DIVSI-Perspektiven 4

Michael Fehling/Utz Schliesky (Hrsg.)

# Neue Macht- und Verantwortungsstrukturen in der digitalen Welt

in Verbindung mit dem Deutschen Institut für Vertrauen und Sicherheit im Internet

Nomos

DIVSI
Deutsches Institut für Vertrauen und Sicherheit im Internet

DIVSI-Perspektiven

herausgegeben vom
Deutschen Institut für Vertrauen und Sicherheit
im Internet

Band 4

Prof. Dr. Michael Fehling, LL.M./
Prof. Dr. Utz Schliesky (Hrsg.)

# Neue Macht- und Verantwortungsstrukturen in der digitalen Welt

in Verbindung mit dem Deutschen Institut für Vertrauen und Sicherheit im Internet

Nomos

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

ISBN 978-3-8487-3253-1 (Print)

ISBN 978-3-8452-7601-4 (ePDF)

1. Auflage 2016

# Vorwort

In Kooperation mit der Hamburger Bucerius Law School und dem Kieler Lorenz-von-Stein-Institut hatte DIVSI zu einem zweitägigen Symposium eingeladen. „Neue Macht – und Verantwortungsstrukturen in der digitalen Welt“ sollten in einem Kreis von Vertretern des öffentlichen Lebens und der Wissenschaft erörtert werden.

Ich selber bin in einer Zeit groß geworden, in der ein demokratisches, gesellschaftliches Zusammenleben in einer freien, sozialen Marktwirtschaft entwickelt wurde. Der ständige Ausgleich zwischen Starken und Schwachen ist dabei eine der Hauptaufgaben. Die Macht- und Verantwortungsteilung zwischen Staat, Wirtschaft und Gesellschaft hat über die Jahre viel Grundstabilität gewonnen. Sie hat diese Stabilität behalten bei allen Schwankungen, die es gab. Doch gilt das auch weiterhin? Entwickeln sich nicht schleichend oder schon deutlich sichtbar Verschiebungen in diesem Gefüge?

Nach meiner Einschätzung ist es für die Menschen in ihrem alltäglichen Leben zu einer zentralen Frage geworden, wie sich die Grundbedürfnisse Vertrauen und Sicherheit gerade im digitalen Zeitalter entwickeln. Die technischen Veränderungen haben erhebliche Einflüsse auf unsere Gesellschaft, besonders auch durch ihre nicht nachlassende Geschwindigkeit. Dabei müssen wir die etwas romantische Vorstellung aus der Zeit des aufkommenden Internets zu den Akten legen, dass alle Menschen gleich sein werden, wenn sie moderne digitale Technik nutzen. Unsere Lebenswelt-Forschung, die wir in den DIVSI Internet-Milieus abbilden, zeigt eher, dass die Unterschiede sich verstärken.

Umso mehr sind die Verantwortlichen unseres Gemeinwesens aufgerufen und gefordert, Lösungen für die anstehenden Probleme zu entwickeln. Es ist hohe Zeit, aktiv zu werden. Die Historie der Menschheit zeigt uns, dass vor allem jene Gesellschaften gewonnen haben, die ihre Zukunft im Blick hatten und nicht die, die ihre Vergangenheit bewahren wollten.

Das Hamburger Symposium hat natürlich keine endgültigen Lösungen präsentieren können. Gleichwohl mögen der gedankliche Austausch und die dabei zutage gekommenen neuen Ideen ein klein wenig dazu beitragen, Anregungen für die Lösung der auf dem Tisch liegenden Aufgaben zu liefern.

Mit Freude habe ich Hamburgs Ersten Bürgermeister Olaf Scholz im Festsaal der Bucerius Law School begrüßt. Er hat es sich nicht nehmen lassen, das Symposium persönlich zu eröffnen. Dieser Einsatz unterstreicht die Bedeutung und Wichtigkeit solcher Veranstaltungen. Einer der Schwerpunkte in seiner Regierungserklärung für die laufende Legislaturperiode der Hamburgischen Bürgerschaft heißt, das moderne Hamburg ist digital. Ich darf diesen Gedanken des Bürgermeisters um eine bundesweite Perspektive ergänzen: Es liegt an uns allen, dass dieser Anspruch in jedem Winkel von Deutschland erfüllt wird.

*Matthias Kammer*

Direktor
Deutsches Institut für Vertrauen und Sicherheit im Internet

# Inhalt

# Grußwort

Sehr geehrter Herr Kammer,
sehr geehrter Herr Professor Thorn, sehr geehrter Herr Albrecht,
sehr geehrter Herr Kleindiek,
meine sehr verehrten Damen und Herren,

ich heiße Sie heute hier in Hamburg herzlich willkommen.

Sie haben sich ein großes Thema vorgenommen. Die Digitalisierung ist schließlich der Kern vieler gesellschaftlicher und wirtschaftlicher Umbrüche, die wir derzeit erleben. Die Frage nach den neuen Macht- und Verantwortungsstrukturen in der digitalen Welt ist daher so naheliegend, dass es oftmals schwerfällt, sie nüchtern und rational zu stellen und zu diskutieren.

Ich bin aber ganz zuversichtlich, dass Ihnen das heute und morgen hier an der Bucerius Law School gelingen wird. Denn, dass Sie sich Hamburg als Ort für diese Debatte ausgesucht haben, hat durchaus Sinn.

Als ein zentraler Standort der Medien- und Digitalwirtschaft haben wir mit zu den ersten gehört, die die Folgen der Digitalisierung in Wirtschaft und Öffentlichkeit zu spüren bekamen. Um nicht dauerhaft als Getriebene der Zeitläufte durch den Wandel gehetzt zu werden, fördern wir heute die digitale Transformation mit Nachdruck – das gilt für die Hafenlogistik genauso wie für die Lehrangebote unserer Schulen und Hochschulen, für die Verkehrssteuerung ebenso wie für die staatlichen Museen.

Hamburg entwickelt sich zu einer digitalen Stadt und wenn wir es richtig angehen, dann haben wir die Möglichkeit, diese große und moderne Stadt mithilfe neuer Technologien noch lebenswerter und wirtschaftlich stärker zu machen.

Wesentlich ist dafür, dass uns das Management des Technologiebruchs gelingt. Denn hinsichtlich Relevanz und Radikalität ist das, was wir derzeit erleben, allenfalls mit der Erfindung des Buchdrucks und der frühen Industrialisierung und Elektrifizierung zu vergleichen.

Die neuen technologischen Möglichkeiten ergreifen unsere Wirtschaft und unsere Gesellschaft seit zwei Jahrzehnten wellenweise. Zunächst hat die Digitalisierung die Informations- und Kommunikationsmöglichkeiten erfasst und insbesondere die Medien- und Kreativwirtschaft vor neue Herausforderungen gestellt.

In einer zweiten Welle haben sich die Produktions- und Logistikprozesse tiefgreifend verändert und tun es noch. Das Schlagwort von der Industrie 4.0 ist mittlerweile in aller Munde. Hier im Hamburger Hafen, im Smart Port, lässt sich erleben, wie weitreichend der Wandel ist.

Und in einer dritten Welle ergreift die Digitalisierung die öffentliche Infrastruktur und den öffentlichen Raum. Die Schnittstellen der technischen Systeme werden zunehmend allgegenwärtig und ermöglichen uns Formen der Zusammenarbeit und Prozesssteuerung, die noch vor wenigen Jahren undenkbar waren.

Längst ist es zu einer Art Wettbewerb geworden, möglichst große Zahlen künftig vernetzter Geräte zu prognostizieren – wahlweise verheißungsvoll oder verängstigend.

Schon als es mit der Digitalisierung im Westen der USA, im Silicon Valley, so richtig losging, da war viel die Rede von der so genannten „California Ideology". Gemeint war damit die Überzeugung, dass die neuen digitalen Möglichkeiten in der Lage seien, unsere Gesellschaften unbegrenzt freier und partizipativer zu machen, besser und gerechter. Der frühe Leitsatz von Google „Don't be evil" fällt in diese Zeit und fußt auf diesen Überzeugungen.

Ich will hier nicht einer naiven Technikgläubigkeit das Wort reden, aber es könnte nicht schaden, wenn wir uns von diesem Optimismus ein wenig abgucken würden. Denn die grundsätzliche Überzeugung, dass es möglich ist, mit technischen Innovationen unser Leben zu verbessern, teile ich ausdrücklich. Der Fortschritt nicht nur der Industrie-, sondern auch der digitalen Gesellschaft ist eng verknüpft mit der technologischen Entwicklung und unserer gesellschaftlichen Fähigkeit, uns diese nutzbar zu machen.

Hier können wir durchaus lernen von einer Kultur wie der US-amerikanischen, die in neuen Möglichkeiten zunächst einmal Chancen und nicht Risiken entdeckt. Die moderne Gesellschaft, in der wir leben, ist geprägt davon, dass soziale und wirtschaftliche Veränderung möglich ist. Sie muss daher auch lernen, mit Unsicherheiten und Unübersichtlichkeiten umzugehen.

Wer den Fortschritt durch Technik will, der muss aushalten können, dass manches gut klingende Vorhaben scheitert und aus manch unscheinbarem Anfang Großes entstehen kann.

Die frühen Träger des digitalen Wandels, jene weltumspannenden Marken des Internets, von denen einige auch ihre Deutschland-Dependancen hier in Hamburg haben, sind oftmals aus kleinen und simplen Ideen ent-

standen. Sie haben Nischen besetzt und sind aus diesen hinausgewachsen zu globalen Plattformen und Anbietern.

Die Geschwindigkeit, in der das passiert, setzt all diejenigen unter Druck, die sich um vernünftige regulatorische Rahmenbedingungen bemühen.

Das lässt sich exemplarisch an der Innovationsdynamik im Medien- und Kommunikationssektor zeigen:

Die gedruckte Presse hat noch Jahrhunderte gebraucht, bis sie weltweit auf eine Nutzerzahl von über 50 Millionen gekommen ist, das Radio brauchte 38 Jahre, das Fernsehen noch 13. Digitale Plattformen wie Google+ schaffen eine vergleichbare Marktdurchdringung heute binnen sechs Monaten.

Das führt immer wieder dazu, dass neue Angebote oder Applikationen längst fester Bestandteil unseres Alltags geworden sind, bevor der Gesetzgeber sie überhaupt als relevant entdeckt hat.

Meine Damen und Herren,

angesichts dieser fundamentalen Veränderungen wird in den Debatten über die Digitalisierung immer wieder so getan, als gäbe es eine digitale Stunde Null, als müssten wir die normativen und ökonomischen Grundlagen unserer Gesellschaften völlig neu bestimmen.

Anders als oftmals beabsichtigt, führt diese Sichtweise dazu, dass Veränderungen unwahrscheinlicher werden. Transformationsprozesse gelingen in der Regel eben nicht mit einem großen Sprung oder einem Ruck, der durchs Land gehen muss.

Zunächst einmal gilt die Werteordnung unseres Landes und unserer Gesellschaft ganz unabhängig von der Frage der technologischen Möglichkeiten. Das ist auch ein Hinweis auf die Frage nach den künftigen Machtstrukturen: Auch künftig wird es demokratisch legitimierte Machtausübung durch entsprechend ausgestattete gesellschaftliche Institutionen geben. Technologische Innovationen fordern demokratische Systeme heraus, aber sie verändern sie nicht automatisch und an sich.

Letztlich müssen sich Innovationen an den durch sie ermöglichten gesellschaftlichen und wirtschaftlichen Mehrwerten messen lassen. Den dazu nötigen politischen Diskurs müssen wir organisieren.

Daran müssen sich auch globale Anbieter gewöhnen: Wir haben das jüngst am Bespiel Uber erlebt. Allein die Tatsache, dass eine Geschäftsidee technisch umsetzbar ist, heißt noch längst nicht, dass sie damit auch auf dem Boden unseres Rechtsstaates steht.

Wer Fahrdienste wie Uber Pop zulassen möchte, der muss dazu die bundesgesetzlichen Regelungen zur Personenbeförderung ändern. Das geht aber nicht dadurch, dass ein kapitalstarkes Unternehmen viele Anwälte beschäftigt und auch nicht durch beharrliches Ignorieren von Gerichtsurteilen. Dafür bedarf es eines demokratischen Diskurses und der daran anknüpfenden entsprechend legitimierten Entscheidungen.

Das Beispiel zeigt sehr schön, dass es Grundsätze gibt, die wir bewahren wollen, ganz unabhängig davon, was vielleicht möglich wäre.

Es ist sinnvoll, dass der demokratische Souverän sich hier jeden Einzelfall ansieht und auch einzeln bewertet. Denn während wir Uber Pop darauf hinweisen mussten, dass deren Geschäftsmodell nicht okay ist, haben wir hier in Hamburg mit MyTaxi gleichzeitig ein Beispiel dafür, wie die Digitalisierung in der Verkehrsbranche funktioniert.

Und wir haben mit Anbietern anderer Sharing-Plattformen wie AirBNB und 9Flats Regelungen gefunden, auf deren Basis ihr jeweiliges Geschäftsmodell funktionieren kann. Diese Gesetzesmacht haben die demokratischen Rechtsstaaten. Wir haben keinen Anlass, uns da künstlich klein zu machen vor dem halbstarken Gebaren manches Anbieters.

Zugleich sollten wir uns davor hüten, selber wie Halbstarke aufzutreten. Gerade wenn wir in eine technologisch offene Zukunft blicken, ist es ratsam, Schritt für Schritt zu gehen.

Wir erleben das zum Beispiel seit Jahren immer wieder auf Neue in der Medienpolitik, die sich mit als erste mit den Folgen der Digitalisierung auseinandersetzen musste. Da werden große Entwürfe für neue Medienordnungen geschrieben, die angesichts der Digitalisierung öffentlicher Kommunikation möglichst alles möglichst ganz anders zu denken und zu ordnen versuchen.

In der Regel handelt es sich bei diesen Entwürfen um akademisch wertvolle Gedankenspiele ohne politische Relevanz. Meistens sind sie erledigt in dem Moment, in dem sie das Licht der Öffentlichkeit erblicken. Ein wenig ist es da wie mit dem seit den 1970er Jahren geforderten einheitlichen Arbeitsgesetzbuch. Einen derartigen Wurf kann es gar nicht geben, weil eine neuerliche Nulllinie des Interessenausgleichs nicht bestimmbar ist.

In den aktuellen Debatten über eine künftige Medien- und Kommunikationsordnung gehen wir daher anders vor. Wir diskutieren nicht die Kompetenzverteilung zwischen Ländern, Bund und Europa und propagieren auch keine völlig neue Ordnung, sondern versuchen die Schnittstellen zwischen Landes-, Bundes- und Europarecht besser zu managen.

Das kann gelingen, wenn wir uns auf gemeinsame Regulierungsziele, auf Kollisionsregeln und auf Governance-Instrumente verständigen.

Diesen Ansatz verfolgen wir aktuell in der Bund-Länder-Kommission, in der sich die Länder gemeinsam mit dem Bund vor allem über die Schnittstellenthemen wie Kartellrecht und Vielfaltssicherung oder Intermediär-Regulierung austauschen, um gemeinsam abgestimmte Regulierungsvorschläge zu entwickeln.

Diese Herangehensweise scheint mir für Fragen des Managements der Digitalisierung ganz generell sinnvoll zu sein.

Angesichts der Innovationsdynamik werden wir schließlich kaum in der Lage sein, ex-ante Vorgaben zu machen. Viel wichtiger ist es, dass wir abstrakte und prinzipiengeleitete Vorstellungen entwickeln, die dann entweder auf dem Wege der Co- und Selbstregulierung oder aber im Rahmen der deutschen oder europäischen Gesetzgebung angewendet werden.

Das ist keine Aufgabe für den Gesetzgeber allein, sondern hier sind Wirtschaft und Gesellschaft gleichermaßen in der Pflicht, gemeinsame Überlegungen zu entwickeln und zur Geltung zu bringen.

Meine Damen und Herren,

von diesen Gedanken lassen wir uns auch leiten, wenn wir darüber nachdenken, wie sich Hamburg als digitale Stadt weiterentwickeln soll.

Wir stehen vor der Aufgabe, die Schnittstellen der Verwaltung zu den Bürgerinnen und Bürgern ebenso zu digitalisieren wie unsere öffentliche Infrastruktur. Und wir haben die Chance, dadurch Innovationsräume für Unternehmen zu öffnen, in denen neue Angebote und Technologien ausprobiert und in Piloten zur Marktreife geführt werden können. Dabei geht es letztlich immer darum, durch Technologie die Qualität unserer Services zu verbessern und Ressourcen effizienter zu nutzen. Wir haben uns in Hamburg vorgenommen, die Digitalisierung und ihre Potenziale zu verstehen und als Chancen zu begreifen. Wir wollen auf Augenhöhe sprechfähig sein. In der Stadt passiert schon unglaublich viel. Um diese Prozesse zu bündeln, aufeinander abzustimmen und Synergien zu heben, richten wir derzeit in der Senatskanzlei im

Amt Medien eine Leitstelle für die Digitale Stadt ein. Sie soll dabei helfen, einen besseren Überblick über die zahlreichen Projekte und Prozesse zu erlangen. Zugleich belassen wir die Verantwortung für die einzelnen Projekte der Digitalisierung ausdrücklich bei den fachlich zuständigen Behörden. Wir wollen nicht, dass die Trans- formationsthemen in irgendwelche Stäbe oder ins IT-Referat delegiert werden. Sie müssen Gegenstand

des alltäglichen Verwaltungshandelns werden. Erst dann wird es uns gelingen, die Chancen der Digitalen Stadt voll zu entwickeln.

