischer Steuerung ein Sammelsurium aus internationalen Richtlinien, nationalen Absichtserklärungen sowie in Archiv-Netzwerken entwickelten Best-Practices zu sein. Archivpolitik findet noch am ehesten dort statt, wo finanzielle Ressourcen für die Umsetzung der digitalen Transformation in Archiven freigegeben werden. So ist die Notwendigkeit der zusätzlichen Finanzierung mittlerweile im Bewusstsein der Politik angekommen und es sind auch Mittel freigegeben worden. Wünschenswert wäre jedoch darüber hinaus, dass die Politik ihren Gestaltungsauftrag stärker wahrnehmen würde. Denn in Zeiten, in denen immer mehr Daten in der datengetriebenen Verwaltung erzeugt, ausgetauscht und der Öffentlichkeit zur Ver-

fügung gestellt werden, verschwimmen die Grenzen zwischen den Aufgaben der datenerzeugenden und -bereitstellenden staatlichen Institutionen. Digitale Archivpolitik muss daher die Grenzen der Organisationseinheit verlassen und zunehmend darauf abzielen, dass die Funktion der Erhaltung der digitalen Objekte auch weiterhin gewährleistet wird. Digitale Archivpolitik ist nicht zuletzt die Neuaushandlung der Frage, wer diese Funktion künftig gewährleisten soll.

---

## Literatur

- Berger, Hannes. 2016. Das deutsche Archivrecht im Wandel. *Zeitschrift für Landesverfassungsrecht und Landesverwaltungsrecht* 1(1): 12–22.
- Bundesregierung. 2014. Digitale Agenda 2014–2017. [https://www.de.digital/DIGITAL/Redaktion/DE/Publikation/digitale-agenda.pdf?\\_\\_blob=publicationFile&v=3](https://www.de.digital/DIGITAL/Redaktion/DE/Publikation/digitale-agenda.pdf?__blob=publicationFile&v=3). Zugegriffen am 07.03.2019.
- Burkhardt, Martin. 2006. *Arbeiten im Archiv. Praktischer Leitfaden für Historiker*. Paderborn: UTB.
- Europäische Kommission. 2010. Eine Digitale Agenda für Europa. KOM(2010)245 endgültig. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:DE:PDF>. Zugegriffen am 07.03.2019.
- Europeana. 2019. Europeana Collections. <https://www.europeana.eu/portal/de>. Zugegriffen am 07.03.2019.
- Gillner, Bastian. 2018. Offene Archive. Archive, Nutzer und Technologie im Miteinander. *Archivar* 71(1): 13–21.
- International Council on Archives. 2011. Universal Declaration on Archives. <https://www.ica.org/en/networking/unesco/unesco-officially-endorses-uda>. Zugegriffen am 07.03.2019.
- Lepper, Marcel, und Ulrich Rauff, Hrsg. 2016. *Handbuch Archiv. Geschichte, Aufgaben, Perspektiven*. Stuttgart: J.B. Metzler.
- nestor. 2003. nestor Handbuch. Eine kleine Enzyklopädie der digitalen Langzeitarchivierung. [nestor.sub.uni-goettingen.de/handbuch/artikel/nestor\\_handbuch\\_artikel\\_228.pdf](http://nestor.sub.uni-goettingen.de/handbuch/artikel/nestor_handbuch_artikel_228.pdf). Zugegriffen am 07.03.2019.
- nestor. 2013. *nestor-Arbeitsgruppe OAIS-Übersetzung/Terminologie. Referenzmodell für ein Offenes Archiv-Informations-System. Deutsche Übersetzung 2.0. nestor-materialien* 16. Frankfurt a. M.: nestor.
- UNESCO. 2003. Charter on the preservation of digital heritage. [http://portal.unesco.org/en/ev.php?URL\\_ID=17721&URL\\_DO=DO\\_TOPIC&URL\\_SECTION=201.html](http://portal.unesco.org/en/ev.php?URL_ID=17721&URL_DO=DO_TOPIC&URL_SECTION=201.html). Zugegriffen am 07.03.2019.
- UNESCO. 2019. UNESCO PERSIST Programme. <https://unescopersist.org/about/>. Zugegriffen am 07.03.2019.
- UNESCO/University of British Columbia (UBC). 2012. Vancouver declaration. The memory of the world in the digital age: Digitization and preservation. [http://www.unesco.org/new/en/member-states/single-view/news/unesco\\_releases\\_vancouver\\_declaration\\_on\\_digitization\\_and\\_pr/](http://www.unesco.org/new/en/member-states/single-view/news/unesco_releases_vancouver_declaration_on_digitization_and_pr/). Zugegriffen am 07.03.2019.
- Upward, Frank. 1996. Structuring the records continuum. Part one. Postcustodial principles and properties. *Archives & Manuscripts* 24(2): 268–285.
- Wolf, Christina. 2016. Eines für alle: das Archivportal-D. Neue Zugangswege zu Archivgut. In *Neue Wege ins Archiv. Nutzer, Nutzen, Nutzung. 84. Deutscher Archivtag 2014 in Magdeburg*, (Tagungsdokumentationen zum Deutschen Archivtag, Bd. 19), Hrsg. Verband deutscher Archivarinnen und Archivare e.V. (VdA), 47–63. Fulda: VdA.