Wir müssen hier unseren eigenen Weg finden Denn wir über Macht- und Verantwortungsstrukturen reden, dann lassen sich die oft herausgehobenen Blaupausen US-amerikanischer Smart Cities nämlich nicht ohne Weiteres nach Europa und nach Deutschland übertragen. Das hat auch etwas damit zu tun, dass wir hier nicht so sehr vor der Aufgabe stehen, neue Serviceangebote digital zu entwickeln. Vielmehr müssen wir bestehende Angebote ins Digitale übersetzen.

Das heißt auch, dass wir mit den bisherigen Erwartungen an die Verwaltungsdienstleistung umgehen müssen, wenn wir neue Optionen schaffen. Es geht auch hier darum, die digitale Disruption in einen beherrschbaren Transformationsprozess zu überführen. Dazu gehört, dass wir mit den veränderten gesellschaftlichen und wirtschaftlichen Erwartungen an Staat und Verwaltung umgehen.

Ein Beispiel dafür ist das Transparenzgesetz, das wir in Hamburg in der vergangenen Legislaturperiode verabschiedet haben und das die Grundlage geschaffen hat für ein Transparenzportal, in dem alle wesentlichen Informationen über das Handeln von Senat und Verwaltung für jede Bürgerin und jeden Bürger zugänglich sind.

Mit diesem Schritt haben wir die bisherige Logik des Verwaltungshandelns umgedreht. Es ist noch gar nicht so lange her, da musste derjenige, der eine Auskunft haben wollte, begründen, warum er einen Anspruch darauf hat, sie zu bekommen. Jetzt muss der Staat „begründen“, warum er eine Information nicht preisgibt. Diese Umkehr der Beweislast ist eine richtige und sinnvolle Antwort auf die berechtigten Partizipationsan- sprüche der Bürgerinnen und Bürger.

Zugleich liefern OpenData-Portale auch privaten Unternehmen die Möglichkeit, aufsetzend auf zugänglichen öffentlichen Datenbeständen Geschäftsmodelle zu entwickeln und an den Markt zu bringen.

Neben der Transparenz öffentlicher Daten ist der Schutz individueller Daten ein weiteres wichtiges Prinzip der neuen digitalen Ordnung. Hier haben wir es mit einer zentralen Bürgerrechtsfrage zu tun – vor allem, wenn es um den Schutz dieser Daten vor dem Zugriff des Staates geht. Die Debatte über die Datenschutzgrundverordnung der EU zeigt, wie viel Arbeit wir hier noch gemeinsam zu leisten haben und wie sehr dieses Politikfeld noch in Bewegung ist. Allerdings findet die Debatte an der richtigen Stelle statt. Denn nur ein europaweites Recht hat eine Chance relevant

zu sein. Die Nationalstaaten sind für eine Regelung im weltweiten Web oft zu klein.

Vielleicht erleben wir zurzeit ja sogar einen Paradigmenwechsel weg von der reinen Datensparsamkeit hin zur individuellen Datensouveränität, die vorrangig darauf zielt, den Einzelnen wirklich informationell selbstbestimmt sein zu lassen. Die Sensibilität dafür, dass sinnvoller Schutz nicht in übergriffigen Paternalismus ausufern darf, scheint mir jedenfalls zu wachsen.

Neben Transparenz und Datenschutz ist die Frage, wem künftig der öffentliche Raum gehört, ebenfalls ganz entscheidend. Und zwar auf zwei Ebenen. Zum einen im physischen öffentlichen Raum unserer Städte und Kommunen. Wir stehen hier in Technologieprojekten immer wieder vor der Situation, Know-How einkaufen zu müssen, dass wir in der Verwaltung selbst nicht vorhalten können. Mal geschieht dies in Form klassischer Auftragsvergabe, immer häufiger aber auch in PPP-Konstruktionen, in denen Private einen Teil der Gewährleistung der Infrastruktur in eigener Verantwortung übernehmen.

Es ist wichtig, dass wir souverän in der Lage festlegen, wann wir welchen Weg gehen wollen. Die Konsequenz der Digitalisierung der Stadt darf schließlich keine unreflektierte und schleichende Privatisierung des öffentlichen Raumes sein. Wann hier welches Modell der Zusammenarbeit sinnvoll ist, müssen demokratisch legitimierte Instanzen entscheiden können.

Um diesen Prozess der Reflektion voranzubringen, schaffen wir ein Digital City Science Lab an der HafenCity Universität. Dort sollen Hochschulen, Unternehmen und staatliche Strukturen zusammenkommen und einen Plan für die Digitalisierung der Stadt entwickeln.

Zum anderen geht es um den öffentlichen Raum im Sinne der gesellschaftlichen Kommunikationssphäre, auf die unsere Demokratie unabdingbar angewiesen ist. Auch hier verändern sich die Strukturen durch das Auftreten neuer digitaler Anbieter weitgehend.

Wo früher Medienhäuser und Publikum in direktem Austausch standen, haben sich neue Intermediäre etabliert, die Inhalte kuratieren und dabei helfen, das vermeintlich richtige und relevante Angebot zu finden. Das bedeutet aber auch, dass sie zunehmend Einfluss darauf haben können, welche Vielfalt an Information gesellschaftlich zur Verfügung steht und was davon überhaupt noch bei uns ankommt.

Die politische und gesellschaftliche Debatte, die wir hier im Moment immer noch führen, dreht sich zu sehr um das „an sich" dieser Intermediä-

re und viel zu wenig um das „für sich“. Viel zu viele versuchen zu erläutern, warum hier vermeintlich ein strukturelles Problem entsteht, und viel zu wenige versuchen, zu klären, welche Regeln wir brauchen, um die neuen Funktionen dieser Intermediäre gesellschaftlich gewinnbringend zu nutzen.

Wir sind hier politisch gefragt, Spielregeln zu entwickeln, die einerseits eine freie und liberale Öffentlichkeit nach wie vor ermöglichen und die andererseits Diskriminierung und Einschränkungen von Vielfalt verhindern.

Die neuen Macht- und Verantwortungsstrukturen der digitalen Gesellschaft werden nichts vollkommen Neues sein, sondern sich aus dem entwickeln, was wir schon kennen.

Angesichts der durch die Digitalisierung ebenfalls weiter beförderten Trends der Individualisierung und der Globalisierung werden wir aber stärker als in der Vergangenheit Modelle entwickeln müssen, die nicht von einem einzigen steuernden Zentrum ausgehen, sondern die eine Vielzahl von Verantwortlichkeiten miteinander vernetzen.

In diesem Sinne ist die Netzwerkgesellschaft auch mehr als eine bloße Metapher für eine Gesellschaft, die ihre Kommunikation über das Internet erledigt.

Der Begriff beinhaltet vielmehr auch die Erkenntnis, dass wir in modernen digitalen Gesellschaften Strukturen von Governance bauen müssen, in denen klare Rahmenbedingungen und Prinzipienvorgaben ebenso selbstverständlich sind wie weite Verantwortungsspielräume für Unternehmen und Zivilgesellschaft. Anders werden wir der Disruptionen des digitalen Zeitalters nicht Herr werden. Regierung und Parlamente werden sich nicht aus der Führungsaufgabe für die Gesellschaft zurückziehen. Im Gegenteil: Dort, wo allgemeinverbindliche Regeln identifiziert, formuliert und durchgesetzt werden müssen, ist Politik unerlässlich. Hier übt sie demokratisch legitimierte Macht aus.

Politik konnte noch nie dezisionistisch quasi im Alleingang eine gesellschaftliche Ordnung festlegen. Das passt schon gar nicht zu den veränderten Konzepten von Transparenz, Individualität und Öffentlichkeit, die die digitale Gesellschaft prägen. Weil aber die Frage nach der Durchsetzung der demokratisch gewollten Machtstrukturen der digitalen Gesellschaft letztlich auch technologisch beantwortet wird, müssen wir uns gemeinsam darum kümmern, dass wir auch selbst über relevante digitale Werkzeuge verfügen.

Die Plattformen der digitalen Gesellschaft stammen weit überwiegend nicht aus Deutschland und Europa. Oftmals sind wir lediglich noch Anwender anderweitig entwickelter Technologien.

Das dürfen wir auf die Dauer nicht zulassen. Wir müssen daher auch die Rahmenbedingungen dafür schaffen, dass Innovation und Wachstum deutscher und europäischer Anbieter möglich sind und gefördert werden.

Mit Blick auf die Bedeutung der Digitalisierung unserer gesellschaftlichen Kommunikation, unserer wirtschaftlichen Prozesse und unseres öffentlichen Raumes stehen wir gemeinsam in der Pflicht, eigene Digitalkompetenz aufzubauen und damit die Grundlage für unternehmerische Innovation zu schaffen.

Wir müssen in der Lage sein, auch aus unserem Kulturkreis heraus digitale Anwendungen und Applikationen zu entwickeln, die uns eine Gestaltung der digitalen Gesellschaft nach unseren Vorstellungen – zum Beispiel in den Bereichen Datenschutz, Transparenz, Öffentlichkeit – ermöglichen.

Auch das ist eine Aufgabe, der sich die Politik der digitalen Gesellschaft stellen muss. Das bedeutet dann allerdings auch, dass wir die vor uns liegenden Fragen auch als wirtschaftspolitische begreifen und dass wir die Unternehmen in diesen Bereichen anhalten, in die Entwicklung neuer Angebote zu investieren, um unsere Gesellschaft wei- ter voranzubringen. Möglich ist das.

Ein Beispiel ist das Projekt der Hamburg Open Online University, das die hiesigen staatlichen Hochschulen gemeinsam entwickelt haben, um ihre Lehr- und Lernangebote auch in digitale Kontexte hinein weiterzuentwickeln.

Im Universitätssektor droht eine Situation, in der ebenfalls wenige globale Plattformen bestimmen, welche Hochschulangebote wo verfügbar sind. Wir haben deshalb einen strategischen Prozess in Hamburg begonnen, in dem die Hochschulen sich selber der neuen digitalen Möglichkeiten bemächtigen und Angebote für Studierende entwickeln, die besser und attraktiver sind als die bisherigen und die zugleich bestehen können in einem völlig neuartigen Wettbewerb.

Die öffentlich finanzierten Hochschulen haben hier hervorragende Möglichkeiten mit ihren Inhalten, die sich eben nicht noch einmal am Markt monetarisieren müssen, hier ganz eigenständige hochwertige Angebote zu machen.

Ich wünsche mir, dass wir in Hamburg mit solchen und weiteren Projekten ein Laboratorium der digitalen Moderne sind.

Mit dem modernsten und digitalsten Haus Europas am Mittelweg.

Mit einer vernetzten städtischen Infrastruktur.

Mit innovativen technologieaffinen Unternehmen.

Und mit der gemeinsamen Leidenschaft, diese neuen Möglichkeiten anzunehmen und daraus etwas zu entwickeln.

Der Kaufmannsgeist und der Bürgerstolz der Hamburgerinnen und Hamburger sind angesichts dieser großen Aufgabe geweckt.

Wir werden etwas daraus machen. Schönen Dank.

*Olaf Scholz*

Erster Bürgermeister der Freien und Hansestadt Hamburg

# Stand der Diskussion um die EU-Datenschutzgrundverordnung[1]

*Jan Philipp Albrecht*

Für uns alle ist ein solches Projekt letztlich etwas, bei dem man sehr viel dazulernt. Denn hier geht es um das Grundrecht auf Datenschutz für alle Bürger in der Europäischen Union sowie – und das gehört eben auch dazu, weil es in der ursprünglichen Gesetzgebung der Europäischen Union so vorgesehen ist – um den freien Verkehr personenbezogener Daten im europäischen Binnenmarkt. Es geht in dieser EU-Verordnung also um substantielle Fragen und Regeln und nicht um kleinteilige Punkte.

Ich persönlich bin davon überzeugt, dass die Datenschutzgrundverordnung in der Art, wie wir sie vorliegen haben und wie wir sie am Ende verabschieden werden, die größte, realistisch greifbare Förderungsmaßnahme ist, die dem Gesetzgeber zur Verfügung steht, um Vertrauen und Sicherheit im Internet zu erreichen und gleichzeitig eine ordentliche Förderung für das Potenzial der europäischen Unternehmen zu erzeugen.

Ich glaube, dass vielen dieses nicht 100-prozentig bewusst ist. Natürlich ist eine EU-Verordnung zunächst mal ziemlich schwer greifbar und sie befindet sich auch in einem Umfeld, in dem wir über ganz viele Maßnahmen diskutieren. Aber wir haben uns sehr lange in der Situation befunden, nur zu beschreiben und haben selten tatsächlich Schritte geliefert, vor allem gesetzgeberische Schritte, um das Beobachtete auch tatsächlich in Bahnen zu lenken. Nur dadurch aber kann für die Zukunft ein vertrauensvoller Rahmen für die Verbraucher, für Unternehmen, für Behörden und für alle Teilnehmer des Lebens im digitalisierten Raum geschaffen werden.

Die Datenschutzgrundverordnung – ich finde eigentlich das Wort „Grund“ kann entfallen – die Datenschutzverordnung ist ein großer Wurf. Ich bin immer noch dankbar, dass die erste Kommissarin der Europäischen Union für Grundrechte dieses Projekt auf den Weg gebracht hat. Viviane Reding, die jetzt wie ich Abgeordnete im europäischen Parlament ist, hat den Vorgang in der letzten Legislaturperiode relativ zügig nach dem Inkrafttreten des Lissabon Vertrages auf den Weg gebracht. In die-

1 Übertragung der Originalrede vom 7. Mai 2015 in Schriftdeutsch.

sem Vertrag wird in Art. 16 explizit der Datenschutz als ein Auftrag für die Europäische Union formuliert. Übrigens ist dort auch festgeschrieben, dass es ein Grundrecht ist.

Damit ist das geschaffen worden, worüber wir auch lange in Deutschland diskutiert haben: Dieses Grundrecht auf informationelle Selbstbestimmung in unseren Verfassungstext sichtbar lesbar einzubringen. Über die Grundrechte-Charta der Europäischen Union und auch über EU-Vertrag ist dies geschehen.

Damit ist ein Stück weit die Frage beantwortet, warum die Datenschutzverordnung die größte realistisch greifbare Maßnahme in der Form ist, in der sie vorgeschlagen wurde. Denn sehr viele Gedanken und Debatten, die man sich in diesem großen Umbruch machen könnte, passen nicht unbedingt in den Rahmen dessen, was wir uns als gesellschaftliche Grundlage gegeben haben. Die Frage zum Beispiel, ob man sich davon verabschieden soll, dass wir als Individuum weiter ein Mitspracherecht bei der Frage haben müssten, welche personenbezogenen Daten von uns für welche Zwecke verarbeitet werden, stellt sich im jetzt geltenden deutschen Verfassungsrecht und in der Europäischen Union nicht.

In Art. 8 der Grundrechte Charta steht relativ klar, dass die Datenverarbeitung von personenbezogenen Daten nur auf Grundlage der Einwilligung des Betroffenen oder einer gesetzlich konkret gegebenen Gesetzesgrundlage erfolgen kann. Genau das ist letztendlich der Auftrag dieser Datenschutzverordnung, die diese jetzt gesetzgeberisch erfüllen soll. Sie soll deutlich machen, wie diese Einwilligung des Betroffenen bei der Bearbeitung von personenbezogenen Daten erfolgen kann. Sie soll festlegen, wie die gesetzlichen Grundlagen aussehen, wo wir die Datenverarbeitung gesellschaftlich für sinnvoll erachten oder ermöglichen wollen. Und sie soll auch festlegen, unter welchen Bedingungen die Individuen, deren Daten verarbeitet werden, Rechte haben – zum Beispiel das Recht auf Auskunft, das Recht auf Löschung, Korrektur und auch das Recht, informiert zu werden bei der Datenverarbeitung.

Außerdem ist sie jetzt realistisch greifbar, weil wir nicht am Anfang stehen bei dieser Reform. Seit dem Lissabon Vertrag – das war im Dezember 2009 – diskutieren wir im Grunde genommen auch über das Gesetzgebungsverfahren und sind einen guten Schritt vorangekommen. Wir haben im europäischen Parlament dazu sehr breite Verhandlungen geführt.

Meine Aufgabe war es, am Ende tatsächlich um die 4000 Änderungswünsche der Abgeordneten des europäischen Parlaments auf einen Text zu bringen und möglichst eine breite Mehrheit dafür zu finden. Im europä-

ischen Parlament ist es so, dass man eigentlich – wenn man es mit einem Gesetz ernst meint – nicht nur eine knappe Mehrheit dafür gewinnen sollte. Denn das Europarecht – darüber kann man auch streiten – sieht immer noch vor, dass sowohl das europäische Parlament als auch der Ministerrat sich auf einen Text einigen müssen. Wenn das europäische Parlament mit knapper Mehrheit etwas beschließt, ist das natürlich nicht unbedingt die stärkste Verhandlungsposition.

Am Ende hatten wir trotz dieser großen Anzahl von Änderungsanträgen eine Zustimmung von etwa 97 % für den Text in der ersten Lesung im europäischen Parlament. Man zeige mir ein anderes Parlament in einer Demokratie, in der das mal geschafft wurde. Da saßen tatsächlich auch EU-Skeptiker und griechische Kommunisten, die dem gleichen Text zugestimmt haben. Das finde ich schon bemerkenswert. Ich glaube, dass es deswegen richtig ist, zu sagen, dass wir hier nicht am Anfang der Debatte stehen, sondern schon ein ganz schönes Stück zurückgelegt haben.

Es besteht die Chance, in absehbarer Zeit ein solches Gesetz auf den Weg zu bringen. Der Ministerrat hat leider etwas länger gebraucht. Das ist ein bisschen auch der Grund weshalb ich leise Kritik an der Art und Weise, wie wir in Europa Politik machen, äußere. Ich sehe nämlich eine gewisse Gefahr in der Gleichberechtigung von Parlament und Ministerrat. Gerade in dieser Transformationsphase müssen wir schnell und zügig Diskussionen gesellschaftlich zum Abschluss bringen. Es sollte keine Ersatzdebatte in einem Ministerrat stattfinden – sozusagen unter dem Deckmantel der Subsidiarität. Die Debatte sollte im europäischen Parlament, in der Volksvertretung, stattfinden.

Ich glaube, darüber muss man sich Gedanken machen. In jedem Fall versuchen wir es in einem zügigen Verfahren zum Abschluss zu bringen. Der Ministerrat hat es unter großer Anstrengung trotzdem geschafft, eine Ausgangsposition zu erreichen, bei der bis zur nächsten Tagung des Justiz- und Innenrates ein so genannter General Approach, eine generelle Ausrichtung, tatsächlich vorliegt. Dafür zolle ich den Beteiligten meinen Respekt. Also könnten wir nach Verhandlungen zwischen Parlament und Ministerrat ein solches Gesetz möglichst bis Ende des Jahres auf den Weg bringen.

Wenn wir es schaffen, diese Einigung zu erzielen – dann sieht die Datenschutzverordnung in allen bisher vorliegenden Texten eine zweijährige Übergangszeit vor, in der sich jeder daran gewöhnen kann. Das gilt für die Verbraucher, damit sie dann merken, es wird ein einheitliches EU-Gesetz auf uns zukommen. Das gilt aber auch für Unternehmen und auch für die

Behörden, damit diese sich an die neue Rechtslage gewöhnen und ihren Alltag und ihre Geschäftstätigkeit und natürlich auch die Frage der Rechtmäßigkeit ihres Handelns darauf aufbauen können.

Wenn wir das also jetzt verabschieden, wird es tatsächlich erst im Jahr 2017 oder 2018 einheitliche europäische Standards geben. Damit wird dann ein Schritt vollzogen, der wahrscheinlich auch schon vor fünf Jahren hätte vollzogen werden können. Die Tatsache, dass Datenaustausch mit dem Entstehen des Internets grenzübergreifend stattfindet, ist nicht neu. Das Internet als Massenmedium musste Mitte der Neunzigerjahre erkennbar dazu führen, dass das so genannte Cloud Computing, die eben nicht klar lokalisierbare Datenverarbeitung, zum Regelfall wird. Der Gesetzgeber hat darauf immer noch nicht reagiert. Einerseits haben wir diesen Umbruch erkannt. Andererseits fehlt es aber noch immer am politischen Mut, entsprechend große Schritte zu gehen.

Natürlich kann es nicht darum gehen, auf den Weg in das digitale Zeitalter schlichtweg alle Werte revolutionär über Bord zu werfen und zu sagen, wir müssen sowieso alles neu denken. Richtig ist es, dass der Blick nach vorne heute wichtiger ist als der Blick nach hinten. Aber richtig ist auch, dass der Blick nach vorne nicht losgelöst von dem sein kann, was wir in den letzten Jahrhunderten in demokratischen Rechtsstaaten entwickelt haben.

Es geht letztlich um Wertefindung in einem Raum, in dem der Nationalstaat nicht mehr in der Lage ist, gemeinsame Werte einheitlich zu regeln. Die Datenschutzgesetzgebung ist meines Erachtens der erste Schritt, die erste Möglichkeit, diese übernationale Werte-Gesetzgebung einheitlich zu gehen.

Sie wird nicht in allen Bereichen des Lebens der richtige Schritt sein. Aber es gibt viele Bereiche – und dazu zählt eben der Datenschutz – in dem dieser Schritt unvermeidbar ist. Das heißt auch, dass natürlich am Ende ein Kompromiss steht. Auch das eine wichtige Erkenntnis, die sich gerade in Deutschland oftmals erst nach langen Diskussionen durchsetzt. Wenn man in einer Europäischen Union, in einem gemeinsamen Binnenmarkt, 28 unterschiedliche Gesetze auf einen Nenner bringt, kann am Ende das Ergebnis nicht genauso aussehen wie die einzelnen 28 Gesetze.

Deshalb wird das Gesetz am Ende nicht so aussehen wie das Bundesdatenschutzgesetz. Ich glaube trotzdem, dass das vielleicht nicht immer nur negativ sein muss. Denn wir alle werden wahrscheinlich zugestehen, dass wir die Weisheit nicht mit Löffeln gegessen haben und alles besser wissen als andere. Man kann voneinander lernen. Für mich ist das Ergebnis, das

das europäische Parlament für die Datenschutzverordnung vorgelegt hat, im Vergleich zum Bundesdatenschutzgesetz sogar ein Fortschritt. Ein Fortschritt vor allen Dingen in zwei Bereichen.

Zum einen müssen wir die Transparenz für den einzelnen stärken. Die Komplexität der technischen Verarbeitung hat seit den achtziger und neunziger Jahren erheblich zugenommen. Damals wurde alles über statische Verarbeitungssysteme geregelt. Heute reden wir über hochdynamische Prozesse, zum Teil sogar über künstliche Intelligenz. Also um Prozesse, die wir nicht mehr hundertprozentig kontrollieren können.

Die Frage, welche Regeln für eine verständliche Transparenz für jedermann tatsächlich Sinn machen, stellt sich besonders. Wir haben in der Datenschutzverordnung dafür gesorgt, dass drei Anknüpfungspunkte geschaffen werden. Das eine ist, wir haben die Zustimmung weiterhin als zentralen verankerten Verarbeitungsgrund mit der Herausforderung, dass sie informiert stattfinden muss.

Der zweite Punkt sind verständliche Datenschutzerklärungen. Zum Beispiel bei den Informationspflichten. Da soll es die Möglichkeit geben, gesetzgeberisch durch technische Standards Symbole zu verankern. Die vermitteln einen schnellen Überblick darüber, welche Art von Daten-Kategorien verarbeitet werden und welche Art von Daten-Verarbeitungsprozessen stattfinden.

Es geht also darum, sozusagen durch Verkehrssymbole wie im Straßenverkehr, den Menschen deutlich zu machen, worauf sie sich einlassen.

Das dritte sind technische Standards. Bisher denken wir immer noch in bekannten Kategorien. Einwilligung ist sozusagen etwas, das man schriftlich auf Papier gibt, oder der Widerspruch ist etwas, wo man etwas durchstreicht. Doch diese Zeiten sind weitestgehend vorbei. Wenn ich mein Mobiltelefon nutze, wenn ich eine App runterlade und benutze oder wenn ich auf einem Browser surfe und einen Internetdienst benutze, werde ich in vielen dieser Fälle nicht mehr explizit bei jeder Nutzung gefragt werden, möchte ich nun dies oder das.

Wir müssen dafür sorgen, dass die Möglichkeit besteht, dass ich selber schon vorher aussenden kann, was ich möchte und was nicht. Da gibt es interessante Entwicklungen auf internationaler Ebene unter dem Stichwort zum Beispiel „Do not track“. Die Möglichkeit also, durch ein standardisiertes Signal zu sagen, ich möchte getrackt werden, etwa um Werbung personalisiert zu erhalten oder nein, ich möchte das nicht.

Die Möglichkeiten, die Zustimmung durch solche technischen Standards zu regeln und auch den Widerspruch müssen ausgebaut werden. Das

macht letztendlich klar, was eigentlich für eine Philosophie hinter dem Datenschutz steht.

Nämlich eine Philosophie, die nicht dafür sorgen soll, dass das Verarbeiten von personenbezogenen Daten verhindert wird. Denn das sieht kein Datenschutzgesetz grundlegend vor, jedenfalls in der Regel. Der Grundsatz ist: Daten können verarbeitet werden, auch personenbezogene Daten können verarbeitet werden. Aber es sind Voraussetzungen dafür zu schaffen. Diese Voraussetzungen wollen wir leichter schaffen. Wir wollen es ermöglichen, indem wir eine besser informierte Öffentlichkeit haben, die in der Lage ist, Verkehrssymbole zu erkennen und ihre Präferenzen, ihre Entscheidungen möglichst frei und informiert abzugeben.

Da wollen wir ansetzen. Das ist ein großer Bereich, den wir im europäischen Parlament gestärkt haben. Ein nächster wichtiger Bereich ist, dass nicht nur für die Verbraucher in der einheitlichen Rechtsordnung dieses Umfeld geschaffen wird, sondern auch für die Unternehmen und für die Behörden. Wir reden ja vor allem über die großen Wachstumschancen, die ohne Zweifel in der Digitalisierung aller Lebensbereiche vorhanden sind. Allen Unternehmen muss klar werden, dass sie im europäischen Markt, der ein gemeinsamer Binnenmarkt ist, sich an die gleichen Standards halten müssen. Damit sie wissen, woran sie sich zu halten haben und wissen, worauf sie sich einlassen können. Das wäre meines Erachtens einer der größten Erfolge für die europäischen Unternehmen. Denn das beseitigt einen der beiden großen Gründe, warum der europäische IT-Markt, die europäische digitale Wirtschaft hinter denen des US-Markts hinterherhinkt.

Es geht nicht, dass man einen gemeinsamen Binnenmarkt geschaffen hat, aber 28 unterschiedliche Regeln erlaubt für die Verarbeitung von personenbezogenen Daten. In einer vernetzten Welt, in der es letztendlich darum geht, dass ich nur einen Internetzugang brauche, um meine Dienste anzubieten, hat derjenige, der gehalten ist, an einem bestimmten Standort zu bleiben, einen erheblichen Nachteil gegenüber denjenigen, die den Standort in diesem gemeinsamen Binnenmarkt schnell wechseln können. Das ist in der Industrie ein Problem, aber das ist im digitalen Markt ein Riesenproblem.

Im digitalen Markt kann so etwas innerhalb von wenigen Stunden passieren. Es ist ohne weiteres möglich, dass ich mir aussuchen kann, für welche Verarbeitungsprozesse ich in welches Rechtssystem innerhalb dieses gemeinsamen Binnenmarktes gehe. Das ist ein unfassbarer, unverantwortlicher Zustand, der dazu führt, dass wir nicht unsere Stärken in der Europäischen Union und unsere Stärken in unserem unternehmerischen

Antrieb und Geist subventionieren. Stattdessen subventionieren wir diejenigen, die es schaffen, sich mobil im europäischen Markt ihre Regeln heraus zu picken. Das sind vor allem diejenigen, die von außen auf den europäischen Markt kommen.

Der zweite Grund, warum die digitale Wirtschaft in Europa hinterherhinkt, hängt mit Folgendem zusammen. Wir waren nicht in der Lage, in den vergangenen Jahren unsere Stärken zu unterstützen. Wir haben eine Marktsituation, dass Behörden und andere Dienstleister, die Produkte kaufen, nicht darauf achten, dass zum Beispiel ihre IT-Systeme kontrollierbar sind. Dass zum Beispiel Aufsichtsbehörden in der Lage sind, die Algorithmen und die unter der Oberfläche liegenden Programmcodes danach zu überprüfen, ob sie rechtskonform sind. Das ist sowohl für die Wettbewerber in einem europäischen Markt untragbar als auch für die Bürger und für einen Rechtsstaat.

Um es ganz konkret zu machen: Wenn in Hamburg auf den Behörden-Computern ein Betriebssystem installiert ist, bei dem klar ist, dass der Anbieter nicht erlaubt, dass man in bestimmte Bereiche des darunter liegenden Codes hereingucken kann, dann kann diese Behörde nicht sicherstellen, dass der Grundsatz der rechtsstaatlichen Bindungen an Recht und Gesetz gewährleistet wird. Deswegen ist es ein untragbarer Zustand. Doch wir lassen diesen Zustand bestehen, nicht nur auf Kosten des Rechtsstaats und seiner Bürger, sondern auf Kosten der Wettbewerber, die uns genau das liefern würden.

Unter anderem zum Teil hier in Hamburg ansässige Unternehmen, die in der Lage sind, gleichwertige Angebote zu leisten wie globale Player, deren Angebot implementiert die europäischen Sicherheitsstandards und Datenschutzstandards im Design. Doch wir greifen diese Chance nicht auf. Ich glaube, dass das in der Europäischen Union ein Riesenfehler war.

Wir brauchen einen Weg hin zu einer Stärkung unserer Stärken. Wir müssen nicht dafür sorgen, dass im Bereich der EU die gleichen Bedingungen herrschen wie im Wilden Westen. Wir haben hier bei uns eine ganz andere Struktur, eine unternehmerische Struktur – wir haben auch eine andere Mentalität. Wir haben auch kleine und mittelständische Unternehmen, die die IT-Wirtschaft in Europa tragen. Das sind keine großen Player, die können nicht von heute auf morgen zum europäischen Google gemacht werden. Doch wir müssen auf diese Struktur bauen und müssen diese Stärken in die Hand nehmen für die kleinen und mittelständischen Unternehmen und für die breite Masse der IT- Unternehmen.

Die Datenschutzverordnung ist der wichtigste Schritt, zunächst einmal überhaupt ein sogenanntes level playing zu schaffen, indem sie überleben können und in dem ihre Stärken auch tatsächlich wirken können. Damit das Internet ein vertrauensvoller, sicherer Ort wird.

# Selbstregelung, Selbstregulierung und regulierte Selbstregulierung im digitalen Kontext* **

*Wolfgang Hoffmann-Riem*

## *A. Zur Begrifflichkeit*

Dieser Beitrag handelt von individuell-privater, gesellschaftlicher und hoheitlicher Einwirkung auf die Ausgestaltung von und Teilhabe an digitaler Kommunikation. Ziel ist die Illustration des Verhältnisses von Regulierung und Selbstregulierung anhand einzelner Beispiele.

Die meisten im Folgenden formulierten Überlegungen betreffen die Internetkommunikation. Das Internet ist ein komplexes, weitgehend selbstregulativ funktionierendes sozio-technologisches System.[1] Es besteht zum einen aus einer technologischen Infrastruktur der Vernetzung von Computernetzwerken unter Nutzung des TCP/IP-Protokolls und unter Einsatz digitaler Algorithmen. Zum anderen handelt es sich um eine auf soziales Handeln ausgerichtete Infrastruktur. Hier werden insbesondere menschliches Wissen und menschliche Fähigkeiten zur Produktion und Reproduktion von Kommunikation und zur Interaktion eingesetzt.

---

* Durch wenige Nachweise ergänzte und aktualisierte Fassung des Vortrags auf dem Symposion „Neue Macht- und Verantwortungsstrukturen in der digitalen Welt“ am 8. Mai 2015.

** Ich bin in letzter Zeit verschiedentlich zu Vorträgen zu IT-Fragen eingeladen worden, die zum Teil auch veröffentlicht worden sind oder veröffentlicht werden sollen. Es ist mir praktisch nicht möglich, Spezialfragen zum IT-Bereich zu behandeln, ohne jeweils auf den gegenwärtigen Entwicklungsstand einzugehen und Problemzonen anzusprechen, die für das zu behandelnde Sonderproblem bedeutsam sind. Dies führt notwendig zu Wiederholungen. Davon ist auch dieser Vortrag nicht frei. Mit dem IT-Thema habe ich mich jüngst auch im Rahmen einer größeren, von mir verfassten Monographie befasst, die unter dem Titel "Innovation und Recht – Recht und Innovation" im Mohr Siebeck Verlag 2016 erschienen ist.

1 Zur Bedeutung des Internet als selbstorganisiertes sozio-technologisches System siehe den Beitrag von *C. Fuchs*, The Internet as a Self-Organizing Socio-Technological System, Human Strategies in Complexity Research Paper, abrufbar unter http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan025288.pdf, Suchabfrage am 16.11.2015.

Kennzeichnend für das Internet - wie auch für andere Bereiche digitaler Kommunikation - ist der Wunsch vieler Akteure, möglichst autonom zu handeln. Ihnen geht es um Selbstgestaltung und gegebenenfalls Selbstregelung. Es gibt aber auch Möglichkeiten und Notwendigkeiten von generell wirkenden Regeln, sei es in Gestalt privater/gesellschaftlicher (Selbst)Regulierung oder hoheitlicher Regulierung.

Bisher fehlt eine allseits akzeptierte Begrifflichkeit zur Unterscheidung der Erscheinungen von Selbstgestaltung, Selbstregelung, Selbstregulierung und Regulierung. Angesichts der Vielfältigkeit und der Vernetzungen der Erscheinungen ist es auch schwer, trennscharfe Begriffe zu bilden und eindeutige Definitionen anzubieten. Im Folgenden wird als Orientierungshilfe gleichwohl der Versuch einer begrifflichen Unterscheidung unternommen, um die Vielfalt möglicher Erscheinungen zu verdeutlichen. Es sei aber hinzugefügt, dass es sich lediglich um begriffliche Annäherungen handelt.

Unter *Selbstgestaltung* verstehe ich individuell oder gemeinschaftlich vorgenommene Maßnahmen zur Verwirklichung von Zielen durch eigenes autonomes Verhalten. Produkte der Selbstgestaltung im IT-Bereich sind etwa die von einzelnen Bürgern verbreiteten Mails oder Blogs oder eine kollaborativ erarbeitete Software, aber auch die von den IT-Unternehmen entwickelten und umgesetzten Geschäftsmodelle.

Für solche Aktivitäten gibt es zum Teil von den Betroffenen selbst entwickelte Verhaltensregeln, etwa eigen gesetzte moralische oder ethische Selbstverpflichtungen oder Regeln der an einem Verfahren oder Produkt Beteiligten über die Art ihres Zusammenwirkens. Hierfür benutze ich den Begriff der *Selbstregelung*. Beispiele sind Codes of Conduct (Verhaltenskodices). Durch Selbstregelung können auch Einrichtungen oder Organisationen – etwa Verbände - geschaffen werden, um die Interessen der Mitglieder zu vertreten oder gemeinwohlorientierte Aufgaben durch oder für sie wahrzunehmen.

Soweit gesellschaftliche Regelsetzung nicht nur das Verhalten der an der Regelsetzung Beteiligten beeinflusst, sondern wenn auch andere Personen die Regeln für sich anerkennen und die Regeln insofern generell wirken, verwende ich den Begriff der *gesellschaftlichen Selbstregulierung*. Diejenigen, die die Regeln – etwa technische Standards oder Verhaltensmuster – beachten wollen, können sich rechtlich, etwa durch Vertrag, dazu verpflichten. Die Betroffenen können die Regeln auch rechtlich unverbindlich halten, aber ihre Beachtung wechselseitig erwarten und die Nichtbeachtung kann gegebenenfalls sozial sanktioniert werden, etwa

durch Abbruch von Geschäftsbeziehungen oder durch Reputationsverlust der Regelverletzer.

Der Begriff "Regulierung"[2] wird allerdings meist nur für hoheitliche Interventionen in gesellschaftliche Prozesse genutzt, durch die mit einer spezifischen Zielrichtung in genereller Weise Vorgaben für Verhalten aufgestellt oder Strukturen für die Lösung bestimmter Probleme geschaffen oder funktionsfähig gehalten werden.

Von *hoheitlich regulierter gesellschaftlicher Selbstregulierung (bzw. Selbstregelung)* – kurz: von *regulierter Selbstregulierung/-regelung*[3] – wird gesprochen, wenn Hoheitsträger für die Lösung von Problemen auf die in (relativer) Autonomie erbrachten Ordnungsleistungen der Mitglieder der Gesellschaft vertrauen, aber regulativ darauf hinwirken, dass dabei (auch) Gemeinwohlzwecke beachtet oder gezielt verfolgt werden. Das hoheitliche Hinwirken kann auf höchst unterschiedliche Weise geschehen, etwa in Gestalt von Verhaltensvorgaben oder -anreizen, durch Einrichtung von Strukturen – etwa korporativer Art – oder durch die Ermöglichung und Unterstützung von gesellschaftlichen Funktionssystemen wie dem Markt.

---

2 Zum Begriff hoheitlicher Regulierung vgl. *Eifert*, Regulierungsstrategien, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts. Band I: Methoden, Maßstäbe, Aufgaben, Organisation, 2. Aufl 2012, § 19, Rn. 16 ff. Andere Regulierungsbegriffe sind enger und benennen insbesondere die Sicherung des Wettbewerbs als spezifisches Regulierungsziel, so etwa *Ruffert*, Begriff, in: Fehling/Ruffert (Hrsg.), Regulierungsrecht, 2010, S. 332 ff. Rn 24 f. sowie die Beiträge in Kirchhof/Korte/Magen (Hrsg.), Öffentliches Wettbewerbsrecht, 2014.

3 Zum Begriff und Konzept regulierter Selbstregulierung, aber auch zu unterschiedlichen Gestaltungen und Begriffsverwendungen s. *Voßkuhle*, Regulierte Selbstregulierung – Zur Karriere eines Schlüsselbegriffs, in: Die Verwaltung, Sonderheft „Regulierte Selbstregulierung" 2001, S. 197 ff. und die weiteren Beiträge dieses Heftes. S. ferner, *Eifert* (Fn. 2), Rn. 52 ff. Aus historischer Perspektive s. die Beiträge in Collin et al. (Hrsg.), Regulierte Selbstregulierung in der westlichen Welt des 19. Und frühen 20. Jahrhunderts, 2014. Arten regulierter Selbstregulierung gibt es gegenwärtig in verschiedenen Gegenstandsbereichen. Beispiele für die Vielfalt der Anwendungsfelder finden sich in dem erwähnten Sonderheft „Regulierte Selbstregulierung". S. ferner – statt vieler -: *Thoma*, Regulierte Selbstregulierung im Ordnungsverwaltungsrecht, 2008; *Stockhaus*, Regulierte Selbstregulierung im europäischen Chemikalienrecht, 2015.

## B. Zum Entwicklungsstand digitaler Technologien und ihrer Nutzung

Das hier behandelte Feld digitaler Kommunikation ist nicht zuletzt dadurch gekennzeichnet, dass die Entwicklung sehr dynamisch verläuft und immer neue Erscheinungsformen digitaler Kommunikation sowie damit verbundene Chancen und Risiken eintreten und je unterschiedliche Gestaltungs- und Regelungsbedarfe auslösen (können). Auch in rechtswissenschaftlichen Analysen sind unterschiedliche Entwicklungsstränge in den Blick zu nehmen und die vielfältigen Interdependenzen der technologischen Entwicklungen, der ökonomischen Strukturen und der Nutzungsmöglichkeiten zu beachten.

Eine Darstellung der Vielfalt an Möglichkeiten beim Auf- und Ausbau der "digitalen Welt" ist in diesem Beitrag ausgeschlossen. Ich beschränke mich auf einige beispielhafte Schlagworte:

- Computerisierung und Digitalisierung der Kommunikation;
- Mobilität digitaler Kommunikation und die Möglichkeit der Informationsverarbeitung praktisch an jedem Ort und zu jeder Zeit ("Ubiquitous Computing");
- neue Möglichkeiten arbeitsteiliger Zusammenarbeit ohne Bindung an einen bestimmten Raum, etwa durch Crowdworker oder Clickworker;
- Speicherung von Daten auf fremden Computern irgendwo ("Cloud Computing");
- Computerisierung der Herstellung und Distribution von Produkten und Dienstleistungen sowie die Vernetzung und automatisierte Steuerung etwa von Produktionsstätten, von Geräten in Haushalten oder von Kraftfahrzeugen (Internet der Dinge);
- Vernetzung informationstechnischer softwareverarbeitender Systeme mit denen der industriellen Produktion und Distribution und mit der Fähigkeit zur Selbstoptimierung, Selbstdiagnose und Selbstkorrektur (Industrie 4.0);
- Verfügbarkeit gewaltiger Mengen von Daten unterschiedlicher Art, Qualität und Herkunft, verbunden mit der Möglichkeit schneller Verarbeitung (Big Data);
- Ausbau künstlicher Intelligenz zur Steuerung digitaler Kommunikation, aber auch zur Auswertung von Big Data und damit Ermöglichung neuer Qualitäten von Prognosen, von Trendermittlungen und der Entwicklung darauf aufbauender Strategien und Kampagnen, etwa zur Be-

einflussung von Werthaltungen, auch des Verhaltens bei politischen Wahlen.

## C. Ergänzende Beobachtungen

Die Beschäftigung mit den technologischen Entwicklungen und ihren verschiedenen Anwendungsfeldern und rechtlichen Folgeproblemen führt in eine Vielzahl unterschiedlicher Problemfelder, von denen hier einzelne ausdrücklich angesprochen werden.

### I. Chancen und Risiken

Die schnelle Entwicklung digitaler Technologien und ihrer Nutzung wird dadurch stimuliert, dass mit ihrer Hilfe vorher ungeahnte Entfaltungsmöglichkeiten für die Menschen, für Unternehmen und für Organisationen entstanden sind und weiter entstehen. Neuartige Problemlösungen werden sichtbar. Auch kann wirtschaftliches Wachstum auf neue Art erzeugt werden. Wird etwa auf den Internetbereich gesehen, so kommen nicht nur die vielen und häufig in schneller Abfolge entwickelten technischen Innovationen in den Blick, sondern auch, dass diese mit vielen kulturellen, gesellschaftlichen, ökonomischen, ökologischen u. ä. Neuerungen verbunden sind, die erhebliche Veränderungen in praktisch allen gesellschaftlichen Bereichen herbeiführen oder doch herbeiführen können.

Die Unterstützung der Entwicklung und Nutzung solcher Chancen, also der Verwirklichung gesellschaftlich als positiv bewerteter Veränderungen, ist auch eine Aufgabe des Rechts. Recht kann insbesondere auch als Innovationsermöglichungsrecht wirken und mithelfen, solche Potentiale auszuschöpfen.

Andererseits sind die neuen Entwicklungen auch mit einer Reihe von Risiken verbunden. Dazu gehört der Befund, dass die durch die neuen Technologien ermöglichten Chancen keineswegs allen Menschen zugutekommen. So gibt es auch Modernitätsverlierer - etwa Personen, die von nachteiligen Wirkungen technologiebedingter Rationalisierungen betroffen sind. Aber auch fast alle Nutzer des Internet können infolge der Nutzung zugleich Risiken ausgesetzt sein, etwa den Risiken von Persönlichkeitsbeeinträchtigungen durch den Umgang Dritter mit den bei der Nutzung anfallenden Daten. Recht muss daher auch in seiner Funktion als

Schutz- und Vorsorgerecht aktiviert werden, aber ebenfalls als Recht zur Abwehr staatlicher Eingriffe.

Dabei ist zu berücksichtigen, dass Risiken im Bereich der digitalisierten Kommunikation nicht nur von Privaten ausgehen können, sondern auch von staatlicher Seite oder von Aktionen, in denen staatliche und private Akteure zu Lasten der Träger von Grundrechten gemeinschaftlich tätig werden – etwa beim Ausspähen von Daten durch Geheimdienste unter (freiwilliger oder rechtlich erzwungener) Mithilfe der IT-Unternehmen.[4]

Zu den Risiken gehören auch Erscheinungsformen der Internet- oder Cyberkriminalität (Cybercrime),[5] der Cyberspionage und -sabotage sowie des Cyberwar.[6] Möglich sind erhebliche Gefährdungen der sozialen und rechtlichen Ordnung sowie der Funktionsfähigkeit existenznotwendiger Infrastrukturen, wie etwa der Energieversorgungs- oder Verkehrssysteme, die in großem Maße von digitalisierter Kommunikation abhängig und deshalb höchst verletzbar sind. Auf dieses Problemfeld kann ich im Folgenden allerdings nur sehr begrenzt eingehen.

## *II. Entgrenzungen*

Viele der neuen Möglichkeiten des Einsatzes digitaler Technologien fügen sich nicht auf einfache Weise in die bisherigen Kategorien der Entwicklung von Technik und des Rechts ein.

Frühere Grenzziehungen – etwa gegenständliche oder territoriale -, sind vielfach nicht oder nicht mehr maßgebend. So verschwimmen im IT-Be-

---

4 Siehe dazu statt vieler *Leisegang*, Schöne neue Überwachungswelt, in: Blätter für deutsche und internationale Politik (8) 2013, 5; *J. Wolf*, Der rechtliche Nebel der deutsch-amerikanischen "NSA-Abhöraffäre". US-Recht, fortbestehendes Besatzungsrecht, deutsches Recht und Geheimabkommen, in: JZ 2011, 1039; *Ewer/Thienel*, Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Datenskandals, in: NJW 2014, 30; *Rottmann*, Totalüberwachung, 2014; *Schaar*, Überwachung total. Wie wir in Zukunft unsere Daten schützen, 2014; 78 ff., *Fox,* TLS, das Vertrauen und die NSA. Wie die NSA die Sicherheitsinfrastruktur des Internet untergräbt, in: DuD 2015, S. 78 ff.

5 Dazu siehe *Reindl-Krauskopf*, Cyber-Kriminalität, in: ZaöRV 2014, S. 563.

6 Dazu siehe *Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, 2014; *P. Shakarian/J. Shakarian/Ruef*, Introduction to Cyber-Warfare, 2013; *Gaycken*, Cyberwar – das Wettrüsten hat längst begonnen, 2012.

reich die Grenzen zwischen Hardware, Software und Orgware[7] ebenso wie die zwischen Dienstleistungen und ihrem Transport mit Hilfe von Kommunikationsinfrastrukturen. Gesellschaftliche und öffentliche Kommunikation werden – wie besonders eindringlich das Internet zeigt – miteinander vermengt. Damit entfallen auch die herkömmlichen Vorstellungen über Privatheit und Öffentlichkeit. Die Technologien und Dienste können durch jedermann, nicht nur durch Private, sondern auch durch staatliche Einrichtungen, genutzt werden - und so weiter.

Vor allem in territorialer Hinsicht ist die Entgrenzung unübersehbar. Die Technologien sind global verfügbar und die Kommunikationsinfrastrukturen, aber auch die mit digitalisierter Technik betriebenen Distributionswege sind transnational und häufig global organisiert. Demgegenüber ist das Recht zum größten Teil national orientiert oder jedenfalls – wie auch das supranationale Recht der Europäischen Union – regional begrenzt. Das ebenfalls wichtige internationale Recht, etwa das Völkerrecht, hat zwar einen weiteren räumlichen Anwendungsbereich, ist aber gegenständlich auf nur einzelne Sektoren bezogen und auch dort lückenhaft.

Die gegenständlichen Entgrenzungen sind eine Herausforderung insbesondere für Rechtsordnungen, die – wie regelmäßig - im Interesse der Handhabbarkeit der Lösung von Problemen im Rahmen des Rechts deren Komplexität möglichst reduzieren wollen, um sie in bestimmten, meist spezialisierten Sektoren der Rechtsordnung in spezifischer Weise bearbeiten zu können. Die territorialen Entgrenzungen erschweren darüber hinaus den wirksamen Einsatz von Recht. Die Kommunikationsinfrastrukturen und Kommunikationsströme sowie Dienste betreffen meist Gebiete mit unterschiedlichen wirtschaftlichen und politischen Ordnungen, mit unterschiedlichen Rechtskulturen, auch mit unterschiedlichen Einstellungen zur Sinnhaftigkeit und Möglichkeit regulativer Einwirkungen usw. Diese Heterogenität führt dazu, dass selbst dort, wo es für den Umgang mit möglichen Problemen defizitären Rechtsgüterschutzes in der je nationalen Rechtsordnung nutzbares Recht gibt oder dort geschaffen werden könnte, es nicht zum wirkungsvollen Einsatz von hoheitlich gesetztem Recht kommt. Oder es bleibt wirkungslos, weil es für die Unternehmen erhebliche Möglichkeiten des Ausweichens vor regulativen Einwirkungen gibt, die von ihnen auch genutzt werden.

---

7 Zu der letzteren zählen etwa Benutzerhandbücher, Anforderungen an die IT-Sicherheit oder an IT-Projekte und die Methoden ihrer Abwicklung.

Solche Umstände – aber auch die sogleich zu behandelnden Besonderheiten der Netzwerkökonomie – sind mitursächlich dafür, dass in digitalen Kontexten privat-gesellschaftliche Selbstregelungen und -regulierungen erheblich bedeutsamer sind als hoheitlich gesetztes Recht. Hoheitsträger nutzen allerdings auch Möglichkeiten, die private Selbstregelung/-regulierung rechtlich-regulativ zu umhegen, zumindest dafür zu sorgen, dass die jeweils geltende Rechtsordnung ihre Schutz- und Ermöglichungsfunktionen in den im Übrigen selbstregulierten Bereichen nicht völlig einbüßt.

## *III. Marktentwicklungen – Besonderheiten der Internetökonomie*

Der Versuch hoheitlicher rechtlicher Einwirkung auf den IT-Bereich muss den schon erfolgten und vermutlich weiter voranschreitenden Aufbau erheblicher Marktmacht (die Oligopolisierung wichtiger Bereiche durch Unternehmen wie die „Big Five" Google, Facebook, Microsoft, Amazon und Ebay) einkalkulieren. Die Marktmacht wird von diesen Unternehmen auch genutzt, um in großem Umfang die eigene Betätigung möglichst nur selbstregulativ zu gestalten und/oder hoheitlicher Regulierung möglichst auszuweichen.

Um Ursachen für die Entstehung solcher Marktmacht verstehen zu können, ist ein Blick auf die ökonomischen Strukturen im Internet hilfreich. Dabei begrenze ich mich in dem folgenden Exkurs auf einzelne typische Bestimmungsfaktoren für die Entstehung von Marktmacht.

Für die Internetökonomie[8] haben die Wirtschaftswissenschaftler Besonderheiten in den Marktstrukturen herausgearbeitet, die sich vor allem auf drei Themenfelder beziehen.

Gegenstand ökonomischer Betätigung sind sogenannte Informationsgüter. Mit ihnen sind Netzwerkeffekte verbunden.[9] Für diese Güter ist typisch, dass selbst bei hohen Fixkosten ihrer Erstellung die Durchschnittskosten der Informationserzeugung und –vervielfältigung unendlich fallen, da nur geringe variable Kosten entstehen und die Güter sich beim Konsum nicht oder praktisch nicht verbrauchen. Erfolgt die Nutzung von Netz-

8 Zu ihr siehe *R. Peters*, Internet-Ökonomie, 2010; *Clement/Schreiber* Internet-Ökonomie. Grundlagen und Fallbeispiele der vernetzten Wirtschaft, 2013.

9 Zu ihnen siehe statt vieler *Engert*, Regelungen als Netzgüter. Eine Theorie der Rechtsvereinheitlichung und Vertragsrecht, in: AcP 2013, S. 321, m. w. Hinw. auf wirtschaftswissenschaftliche Literatur und Probleme rechtlicher Regulierung.

werkgütern über Kommunikationsnetze – hier die der Telekommunikation -, ist ferner von Bedeutung, dass diese Güter für die Konsumenten und vor allem für die Unternehmen selbst einen umso höheren Nutzen haben, je größer die Zahl derjenigen ist, die bereits mit dem Netz verbunden sind und es nutzen. Hier spricht man von den direkten Netzeffekten, die erfolgreichen Unternehmen exponentielle Wertsteigerungen ermöglichen. Hinzu können indirekte Netzeffekte treten, die nicht durch unmittelbare Kommunikationsbeziehungen entstehen, sondern durch die Einschaltung Dritter – etwa Unternehmen der Werbewirtschaft –, die ebenfalls erhebliche Vorteile bei steigenden Konsumentenzahlen haben. Netzgüter ermöglichen sogenannte Skalenvorteile.

Erfolgreiche Unternehmen haben – dies ist der zweite Aspekt – Aussicht auf besonders hohe Gewinne und in der Folge die Möglichkeit, mit ihrer Hilfe in benachbarte oder weiter entfernte Tätigkeitsbereiche vorzudringen und auf diese Weise die Marktposition wechselseitig zu verstärken (Konglomerateffekte[10]). Die Kombination verschiedener Produkte und Dienste kann deren Wert für die Nutzer erhöhen, sie kann aber auch zu Marktverschließungen führen mit der Folge, dass Wettbewerb unterbunden wird.

Der dritte wichtige Effekt ist die Mehrseitigkeit der Märkte,[11] nämlich die Möglichkeit der Verknüpfung der Tätigkeiten unterschiedlicher Akteure mit unterschiedlichen Betätigungsfeldern. So können Plattformbetreiber, Konsumenten, Werbetreibende und Content-Provider in aufeinander bezogenen unterschiedlichen Betätigungsfeldern tätig werden und es gibt Möglichkeiten, ökonomische Austauschbeziehungen in asymmetrischer Weise auszubilden.

Dies lässt sich besonders gut in dem Dreiecksverhältnis zwischen einer Suchmaschine, den Nutzern und den Werbetreibenden beobachten. Im Bereich des Internet hat es sich eingebürgert, dass viele Leistungen scheinbar unentgeltlich erbracht werden, das heißt ohne eine in Geld ausgedrückte Gegenleistung der Nutzer. Diese erbringen gegenüber dem Suchmaschinenbetreiber allerdings durchaus Gegenleistungen, und zwar schon dadurch, dass sie den Angeboten Aufmerksamkeit zuwenden. Ferner eröff-

10 Vgl. etwa dazu Monopolkommission, Hauptgutachten XX, 2014, S. 63.

11 Allgemein dazu siehe *Reiss/Günther*, Mehrseitige Märkte: Paradigmenwechsel vom Markt- zum Netzwerk-Ansatz, in: Wirtschaftswissenschaftliches Studium (39) 2010, S. 176; *Cennano/Santaló*, Platform competition: Strategic trade-offs in platform markets, in: Strategic Management Journal 2013, S. 1031.

nen sie den Unternehmen die Möglichkeit, die beim Kommunikationsvorgang anfallenden Daten, gegebenenfalls auch die in den Kommunikationsinhalten auffindbaren Informationen, zu speichern und für die Optimierung des eigenen Angebots oder für andere Zwecke zu verwerten, darüber hinaus aber auch an Dritte weiterzugeben, etwa entgeltlich zu veräußern.

Soweit – wie etwa in sozialen Netzwerken üblich – die Dienste mit begleitenden Werbemaßnahmen verbunden sind, wird die Aufmerksamkeit der suchenden Nutzer zugleich auf die Werbebotschaften gelenkt, so dass den werbetreibenden Unternehmen Werbungschancen eingeräumt werden. Dafür leisten die Werbeunternehmen ein Entgelt an das IT-Unternehmen

Die beim Nutzungsvorgang anfallenden Verbindungs- und Inhaltsdaten haben offenbar – wie beispielsweise an den immensen Gewinnen bei dem Einsatz der Suchmaschine Google ablesbar ist – einen hohen Wert, für den aber nicht die Nutzer entgolten werden. Immerhin können sie die Dienste entgeltfrei nutzen.

Aufgrund dieser – hier nur vereinfacht dargestellten – ökonomischen Besonderheiten ist es den erwähnten „Big Five" gelungen, eine marktbeherrschende, oligopolistische Stellung aufzubauen. Aufgrund der Besonderheiten der Netzökonomie können Machtpositionen gefestigt und mit Hilfe der hohen Gewinne immer weiter ausgebaut werden, so dass Chancen einer Korrektur über Marktkräfte kaum bestehen.

## *D. Selbstgestaltung –Selbstregelung - Selbstregulierung – gesellschaftlich oder hoheitlich regulierte Selbstregulierung[12] (Beispiele)*

Solche und weitere Rahmenbedingungen haben dazu geführt, dass Selbstgestaltung, Selbstregelung und Selbstregulierung die vorherrschenden Arten der Ausgestaltung der IT-Infrastrukturen und der Abwicklung und Nutzung der Dienste sind.

Das gilt insbesondere für den Internetbereich. Die Befassung mit der Entwicklung des Internet ergibt, dass das Internet von Anfang an in hohem Maße auf weitgehend autonome Selbstgestaltung und Selbstregulierung der Akteure vertraut hat.[13] Zwar hat das Internet in der Phase seiner

12 Als Einführung in Fragen der Selbstregulierung und ihrer hoheitlichen oder gesellschaftlichen Regulierung s. *Eifert*, (Fn. 2), Rn. 52 ff., 144 ff. – jeweils m.w. Hinw.

13 Zur Geschichte des Internet s. statt vieler *Abbate*; Inventing the Internet, 1999; *Hafner/Lyon*: ARPA KADABRA oder Die Geschichte des Internets, 2000.

Entstehung hoheitliche Geburtshelferdienste durch das amerikanische Militär und amerikanische Hochschulen erfahren und es gibt auch weiterhin begrenzte Kooperationen mit staatlichen Stellen bei der Entwicklung des Internet. Insbesondere nach seiner in den 1990er Jahren erfolgten weitgehenden Kommerzialisierung ist der staatliche Einfluss auf seine Gestaltung jedoch marginalisiert worden. Gegenwärtig unterliegt die Entwicklung des Internet weitestgehend privaten, insbesondere unternehmerischen Entscheidungen.

## *I. Private Selbstgestaltung/Selbstregelung*

In der Bundesrepublik Deutschland ist die auch grundrechtlich abgesicherte Rechtsmacht zur autonomen Gestaltung des eigenen Handelns durch Einzelne und Gruppen ein tragendes Element des Rechtsstaats. Die Grundrechte der allgemeinen Handlungsfreiheit oder der Berufs- und Eigentumsfreiheit, aber auch der Meinungs- und Medienfreiheit (Art. 2, 12, 14 und 5 GG) sind im deutschen Recht Konkretisierungen des Autonomiegrundsatzes und damit der Rechtsmacht zur Selbstgestaltung. Vergleichbares gilt in anderen rechtsstaatlichen Ordnungen, etwa in den EU-Staaten oder den USA.

Eigenverantwortung haben die Unternehmen dementsprechend für die Gestaltung von Geschäftsmodellen im Internetbereich. Da es keine global wirksamen hoheitlichen Regelungsstrukturen für die Dienste im Internet gibt, sind die Möglichkeiten der Unternehmen zur autonomen Gestaltung besonders groß. Dort, wo die Unternehmen ihren Geschäftssitz oder eine Niederlassung haben oder ihre Geschäfte abwickeln, sind sie allerdings an die jeweils maßgebende nationale Rechtsordnung gebunden, für den Bereich der EU auch an die Europäischen Verträge und ergänzende Verordnungen und Richtlinien.[14]

In den Autonomiebereich fällt insbesondere die Entwicklung der eigenen Geschäftsmodelle und dabei auch die Gestaltung der Beziehungen zu den Nutzern von Diensten. Dies geschieht zum Teil durch als Selbstbin-

14 Zur Rechtsbindung s. EuGH, Urteil Google Spain und Google, C-131/12, EU: C: 2014: 317 = EuGRZ 2014, 320 ff. S. ferner Art. 2, 3 der – allerdings erst im Jahre 2018 maßgeblichen - EU-Datenschutzgrundverordnung vom 27. April 2016; Verordnung (EU) 2016/679; deutsche Fassung: Amtsblatt der EU L 119/1 vom 4. Mai 2016.

dung formulierte, aber rechtlich gegenüber den Nutzern nicht verbindliche Verhaltensgrundsätze u.ä. Ein Beispiel sind die sog. Facebookgrundsätze.[15] Besonders wichtig sind die von den Unternehmen aufgestellten Allgemeinen Geschäftsbedingungen; auf sie wird näher unten (VI) eingegangen.

Autonomie prägt auch die technische Ausgestaltung und Steuerung der Infrastrukturen und Dienste. Dies gilt insbesondere für die Entwicklung der digitalen Algorithmen oder allgemeiner des in die Architektur und Normungen des Internet eingeschriebenen „Code".[16] Algorithmen, also technische Regeln, steuern auch die über das Internet abgewickelten Dienste. Derartige Algorithmen werden von den Unternehmen in eigener Verantwortung entwickelt und eingesetzt. Sie werden grundsätzlich als Geschäftsgeheimnisse behandelt und unterliegen keinen Anforderungen an Transparenz oder Kontrollierbarkeit. Allerdings müssen bei der Entwicklung und dem Einsatz der Algorithmen rechtliche Vorgaben – wie etwa die des Datenschutzrechts – beachtet werden.

Die algorithmenfundierte Technoregulierung wird beispielsweise für das Profiling eingesetzt, also für die automatisierte Verarbeitung personenbezogener Daten von Nutzern, um bestimmte persönlich Aspekte (wie Vorlieben, Interessen, die wirtschaftliche Lage oder den Aufenthaltsort) zu erfassen, typisierend zu klassifizieren sowie zu analysieren und als Grundlage für Prognosen zu nehmen. Die Ergebnisse dienen dann beispielsweise als Mittel der personalisierten Informationselektion, etwa für Werbeansprachen oder für die Filterung der Suchergebnisse bei Google oder des Newsfeed von Facebook. Mittelbar werden sie dadurch auch bedeutsam für Wahrnehmungen der Nutzer, deren Einstellungen und deren Entscheidungen auch im alltäglichen „Offline-Leben".[17] Ein anderes Beispiel für den Einsatz von Algorithmen ist das Blockieren des Zugangs zu unerwünschten, etwa kinderpornographischen oder rassistischen, Inhalten im Internet.

---

15 Siehe http://www.facebook.com/principles.php.

16 Zu ihm s. *Lessig*, Code Version 2.0, 2006. Zu seiner Auswirkung auf Regulierung und Verhaltenssteuerung kritisch *Hildebrandt*, Smart Technologies and the End(s) of Law, 2016 m. w. Hinw.

17 Dazu vgl. statt vieler *Pariser*, Filter Bubble, 2011; *Lewandowski/Kerkmann/Sünkler*, Wie Nutzer in Suchprozessen gelenkt werden, ferner: *Jürgens/Stark/Magin*, Gefangen in der Filterbubble? Beide in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 75 ff, 99 ff.

Das Internet gewährt nicht nur den Anbietern von Leistungen, sondern auch den individuellen Nutzern erhebliche Möglichkeiten der Selbstgestaltung. In einer spezifisch gesteigerten Weise wird Selbstgestaltung in Bereichen von Open Source[18] und Open Content[19] oder allgemeiner von Open Innovation genutzt. Die dort mögliche und übliche Kollaboration mehrerer ist eine Form kollektiver Selbstgestaltung, eingerahmt durch dafür entwickelte gesellschaftliche Regeln als Formen der Selbstregulierung. Aufgrund solcher Regeln kann das Ergebnis kollaborativer Entwicklungen rechtlich mithilfe der sogenannten Copyleft-Klausel[20] als Leistung derart abgesichert werden, dass diese nicht durch Einzelne zur kommerziellen Verwertung nutzbar ist. Die Copyleft-Klausel nutzt das Instrumentarium des staatlichen Urheberrechtsschutzes, verkehrt aber seine übliche Schutzrichtung, indem die an sich durch das Urheberecht geschützte proprietäre Nutzung für diese kollaborativ geschaffenen Werke selbstregulativ ausgeschlossen wird.

Eine weitere Form privater Selbstregulierung mit allgemeiner Wirkung sind technische Standards, die von einem Unternehmen oder kollaborativ von mehreren entwickelt werden und in einem bestimmten Geschäftsfeld auch von anderen genutzt werden, ohne dadurch aber rechtlich verbindlich zu werden. Sie können sich auf Hard- wie auf Software beziehen. Setzen Standards sich faktisch allgemein durch, wirken sie funktional wie Standards, die förmlich (privat oder hoheitlich) gesetzt werden. Die Standardentwicklung in Gestalt der faktischen Durchsetzung bestimmter Parameter am Markt führt zu deren faktischen Verbindlichkeit. Dies ist eine Form informeller gesellschaftlicher Selbstregulierung. Werden gesellschaftlich gebildete Standards allerdings im hoheitlich gesetzten Recht als maßgebend anerkannt – etwa für Haftungsfragen - oder rechtlich für verbindlich erklärt, erfolgt durch diesen Transfer zugleich eine rechtliche Transformation.

---

18 Dazu siehe *Hartmann/Jansen*, Open Content – Open Access, 2008; *Chesbrough/van Haverbeke/West*, Open Innovation, 2011.

19 Ein Beispiel ist das Internetlexikon Wikipedia. Speziell zur Art der Selbstregulierung beim Persönlichkeitsschutz siehe *Dilling*, Persönlichkeitsschutz durch Selbstregulierung in der Wikipedia, in: ZUM 2013, S. 380 f.

20 Zu ihr siehe *Jaeger/Metzger*, Open Source Software. Rechtliche Rahmenbedingungen der freien Software, 2015, S. 23 ff.

## II. Gesellschaftliche Selbstregulierung

Beispiele für in gesellschaftlicher Verantwortung geschaffene Regeln für gesellschaftliches, autonomes Verhalten sind etwa informelle Regeln des Anstands. Hierzu gehört die in der Anfangszeit des Internet maßgebende Netiquette[21] als Set von Verhaltensregeln für die Internetnutzung. Zur Unterstützung der Wirkungskraft dieser Handlungsform gesellschaftlicher Eigenregulierung wurden Strategien des „Naming and Shaming" genutzt, also die kollektive, wenn auch weitgehend nur informell abgestimmte Ächtung eines von der Community nicht gebilligten Verhaltens.

In den Bereich formeller gesellschaftlicher Regulierung privaten Verhaltens fallen Codes of Conduct, wenn sie von Verbänden entwickelt werden, die ihrerseits deren Beachtung durch die Verbandsmitglieder erwarten und gegebenenfalls die Nichtbeachtung sanktionieren. Ein Beispiel ist der Kodex für Anbieter nutzungsbasierter Online-Werbung des "Deutschen Datenschutzrats Online-Werbung",[22] der freiwilligen Selbstkontrolleeinrichtung der digitalen Werbewirtschaft.

Durch Verbände können auch technische Standards als gesellschaftliche Regulierung gesellschaftlicher Selbstregulierung entwickelt werden, wie etwa IT-Sicherheitsstandards,[23] die zumindest als Empfehlungen angeboten werden, aber auch rechtliche Folgen haben können, etwa für die Beurteilung von Fahrlässigkeit bei der Produktion von Gütern.

Solche im gesellschaftlichen Bereich geschaffenen Regeln haben häufig nicht nur für die Mitgliedsunternehmen der Verbände Bedeutung, sondern können mittelbar auch Wirkungen für Dritte entfalten. Ein Beispiel ist das Robot-Exclusion-Standardprotokoll (REP). [24] Es regelt die Möglichkeit

---

21 Dazu siehe die Netiquette-Guidelines von 1995, abrufbar unter www.ietf.org/rfc/rfc1855.txt, Suchabfrage am 16.11.2015.

22 Zu ihr siehe die Kodizes des Deutschen Datenschutzrats Online-Werbung (DDOW), abrufbar unter www.meine-cookies.org/DDOW/die_kodizies/index.html.

23 So hat der Bitkom-Arbeitskreis Sicherheitsmanagement einen "Kompass der IT-Sicherheitsstandards" (2014) erarbeitet, der insbesondere das Thema "Elektronische Identitäten" behandelt, siehe dazu BITKOM/DIN (Hrsg.), Kompass der IT-Sicherheitsstandards – Auszüge zum Thema Elektronische Identitäten, 2014, abrufbar unter www.bitkom.org/Publikationen/2014/Leitfaden/Kompass-IT-Sicherheitsstandards/140311_Kompass_der_IT-Sicherheitsstandards.pdf.

24 Zum REP siehe *Höppner*, Das Verhältnis von Suchmaschinen zu Inhalteanbietern an der Schnittstelle von Urheber- und Kartellrecht, in. Wettbewerb in Recht und Praxis 2012, S. 625 (631 f., 636 ff.).

der Betreiber von Websites, diese oder Teile davon gegenüber den Web-Crawlern (Robots) zu sperren. So werden Suchmaschinen daran gehindert, diese Inhalte zugänglich zu machen. Obwohl Informationsanbieter regelmäßig daran interessiert sind, dass ihre Internetangebote über Suchmaschinen aufgefunden werden können, kann es auch in ihrem Interesse liegen, dies auszuschließen oder die eigene Leistung von anderen Unternehmen nur gegen Entgelt nutzen zu lassen. Das selbstregulativ geschaffene REP, dem sich verschiedene Internetunternehmen einschließlich Google angeschlossen haben, betrifft die Zugänglichkeit fremder Angebote für Web-Crawler. Es ist nicht das Ergebnis eines Interesseclearing zwischen Vertretern aller Beteiligten, sondern eine einseitige Setzung des mächtigeren Teils der Internetwirtschaft, die erhebliche Auswirkung auf Dritte hat.

### *III. Hybride Regulierung*

Von hybrider Regulierung spreche ich, wenn eine Regelung gesellschaftlich selbstregulativ zustande kommt, aber staatliche Stellen bei der Entwicklung der Regeln und/oder bei der Bestimmung ihrer Relevanz mitwirken. Ich nenne einzelne Beispiele.

Hybrid gestaltet ist die Entwicklung des Datenschutzkodex der Versicherungsunternehmen, der gemeinsam von dem Gesamtverband der Deutschen Versicherungswirtschaft und den deutschen Datenschutzbehörden sowie der Verbraucherzentrale Bundesverband (vzbv) erarbeitet worden ist.[25]

Eine weitere Art hybrider Regulierung findet sich im IT-Sicherheitsgesetz.[26] Dieses reagiert auf Gefahren, die oben (C I) mit den Stichworten Cybercrime und Cybersabotage angesprochen worden sind. Die betroffenen Unternehmen sind zur Schaffung geeigneter technischer und organisatorischer Vorkehrungen für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen und zur Vermeidung von Störungen verpflichtet (§ 8 a Abs. 1). Sie sowie ihre Branchenverbände können Vorschläge für Sicherheitsstandards erarbeiten (§ 8 a Abs. 2). Das Bundesamt für Sicherheit in der Informationstechnik überprüft die Eignung solcher Standards

25 Datenschutzkodex des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV), dem die Versicherungsunternehmen freiwillig beitreten können.

26 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015, BGBl. I vom 24. Juli 2015, S. 1324.

zur Erfüllung der Sicherheitsanforderungen und stellt bei erfolgreicher Prüfung ihre Eignung fest.

Eine wieder andersartige hybride Regulierungsform gibt es bei der Domainvergabe für das Internet. Bei der hierfür geschaffenen Internet Corporation for Assigned Names and Numbers (ICANN).[27] handelt sich um eine Einrichtung der Selbstregulierung durch private Akteure unter – bisher jedenfalls – der Mitwirkung einer staatlichen (konkret: amerikanischen) Aufsichtsbehörde.

Auf dem Zusammenwirken staatlicher und nichtstaatlicher Akteure (Unternehmen, NGOs, technische Communities und Wissenschaftler) beruht das im NETmundial-Multistakeholder-Statement vom 24. April 2014 enthaltene Regelwerk, das zum einen "Internet Governance Principles" und zum anderen eine "Roadmap for the future Evolution of the Internet Governance Ecosystem" enthält.[28] Hier wurden in einem mehr oder minder partizipatorischen Prozess entwickelte Prinzipien aufgestellt, und zwar in Gestalt von Human Rights and Shared Values, aber auch von Forderungen nach kultureller und sprachlicher Diversität, Sicherheit, Stabilität und Resilienz des Internet sowie seiner offenen Architektur. Ziel ist es, Innovation und Kreativität zu schützen. Die "Roadmap" enthält Anregungen zur Umsetzung solcher Prinzipien. Rechtliche Verbindlichkeit besteht nicht. Mögliche Sanktionen für die Missachtung der Prinzipien oder die Nichtbeteiligung an Prozessen ihrer Verwirklichung sind das "Naming and Shaming".[29]

---

27 Zu ICANN siehe *Voegeli*, Die Regulierung des Domainnamensystems durch die Internet Corporate for Assigned Names and Numbers (ICANN), 2006; *Viellechner*, Transnationalisierung des Rechts, 2013, S. 134 ff., 147 ff. Gegenwärtig laufen Bemühungen, den US-staatlichen Einfluss, insbesondere Aufsichtsrechte, abzubauen und ICANN noch stärker selbstregulativ arbeiten zu lassen (s. dazu www.icann.org sowie https://meetings.icann.org/en/dublin54, Suchabfrage am 16.11.2015).

28 Näher dazu *Kleinwächter*, PINGO (2014), p. 5 et seq. http://www.circleid.com/posts/20140510_pingo_net_mundial_adopts_principles_on_internet_governance/

29 Dazu siehe *Kleinwächter*, PINGO (2014), p. 5 et seq. (Fn. 28).

### *IV. Selbstverpflichtungen zur Vermeidung hoheitlicher Sanktionen*

Eine spezifische Kombination von hoheitlicher Einwirkung und der Einflussnahme auf deren Umsetzung findet sich im Bereich zwar rechtlich freiwilliger, aber hoheitlich angestoßener Selbstverpflichtungen.[30]

Im IT-Bereich gibt es solche Selbstverpflichtungen[31] beispielsweise in Reaktion auf Beanstandungen der Kartellaufsicht. Ausgangspunkt sind die von Kartellbehörden im In- und Ausland gegen Internetunternehmen eingeleiteten Kartellverfahren. Ein noch schwebendes gegen Google gerichtetes Kartellverfahren der EU-Kommission betrifft beispielsweis Vorwürfe wegen der Art des Vorgehens von Google bei der (Nicht-)Aufnahme der Informationsangebote Dritter in den Suchmaschinenindex sowie hinsichtlich der Beeinflussung des Rankings von Angeboten auf Suchanfragen, verbunden mit dem Vorwurf, eigene Google-Dienstleistungen nach vorn zu ziehen. Andere Themen sind der Ausschluss von Werbekunden aus dem Werbeangebot sowie die unentgeltliche Verwertung journalistischer Angebote in Gestalt sogenannter Snippets. Schließlich sind auch Ausschließlichkeitsvereinbarungen gegenüber Werbepartnern, Geräteherstellern und Websitebetreibern Thema des Verfahrens.[32]

Solche Verfahren sind in der Vergangenheit häufig durch Selbstverpflichtungen der Unternehmen beendet worden. Das betroffene Unternehmen konnte dadurch Auflagen oder Verbote sowie Geldbußen vermeiden; als Voraussetzung musste es sich aber zu gewissen Änderungen seiner Praxis oder auch zu finanziellen Leistungen verpflichten. Der Vorteil war ein wechselseitiger. Der Hoheitsträger war von häufig schwierigen Nachweisproblemen und den Belastungen eines möglichen anschließenden gerichtlichen Verfahrens befreit, das betroffene Unternehmen konnte seine eigenen Interessen durch die Formulierung der Selbstverpflichtungserklärung im Zweifel besser durchsetzen als bei einer einseitigen hoheitlichen

---

30 Allgemein zu Selbstverpflichtungen siehe statt vieler *Eifert*, (Fn. 2), Rn. 73 ff.

31 Eine Auflistung solcher Verfahren findet sich in: Monopolkommission, (Fn. 10), S. 66 f.; s. auch *Hopf*, Der Missbrauch einer marktbeherrschenden Stellung von Internetsuchmaschinen, dargestellt am Beispiel von Google, 2014, S. 3 f.; *Daly*, Dominating Search, Google Before the Law, in: König/Rasch (Hrsg.), Society of the Query Reader. Reflections on Web Search, 2014, S. 86 ff.

32 Ähnliche Vorwürfe waren Gegenstand eines gegen Google gerichteten Verfahrens der US-amerikanischen Federal Trade Commission (FTC). Diese verneinte am Ende allerdings ein wettbewerbswidriges Verhalten von Google. Siehe dazu *Daly*, (Fn. 31), S. 93 ff.

Maßnahme und es konnte die als Sanktion gedachte Zahlungsverpflichtung möglicherweise geringer halten als bei der Verhängung einer Geldbuße. Andererseits könnte die Aussicht auf die Beendigung eines Beanstandungsverfahrens durch Selbstverpflichtung die Unternehmen motivieren, ihre Marktmacht möglichst weitgehend auszureizen und dabei Beanstandungsverfahren ohne Risiko starker Sanktionierung in Kauf zu nehmen. Der behördliche Verzicht auf den vollen Einsatz ihrer hoheitlichen Gewalt könnte in der Folge zu erheblichen Implementationsdefiziten führen.

## *V. Hoheitlich regulierte gesellschaftliche Selbstregulierung*

Hoheitsträger können regulativ auf die Art und Weise der gesellschaftlichen Selbstregulierung Einfluss nehmen und so Anliegen der Gemeinwohlbindung im Hinblick auf die private Aufgabenerfüllung wahrnehmen. Dies kann gegebenenfalls auch in Gestalt von rechtlich unverbindlichem Soft Law geschehen. Ein Beispiel sind die IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik.[33] Sie sind rechtlich nicht verbindlich. Sie können aber als Grundlage einer Zertifizierung genutzt werden, durch die indiziert wird, dass das Unternehmen geeignete Maßnahmen zur Absicherung seiner IT-Systeme gegen IT-Sicherheitsbedrohungen ergriffen hat.

Ein anderer Typ ist die hoheitlich geprüfte Selbstregulierung. Beispiele sind die in § 38 a BDSG vorgesehenen Verhaltensregeln, die von Berufsverbänden und anderen Vereinigungen zur Förderung der Durchführung von datenschutzrechtlichen Regelungen geschaffen werden. Die Verhaltensregeln sollen die gesetzlichen Vorgaben durch Satzung oder Vertrag konkretisieren. Dies ist eine freiwillige Aktion. Die Regelungen können allerdings der zuständigen Aufsichtsbehörde unterbreitet werden, damit sie die Vereinbarkeit der Entwürfe mit dem geltenden Datenschutzrecht überprüfen kann.[34] Die (in der Praxis allerdings nichtbedeutsam geworde-

33 Dazu siehe die Homepage des Bundesamts für Sicherheit in der Informationstechnik (BSI) www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html.

34 Zur Selbstregulierung im Bereich des Datenschutzes siehe etwa *Pabel*, Umsetzung der Selbstregulierung: Probleme und Lösungen, in: RDV 2003, S. 11; *Bizer*, Selbstregulierung des Datenschutzes, in: DuD 2001, s. 168 ff.; *Hoeren*, Prüfungsbescheide der Datenschutzaufsicht und ihre verwaltungsrechtliche Bindungswir-

ne) Qualitätsbestätigung durch die Aufsichtsbehörde soll nicht als Maßnahme kooperativen Zusammenwirkens erfolgen, soll aber in Gestalt eines feststellenden Verwaltungsaktes Rechtssicherheit über die zutreffende Auslegung des Datenschutzrechts schaffen.[35]

Die EU-Datenschutzgrundverordnung[36] sieht ähnliche Möglichkeiten hoheitlicher Regulierung von Selbstregulierung vor. Sie ermuntert dazu, dass Verbände und andere Vereinigungen Verhaltensregeln ausarbeiten, die eine ordnungsgemäße und wirksame Anwendung der Verordnung erleichtern.[37] Art. 40 Abs. 2 der Verordnung führt ausdrücklich eine Vielzahl von Themenbereichen auf, für die Präzisierungen erfolgen können. Die Präzisierungsanregungen sind als regulative Orientierungen für die Verhaltensregeln gedacht, zu deren Erlass die Verbände oder Vereinigungen allerdings nicht verpflichtet sind. Ebenso sind sie nicht verpflichtet, von der weiteren in Abs. 5 vorgesehenen Möglichkeit Gebrauch zu machen, den Entwurf der Aufsichtsbehörde vorzulegen, die – wenn dies geschieht - in einer Stellungnahme darlegt, ob die Verhaltensregeln mit der Verordnung vereinbar sind. Sind dafür ausreichende Garantien vorhanden, wird der Entwurf der Verhaltensregeln von der Behörde genehmigt (Abs. 5). Anschließend gelten unterschiedliche Verfahren je nachdem, ob der Entwurf Verarbeitungstätigkeiten nur in einem oder in mehreren Mitgliedstaaten betrifft (Abs. 6 – 8). Sind die Prüfungen positiv, kommt es am Ende des Verfahrens zu einer amtlichen Veröffentlichung (Abs. 6, 11). Für die in mehreren Mitgliedstaaten geltenden Verhaltensregeln kann die EU-Kommission sogar im Wege von Durchführungsrechtsakten beschließen, dass sie allgemeine Gültigkeit in der EU besitzen (Abs. 9). Art. 41 der Verordnung sieht für die Überwachung der Einhaltung der Verfahrensregeln Möglichkeiten der Akkreditierung geeigneter Stellen vor. Angestrebt werden auch datenschutzspezifische Zertifizierungsverfahren sowie Datenschutzsiegel und –prüfzeichen (Art. 42 der Verordnung). [38]

---

kung, 2001; *Schröder*, Selbstregulierung im Datenschutzrecht – Notwehr oder Konzept? in: ZD 2012, S. 418.

35 Näher dazu *Hullen* in: Plath, Bundesdatenschutzgesetz, 1. Aufl. 2013, Kommentierung zu § 38 a BDSG.

36 S. oben Fn. 14.

37 S. Nr. 77, 98 der Erwägungsgründe.

38 Zur Einschätzung solcher Instrumente – allerdings noch auf der Grundlage des ursprünglichen Vorschlags der EU-Kommission zur Datenschutzgrundverordnung – *Hornung/Hartl*, Datenschutz durch Marktanreize – auch in Europa? Stand der Diskussion zu Datenschutzzertifizierung und Datenschutz, in: ZD 2014, S. 219.

Um eine Form regulierter gesellschaftlicher Selbstregulierung handelt es sich auch bei dem folgenden Beispiel. Nach § 19 des Jugendmedienschutz-Staatsvertrages können zur Kontrolle der Einhaltung der Bestimmungen des Staatsvertrages und anderer Regeln Einrichtungen Freiwilliger Selbstkontrolle u. a. für Telemedien gebildet werden.[39] Soweit diese bestimmte Voraussetzungen (Unabhängigkeit, Vorgaben für die Entscheidungen der Prüfer, Verfahrensregeln u. a.) erfüllen und das in diesem Paragraphen geregelte Anerkennungsverfahren erfolgreich absolviert haben, können die Mitgliedschaft eines Anbieters von Telemedien in einer solchen Einrichtung und zusätzlich die Beachtung ihrer Statuten eine Privilegierung des Anbieters gegenüber Aufsichtsmaßnahmen der zuständigen Landesmedienanstalt bewirken: Nach Art. 20 Abs. 5 dieses Staatsvertrages ist nämlich bei behaupteten Verstößen gegen den Jugendschutz zunächst diese Einrichtung mit den Behauptungen zu befassen. Aufsichtliche Maßnahmen gegen den Anbieter sind nur ausnahmsweise möglich, nämlich wenn die Entscheidung oder die Unterlassung einer Entscheidung durch die Selbstkontrolleinrichtung "die rechtlichen Grenzen des Beurteilungsspielraums überschreitet".

Als ein weiteres Beispiel regulierter Selbstregulierung sei auf die Auditierung nach § 9 a BDSG verwiesen.[40] Sie ist mit einer Vermutung der Regelbeachtung nach Bewertung des Datenschutzkonzepts versehen. Das in § 9 a S. 2 BDSG zur Ausführung vorgesehene Gesetz ist allerdings nicht zustande gekommen.[41]

Eine besondere Art hoheitlicher Regulierung von gesellschaftlicher Selbstregulierung kann gelegentlich auch die Gerichtsbarkeit nutzen. Ein Beispiel ist die Google-Entscheidung des EuGH,[42] in der dieses Gericht der Google Inc. auferlegt hat, Vorkehrungen zum Schutz des sogenannten

---

39 Siehe dazu die Homepage der Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter (abrufbar unter www.fsm.de).

40 Dazu siehe statt vieler *Scholz*, in: Simitis, Bundesdatenschutzgesetz, 8. Aufl. 2014, Kommentierung zu § 9 a BDSG, Rn. 40 ff.

41 Der von der Bundesregierung eingebrachte "Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften" vom 18.02.2009 (BT-Drs. 16/12011) ist der Diskontinuität zum Opfer gefallen: Er wurde wegen konzeptioneller Schwächen und des hohen bürokratischen Aufwandes massiv kritisiert.

42 EuGH, Urteil Google Spain und Google, C-131/12 EU: C: 2014: 317 = EuGRZ 2014, S. 320 ff. In Art. 17 Datenschutzgrundverordnung sind jetzt ausdrückliche Regeln zum „Recht auf Vergessenwerden“ enthalten

Rechts auf Vergessen(werden) beim Betrieb seiner Suchmaschine zu treffen. Google wurde unter Anwendung der EU-Datenschutzrichtlinie 95/46 verpflichtet, unter bestimmten Voraussetzungen den Link zu einer Information in dem europäischen Angebot seiner Suchmaschine zu löschen und damit den Zugang zu der betroffenen Information (die als solche allerdings nicht gelöscht wird) zu erschweren. Die Entscheidungsmacht über die Löschung liegt ausschließlich bei Google, also dem oligopolistischen „Beherrscher" des Suchmaschinenmarktes. Allerdings kann derjenige, der die Löschung beantragt hat und damit keinen Erfolg hat, vor Gericht klären lassen, ob Google die persönlichkeitsschützenden Vorgaben des EU-Rechts eingehalten hat. Keine Rechtsschutzmöglichkeit hat der EuGH demgegenüber demjenigen eingeräumt, dessen Information durch die Beseitigung des Link nicht mehr oder nur noch erschwert zugänglich ist: Es gibt kein Recht auf Verlinkung. Google hat zwischenzeitlich ein Formular zur Beantragung der Löschung von URLs aus den Suchergebnissen veröffentlicht. Auch hat Google einen Beirat mit externen Experten aus europäischen Ländern eingesetzt, der Empfehlungen zur Löschungspraxis entwickelt hat.[43]

Eine völlig andere Art der hoheitlichen Regulierung von gesellschaftlicher Selbstregulierung sind hoheitliche Vorkehrung zur Sicherung der Funktionsfähigkeit selbstregulativer Strukturen, wie insbesondere des Marktes. Hier geht es um die Ermöglichung oder den Erhalt von Wettbewerb. Die Funktionsfähigkeit des Marktes soll in der Weise gesichert werden, dass die verschiedenen Interessen der Marktteilnehmer durch deren autonomes Handeln bestmöglich befriedigt und zugleich Gemeinwohlziele verwirklicht werden. Gegenwärtig hat Kartellrecht allerdings nur geringe Chancen, auf die Funktionsfähigkeit der Internetmärkte nachhaltig einzuwirken. Denn angesichts der Globalisierung der meisten Teilmärkte wäre ein globales Kartellrecht erforderlich; das aber gibt es nicht. Das nationale Kartellrecht kann nur begrenzt auf das Verhalten globaler Akteure einwirken. Das europäische Kartellrecht[44] ist – wegen seines relativ großen An-

---

43 Näher dazu die Homepage des sog. „Experten-Beirats" („The Advisory Council to Google on the Right to be Forgotten"), abrufbar bei Google unter www.google.com/intl/de/advisorycouncil; siehe auch den Abschlussbericht des Beirats (in engl. Sprache), abrufbar unter https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view?pli=1.

44 Dazu siehe statt vieler *Weiß*, Europäisches Wettbewerbsverwaltungsrecht, in: Terhechte (Hrsg.), Verwaltungsrecht der Europäischen Union, Baden-Baden 2011.

wendungsgebiets – grundsätzlich dazu eher geeignet, ist bisher allerdings nicht mit durchgreifendem Erfolg angewandt worden.

Im Übrigen ist darauf hinzuweisen, dass sich mithilfe des Kartellrechts eine Reihe von Problemen oder Gefährdungen nicht bewältigen lassen, die im Internet bestehen und mit der Asymmetrie in der Verteilung von Machtverhältnissen verkoppelt sind. Dies betrifft Probleme wie die Sicherung der Zugangschancengleichheit, der Netzneutralität, der Manipulationsfreiheit, des Persönlichkeitsschutzes u. a.. Kartellrecht als Recht zur Sicherung der Funktionsfähigkeit von Märkten ist für die Bewältigung der mit solchen Zielen verbundenen Probleme grundsätzlich nicht oder doch nur sehr begrenzt geeignet, es sei denn, es werde zu einem sektorspezifischen Regulierungsrecht mit entsprechenden Zielsetzungen ausgebaut. Das aber wäre ein Systembruch im geltenden Kartellrecht. Um ihn zu vermeiden, gibt es in den nationalen Rechtsordnungen meist Spezialnormen zur Sicherung spezifischer Rechtsschutzbedarfe, in Deutschland etwa das Datenschutzrecht oder das Telemedienrecht. Auch deren Regelungen sind Vorkehrungen regulativer Einwirkung auf Selbstregulierung. Aber ihre Wirkungskraft ist schon durch ihren nur regionalen Geltungsbereich beschränkt, der es insbesondere erschwert, auf das Verhalten global aufgestellter und machtvoller Wirtschaftsunternehmen effektiv Einfluss zu nehmen.

## *VI. Besonderheiten bei der Anwendung von Allgemeinen Geschäftsbedingungen*

Ein Beispiel nicht hoheitlicher Regelung sind die Allgemeinen Geschäftsbedingungen, die von den je einzelnen Unternehmen selbstregulierend formuliert werden, beispielsweise von den Betreibern von Internetsuchmaschinen oder Kommunikationsplattformen. Die AGBs sind darauf ausgerichtet, durch Einwilligung der Nutzer in sie verbindlich zu werden. Die Einwilligung in die AGBs[45] ist regelmäßig Voraussetzung für die Inanspruchnahme der Dienste. Rechtlich handelt es sich um einen Vertrags-

45 Zu dem Erfordernis und den Voraussetzungen einer wirksamen Einwilligung siehe statt vieler *Spindler*, Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung, 69. Deutscher Juristentag, Gutachten F, 2012, S. 47 ff., 76 ff. m. w. Hinw. Anforderungen an die Einwilligung enthält nunmehr auch die Datenschutzgrundverordnung der EU (Art. 6 ff.)

schluss (§ 305 BGB) und insofern dem äußeren Erscheinungsbild nach auf beiden Seiten um einen Akt autonomer Entscheidung. Dieser ist insofern rechtlich umhegt, als das deutsche AGB-Recht (§ 305 ff BGB, ergänzt um datenschutzrechtliche Sonderregelungen, darunter auch Art. 6 f der EU-Datenschutzgrundverordnung, bestimmte Anforderungen an die Wirksamkeit der Einwilligung normiert.

Der Vertragsschluss ist gleichwohl durch starke Asymmetrien in der Einflussmacht der Vertragsschließenden gekennzeichnet. So haben die Nutzer – von geringfügigen Ausnahmen abgesehen – keine Möglichkeit der inhaltlichen Einwirkung auf die Geschäftsbedingungen. Diese sind regelmäßig auch nicht im Zusammenwirken mit Verbraucherverbänden oder anderen Nutzerorganisationen geschaffen worden, die Nutzerinteressen artikulieren könnten.

Asymmetrien bestehen auch bei der konkreten Entscheidung über die Erteilung der Einwilligung. Es gibt meist nur weitgehend unzulängliche Informationen der Nutzer über die von der Einwilligung abgedeckten Tätigkeiten, und praktisch keine Angaben darüber, welche ihrer personenbezogenen Daten welchen konkreten Unternehmen für welche konkreten Zwecke weitergegeben oder entgeltlich veräußert werden.

Einer Fiktion kommt vor allem vielfach die Freiwilligkeit der Einwilligung nahe. Dies soll hier am Beispiel von Suchmaschinen illustriert werden. Es gibt zwar verschiedene Suchmaschinen, zwischen denen der Nutzer wählen kann, aber eine davon mit oligopolistischer Marktdominanz. Diese, die Suchmaschine Google, wird von rund 90 Prozent aller Deutschen genutzt. Die Palette ihrer Suchleistungen ist breiter und die Suchmöglichkeiten führen häufig in tiefere Dimensionen als die konkurrierender Unternehmen wie Yahoo oder Bing oder anderer (kleiner) Anbieter. Aber auch viele dieser Unternehmen fordern für die Nutzung der Suchleistung eine Einwilligung dahingehend, dass die dabei anfallenden Daten von den Unternehmen erhoben und weiterverwertet werden können. Art und Umfang solcher Einwilligungen unterscheiden sich von der bei Google nicht maßgebend. Die Nutzer haben insofern zwar eine Möglichkeit, zwischen Suchmaschinen zu wählen, aber nicht die Chance, dadurch ihren Persönlichkeitsschutz besser zu wahren als bei Google. Es gibt allerdings auch Suchmaschinen, die versprechen, auf eine Datenerhebung und Weiterverwertung zu verzichten – wie die Metasuchmaschine MetaGer oder die Suchmaschine Duck Duck Go. Die Breite und Qualität der Angebote sind mit denen von Google – oder auch von Yahoo oder Bing – allerdings nicht vergleichbar.

Nun ist die Möglichkeit der Suche über Google für die meisten Menschen nicht lebensnotwendig, aber in vielen Lebens- und Berufsfeldern wird erwartet, dass solche Suchmaschinen genutzt werden. Dies erhöht den Druck, die geforderten Einwilligungen abzugeben.

Faktischer Druck zur Einwilligung in die AGBs besteht auch für Personen, die Dienste der Kommunikationsplattform Facebook[46] in Anspruch nehmen wollen. Beispielsweise läuft die soziale Kommunikationsteilhabe nicht nur, aber besonders intensiv bei Kindern und Jugendlichen in hohem Maße über Facebook ab;[47] sie würden sich meist kommunikativ isolieren, wenn sie Facebook nicht nutzten, etwa wegen der Verweigerung der Einwilligung in die AGBs seitens der Erziehungsberechtigten. Viele Kinder und Jugendliche würden sich sozial in mancher Hinsicht auch außerhalb der digitalen Kommunikation isolieren, da die über Facebook vermittelten Kommunikationsinhalte vielfach auch die sonstige, insbesondere die Face-to-Face-Kommunikation, bestimmt.

Viele Websites von privaten Unternehmen, aber in starkem Maße auch die von staatlichen Stellen, haben Facebook integriert und tragen so dazu bei, dass Nutzer nur mit Nachteilen von der Freiheit Gebrauch machen können, die Einwilligung zu verweigern und dadurch auf die Facebooknutzung zu verzichten.

Aufgrund solcher und weiterer Faktoren besteht eine Art faktischer Anschlusszwang. Entscheidungsfreiheit aber setzt bei Verträgen Abschlussfreiheit voraus, die zugleich eine Bedingung für die Funktionsweise von Wettbewerbsmechanismen ist.[48] Zwar führt die Einwilligung rechtlich zu einem Vertragsschluss, dieser aber kommt faktisch einer einseitigen Setzung nahe. Aus Nutzersicht handelt es sich nicht um die Teilhabe an Selbstregelung, sondern um Regulierung durch das beteiligte Unternehmen.

---

46 Zu Facebook siehe *Machill/Beiler/Krüger*, Das neue Gesicht der Öffentlichkeit. Wie Facebook und andere soziale Netzwerke die Meinungsbildung verändern, 2013. Siehe auch die Beiträge in Hill/Martini/Wagner (Hrsg.), Facebook, Google & Co. Chancen und Risiken, 2013.

47 Daten zur Nutzung von Facebook und anderen Social-Media-Plattformen, auch durch Kinder und Jugendliche, in: *Tippelt/Kupferschmitt*, Social Web: Ausdifferenzierung der Nutzung – Potenziale für Medienanbieter, in: Media Perspektiven 2015, S. 442 ff.

48 Dazu siehe *Magen*, Ein Wettbewerbskonzept für das Öffentliche Wettbewerbsrecht, in: Kirchhof/Korte/Magen (Hrsg.), (Fn. 2), S. 17, 48 f.

## D. Schlussbemerkung

Die bisher aufgeführten Beispiele zeigen, dass es im IT-Bereich verschiedenartige hoheitliche Einwirkungen auf privat-gesellschaftliches Verhalten sowie auf die maßgebenden Strukturen gibt. Verglichen mit den Gestaltungsmöglichkeiten insbesondere der machtvollen Unternehmen ist die hoheitliche Einwirkungsmacht aber eher marginal. Angesichts der hohen Bedeutung der IT-Infrastrukturen und Dienste für Staat und Gesellschaft sowie angesichts der mit ihrer Nutzung und ihrem weiteren Ausbau verbundenen Chancen und Risiken bestehen erhebliche Zweifel an hinreichenden Möglichkeiten von Hoheitsträgern zur effektiven Sicherung von Gemeinwohlbelangen, insbesondere soweit dies Vorkehrungen zur Korrektur der erheblichen Machtasymmetrien erfordert.

Den deutschen Staat in seiner modernen Gestalt als Gewährleistungsstaat[49] trifft grundsätzlich die Aufgabe, seine Möglichkeiten zur Ausgestaltung des Freiheitsschutzes für alle durch Recht zu nutzen. Dabei stößt er aber aufgrund der weitgehend ohne hoheitliche Regulierung entstandenen Marktstrukturen im Internetsektor und insbesondere aufgrund der bestehenden Machtasymmetrien sowie auch aufgrund des schon beschriebenen Problems vielfältiger Entgrenzungen auf erhebliche Schwierigkeiten. Er mag im territorialen Geltungsbereich seiner Gesetze Vorkehrungen zum Rechtsgüterschutz, etwa zum Persönlichkeitsschutz, schaffen; diese geben aber nur begrenzten Schutz.[50]

Fazit: Im digitalen Kontext des Internet gibt es nicht einen Mangel an Möglichkeiten der Selbstregelung-/regulierung. Allerdings ist die Regulierung von Selbstregulierung im digitalen Kontext aus Nutzersicht in Vielem defizitär.

---

49 Zu diesem Begriff siehe statt vieler *Eifert*, Grundversorgung mit Telekommunikationsleistungen im Gewährleistungsstaat, 1998, S. 18 ff., 193 ff; *Hoffmann-Riem*, Gesetz und Gesetzesvorbehalt im Umbruch. Zur Qualitäts-Gewährleistung durch Normen, in: AöR (130) 2005, 5 (9 f.); *Schuppert*, Der Gewährleistungsstaat: ein Leitbild auf dem Prüfstand, 2005.

50 Näheres hierzu *Hoffmann-Riem*, Innovation und Recht – Recht und Innovation, 2016, Teil 8.

# Verantwortung bei begrenztem Wissen in der vernetzten Welt

*Indra Spiecker genannt Döhmann**

## *I. Einleitung*

Wer sich gegenwärtig mit IT befasst, ist mehr denn je gefordert, sich beständig anzupassen. Die Veränderungen auf diesem Gebiet sind allgegenwärtig; IT wächst exponentiell und beeinflusst kontinuierlich die Welt, in der wir uns bewegen. Die Weichenstellungen von heute sind in ihren Konsequenzen nicht absehbar und werden je nach Sichtweise und persönlicher Einstellung unterschiedlich beurteilt; sicher ist aber, dass viele der Erscheinungen und Entwicklungen von heute auch zukünftige Generationen binden werden.

Die Maxime der Informationstechnologie lautet: Schnell, einfach und bedienerfreundlich. IT ist zumeist nicht als solche erkennbar; sie soll es gerade nicht sein. Ihr Mehrwert wird nicht zuletzt davon beeinflusst, dass und in welchem Ausmaß eine intuitive Benutzbarkeit gegeben ist; Fremdsteuerung und Unkontrollierbarkeit wird in der Folge nicht als bedrängend und einschränkend dargestellt und wahrgenommen, sondern als Vereinfachung und positive Erleichterung des Alltags.

Teil der einfachen, schnellen und nicht erkennbaren IT ist die ihr in vielen Anwendungen inhärente Vernetzung. Dienste, zugrundeliegende Plattformen und Infrastruktur sind untrennbar miteinander verbunden; wer was von einem weiß in einer vernetzten Umgebung ist für den Nutzer – oder datenschutzrechtlich gesprochen den Betroffenen – nicht erkennbar. Die Funktionsweise von Smartphone, vernetzten Geräten, Apps und Internetdiensten erschließt sich dem Benutzer zumeist nicht (mehr); alle technischen Ebenen verschmelzen miteinander.

---

* Inhaberin des Lehrstuhls für Öffentliches Recht, Informationsrecht, Umweltrecht und Verwaltungswissenschaften an der Goethe-Universität Frankfurt a.M. und Direktorin der Forschungsstelle Datenschutz ebenda; zudem Mitglied des IT-Kompetenzzentrums KASTEL am Karlsruher Institut für Technologie.
Besonderer Dank für die ergänzende Recherche geht an stud. iur. Bianca Grujcic und Sonja Hess.

Dies führt dazu, dass zunehmend der Gebrauch von Technik losgelöst von eindeutigen Verantwortungsstrukturen erfolgt. Wer zurechenbar Gefahren und Risiken schafft, wer derjenige ist, der für informationelle Fehlleistungen und Mißbräuche rechtlich und tatsächlich haftet, ist aufgrund der engen Verbindung verschiedener Dienste und verschiedener Infrastrukturen nicht mehr ohne weiteres erkennbar. Am deutlichsten wird dies derzeit bei der Nutzung von Apps: Ob der sog. Appstore, in dem eine Anwendung eingekauft wird, oder aber der dahinterstehende Appanbieter als Verantwortlicher im Sinne des Telemediengesetztes TMG zu interpretieren ist, ist heftig umstritten.[1]

Dass Technikentwicklung jedenfalls Gesellschaft und Recht vor neue Herausforderungen stellt und oftmals auch neue Wertigkeit prägt, ist eine Allerweltserkenntnis. Ebenso ist nicht neu, dass Recht sich immer schon mit der Regulierung von neuen Techniken auseinandergesetzt hat, und dies geschieht durchaus auch auf unterschiedlichen Ebenen und mit verschiedensten Instrumenten.[2] Es mag daher lohnend sein, das weite Feld einer rechtlichen Regulierung von Informationstechnologie unter dem Gesichtspunkt des Technikrechts[3] zu betrachten.

Damit wird dann gleichzeitig ein anderes, dem IT-Recht nicht allein innewohnendes Problem sichtbar: Mit den Entwicklungen in diesem Bereich entsteht neues Wissen. Gleichzeitig wird bestehendes Wissen verändert; Gewißheiten lösen sich auf; neue Entwicklungen werden sichtbar. Damit ist der Umgang mit IT aus rechtlicher Sicht auch immer ein Umgang mit begrenztem Wissen in einer vernetzten Welt.

---

1 Für eine Verantwortlichkeit des App-Anbieters etwa Baumgartner, in: Baumgartner/Ewald, Apps und Recht, Rn. 191; Düsseldorfer Kreis, Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter, S. 6; für den App-Store z.B. Feldmann, in: Taeger (Hrsg.): Die Welt im Netz – Folgen für Wirtschaft und Gesellschaft, Tagungsband DSRI Herbstakademie 2011, S. 61 f.; Degmair, K&R 2013, 213, 215.

2 Siehe nur zu den zwei klassischen Feldern, der Dampfkesselgesetzgebung und dem preußischen Eisenbahngesetz vom Feld, Staatsentlastung im Technikrecht. Dampfkesselgesetzgebung und -überwachung in Preußen 1831–1914, 2007; Lies-Benachib, Immissionsschutz im 19. Jahrhundert, 2002; Michalczyk, Europäische Ursprünge der Regulierung von Wettbewerb, 2010; Schubert, ZRG (GA) 116 (1999), 152–203; Collin u.a. (Hrsg.), Regulierte Selbstregulierung im frühen Interventions- und Sozialstaat, 2012.

3 Siehe dazu nur die Beiträge in Schulte (Hrsg.), Handbuch des Technikrechts, 2011; Berg, JZ 1985, S. 401-407.

## II. Die Akteure

In dieser vernetzten Welt der Unsicherheit treffen verschiedene Akteure aufeinander. Scheinbar lassen sie sich in eindeutige Kategorien einordnen. So ist der Nutzer als End"verbraucher" einer Informationsdienstleistung gegenübergestellt dem Anbieter dieser Dienstleistung. So gibt es kommerzielle und nicht kommerzielle Anbieter von Dienstleistungen. Selbst hier finden sich Untergruppierungen: Manche Anbieter verfolgen ihre Individualinteressen; andere haben sich dem Gemeinwohl verschrieben. Oder man könnte kategorisieren anhand der verschiedenen Ebenen, also nach Anbietern von Infrastruktur, von Zugang zur Infrastruktur, von Plattformen, von konkreten Diensten und schließlich von bestimmten Inhalten. Eindeutigkeiten, Gewißheiten und Verantwortung jedenfalls lösen sich auf. Selbst die Trennung von Staat und Privaten ist uneindeutig: Auch wenn die Architektur und die einzelnen Leistungen in den Händen Privater sind, so ist der Staat doch, und sei es über die telekommunikationsrechtliche Regulierung, ein Hauptakteur, um die Ausgestaltung der vernetzten Welt zu bestimmen; delegierte Universaldienstverpflichtungen[4] tun ein Übriges.

Daher wird bereits aus diesen einführenden Worten deutlich, dass Informationstechnologie sich auch dadurch auszeichnet, dass sie mit herkömmlichen Kategorisierungen bricht und in die Interessen der beteiligten Akteure nicht einheitlich ausgestaltet sind.

Unterscheiden lassen sich zunächst einmal private Akteure (1.) mit ihren individuellen Interessen, der Staat (2.) und schließlich die gerade in Bezug auf datenschutzrechtliche Fragestellungen immer wieder in Erscheinung tretende „Öffentlichkeit" (3.). Alle drei Akteure sind wichtige Elemente in der durch IT eintretenden Verschiebung von Machtstrukturen in einer vernetzten Welt.

### 1. Private Akteure

Private Akteure sind die zentralen Akteure der vernetzten Welt. Die wesentlichen Elemente der Vernetzung werden gegenwärtig von Privaten getragen: Sie sind Diensteanbieter, sie stellen die Infrastruktur bereit, sie

4 Siehe Art. 87 f GG.

schaffen Plattformen, Hard- und Software werden von Privaten entwickelt. Und sie sind die Nutzer und Nachfrager.

Gleichwohl lässt sich differenzieren. Nutzer zeichnen sich in der Regel durch ihre Konsumenten-Stellung aus. Sie sind häufig die Nachfrager verschiedenster Angebote des Informationsdienstleistungssektors; es ist oftmals ihre Bedürfnisbefriedigung, die das Angebot bestimmt.

Was allerdings zunächst aktivisch und damit freiheitlich klingt, kann sehr schnell auch von Passivität geprägt sein und auch Freiheitsbeschränkungen enthalten: Oftmals ist die Nutzereigenschaft fremdgesteuert und -bestimmt, etwa wenn ein Arbeitnehmer durch den Arbeitgeber angehalten ist, sich im Internet auf der Unternehmensseite zu präsentieren oder Materialien für ein Projekt auf einer internetbasierten Dokumentenplatform vorgehalten werden. Aber auch in Räumen ohne deutliches Abhängigkeitsverhältnis bestehen häufig durch die Zugehörigkeit zu einer Gruppe informationstechnisch relevante Aktivitäten, die den Nutzer durchaus auch zum Externen und zum unfreiwilligen Nutzer machen können: Wer Mitglied eines Sportvereins ist, wird bei Veranstaltungen abgebildet; die Kinder einer Schule treten im Rahmen von Unternehmungen in Erscheinung. Den berühmtesten Fall hatte wohl der EuGH in *Lindqvist*[5] zu entscheiden, als eine schwedische Katechetin auf ihrer privaten Webseite Informationen über sich und weitere Ehrenamtliche aus ihrer Gemeinde verfügbar machte: Bezeichnenderweise waren einige ihrer auf diese Weise zur öffentlichen Person gewordene Kollegen nicht einverstanden. Das Problem von Informationen, die sich auf mehr als einen Betroffenen beziehen und damit potentiell von allen Betroffenen genutzt werden können, bleibt rechtlich bisher ungelöst. Oft ist derjenige mächtig, der agiert.

Nutzer sind aber auch in anderer Hinsicht nicht mehr einfach zu klassifizieren; ihnen können daher keine eindeutigen Interessen mehr zugewiesen werden. Das wird besonders dann deutlich, wenn man moderne Formen der Interaktion im Netz betrachtet: Oftmals schaffen die Nutzer überhaupt erst den Mehrwert einer Informationsdienstleistung durch ihre Beiträge und ihre Gestaltungsformen.[6] Ebay, Facebook und individualisierte Google Suchmaschinen liefern dafür eindrückliche Beispiele. In einer von Big Data Anwendungen zunehmend beeinflussten Welt kommen noch weitere Elemente hinzu: Nutzerdaten tragen überhaupt erst dazu bei, Big

5 EuGH Urteil v. 6.11.2003, Rs C-101/01, Slg. 2003, I-12992 - *Bodil Lindqvist*.
6 Siehe dazu schon Spiecker gen. Döhmann, AnwBl. 2011, 256-259.

Data Auswertungen treffen zu können und damit verallgemeinerbare Aussagen zu tätigen.

Damit ist eine weitere große Gruppe der privaten Akteure angesprochen, nämlich die Dienste- und Plattformanbieter einschließlich der Informationsmediäre. Sie gestalten und prägen derzeit die vernetzte Welt. Selbst dort, wo es staatliche Vorgaben gibt, etwa zum Einbau von Smart Metern[7] im Rahmen der Elektrizitätsversorgung, sind es die Privaten, die geeignete Instrumente und Messtechniken entwickeln und bereitstellen[8].

Auch Diensteanbieter, Plattformnbetreiber und Informationsmediäre können völlig verschiedene Vorstellungen von der Ausgestaltung der vernetzten IT-Welt zum Ausdruck bringen, wie sich etwa bei den Stellungnahmen zur Netz-Neutralität[9] oder in den Stellungnahmen zur Entscheidung des EuGH zur Löschverpflichtung in Suchmaschinen[10] zeigt. Verbreitungsinteressen treffen auf Restriktionsinteressen; Produktionsinteressen auf Zugangs- und Verfügbarkeitsinteressen; Individualinteressen auf Allgemeinwohl- und Öffentlichkeitserwägungen.

### *2. Der Staat*

Auch wenn die wesentlichen Akteure der vernetzten Welt im privaten Sektor zu verorten sind, ist der Staat gleichwohl in verschiedenen Rollen tätig.

Zunächst einmal ist er selbst Anbieter bestimmter IT-Dienstleistungen. Dieser Bereich lässt sich unter dem Schlagwort des E-Government fassen.[11] In dieser Eigenschaft fördert der Staat häufig den Einsatz von Informationsdienstleistungen; zum Teil erzwingt er diesen sogar, etwa im Bereich der Finanz- und Steuerverwaltung[12] oder bei Sozialabgaben[13] durch vorgeschriebene elektronische Kommunikationswege. Aber auch das E-

---

7 Vgl. § 21 c EnWG.

8 Dies wird deutlich an § 21 c Abs. 2 EnWG: Danach bestimmt der Markt, ob technische Möglichkeit durch Verfügbarkeit auf diesem gegeben ist.

9 Vgl. z.B. die Beiträge bei Krämer/Spiecker gen. Döhmann (Hrsg.), Network Neutrality and Open Access, 2011; Frevert, MMR 2012, 510-515.

10 Siehe nur statt vieler Kühling, EuZW 2014, 527-532; Spindler, JZ 2014, 981-991.

11 Siehe dazu z.B. Eifert, Electronic Government, 2006; Boehme-Neßler, NVwZ 2001, 374-380; Schliesky, DÖV 2004, 809-818.

12 Z.B. § 5 b EStG, sog. Elster-Verfahren.

13 Z.B. § 28 f Abs. 3 SGB IV.

Health-Gesetz verlangt eine Umstrukturierung des öffentlichen Gesundheitssystems und damit der dort Tätigen.

Gleichzeitig ist der Staat aber auch ein erheblicher Konsument von IT-Dienstleistungen. Der Einsatz von Instrumenten wie Quellen-Telekommunikationsüberwachung, Vorratsdatenspeicherung und Videoüberwachung von öffentlichen Räumen ist ohne den Einsatz von regelmäßig privat entwickelter Informationstechnologie nicht möglich, zum Teil, wie beim sog. „Staatstrojaner", werden für die staatliche Aufgabenerfüllung gezielt Private herangezogen und deren Wissen für die Verwaltung genutzt. Dieses Vorgehen ist nicht beschränkt auf den Bereich der Sicherheitsverwaltung; in gleicher Weise werden die Infrastrukturen für staatliche Leistungen von dritter Seite beschafft. Dies gilt ebenso für die bereits angesprochene Software, die eine elektronische Übermittlung von Daten überhaupt erst möglich macht im Bereich der Finanz-, Steuer- und Sozialverwaltung. Besonders intensiv ist diese staatliche Nachfrage im Bereich der Gesundheitsversorgung deutlich geworden: Die Entwicklung einer elektronischen Gesundheitskarte, die nach wie vor nicht vollständig gelungen ist, hat Milliarden an Entwicklungskosten produziert.[14] Staatlich vorgeschriebene digitale Meßverfahren, z.B. im Umweltrecht, tun ein Übriges.

Eng mit dieser Rolle verbunden ist die Rolle des Staates als eigentlicher Datenverarbeiter und Datennutzer. Der Einsatz von Informationstechnologie für die Aufgabe der Gefahren- oder Terrorabwehr, die Verarbeitung von personenbezogenen Daten im Steuer- und Finanzwesen, die Nutzung von Daten zur Erstellung von Statistiken, die Abfrage von Umweltinformationsdaten zur Bestimmung von Handlungsbedarfen oder die Kartographierung des öffentlichen Raums sind nur einige Anwendungsbereiche, in denen der Staat als einer der größten Datenverarbeiter überhaupt in Erscheinung tritt. Nicht von ungefähr gibt es ein großes Interesse an diesen Daten, gerade auch zur wirtschaftlichen Weiterverwertung.[15]

Schließlich tritt der Staat in seiner Funktion als Wirtschaftsregulator auf. Er ist entscheidender Gestalter von Marktbedingungen in einer Vielzahl von Märkten. Am sichtbarsten ist sein Einfluss im Bereich der Infrastruktur: Mit der Bundesnetzagentur reguliert der Staat die Netzwerkeffekte, die in der Telekommunikationsinfrastruktur auftreten können. Diese

14 Siehe allein die kleine Anfrage zum Entwicklungsstand der Elektronischen Gesundheitskarte von 2011, http://dip21.bundestag.de/dip21/btd/17/056/1705671.pdf.

15 Siehe dazu die Beiträge in Dreier/Fischer/van Raay/Spiecker gen. Döhmann, Zugang zu und Vewertung von öffentlichen Informationen, 2015.

Netzregulierung, die als spezifisches Wettbewerbsrecht verstanden sein will,[16] stellt entscheidende Weichen der verschiedenen Dienstleister und Dienste. Aber auch die Funktion der datenschutzrechtlichen Aufsichtsbehörden, in der Datenschutz-Grundverordnung gestärkt u.a. durch ihre Beteiligung an Risikoassessmentverfahren, fällt hierunter: Aufsichtsbehörden sind entscheidende Weichensteller für die Zulässigkeit und damit für die Durchführung von Datenverarbeitungsvorgängen.

### *3. Die Öffentlichkeit*

Ein bisher noch kaum präzisierter Akteur ist die sog. „Öffentlichkeit". Diese ist zunächst ein Kollektiv ohne Rechtspersönlichkeit; einzelne rechtliche Positionen sind aber eng mit der Öffentlichkeit verbunden, etwa die Jedermann-Zugangsansprüche der Informationsfreiheitsgesetze oder auch die Privilegierung der Verarbeitung „allgemein verfügbarer" personenbezogener Daten in § 28 Abs. 1 S. 1 Nr. 3 Alt. 1 und § 29 Abs. 1 S. 1 Nr. 2 Alt. 1 BDSG.

Die Öffentlichkeit ist Nutzer und gleichzeitig auch Produzent von externen Effekten individueller Tätigkeiten: Mangels Rechtspersönlichkeit kann ein Recht aus den Informationsfreiheitsgesetzen nur durch ein Individuum geltend gemacht werden; wer ein individuelles Interesse an der Verarbeitung von staatlichen Informationen hat, kann über die Weiterverwertungsgesetzgebung dieses wirtschaftlich betreiben. Die Konstruktion und Begründung der Effekte dieser Gesetze zielt aber immer wieder darauf ab, insgesamt zur Transparenz und Information der Öffentlichkeit beizutragen und Partizipation auf breiter Ebene zu ermöglichen.[17] Auch das Ziel dieser Gesetze, die Eigenkontrolle der Verwaltung anzuregen, wird als öffentlichkeitsdienlich verstanden.[18] Öffentlichkeit wird auch immer wieder gerne zitiert, um etwa die Veröffentlichung von Forschungsergebnissen ein-

16 Vgl. § 2 Abs. 4 TKG; ferner Kühne, in: Fuchs/Schwintowski/Zimmer (Hrsg.), Wirtschaft- und Privatrecht im Spannungsfeld von Privatautonomie, Wettberb und Regulierung. Festschrift für Ulrich Immenga zum 70. Geburtstag, 2004, S. 246; Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage 2015, § 1 TKG, Rn. 1 und 12.

17 Bt-Drs. 15/4493, S. 6 linke Spalte.

18 Siehe etwa die Gesetzesbegründung BT-Drs. 15/4493 S. 6 f.; vgl. auch Schoch, Informationsfreiheitsgesetz, § 1, Rn. 9.

zufordern, die mit Hilfe öffentlicher Gelder etwa an staatlichen Universitäten entwickelt worden sind.[19]

Nicht zu vernachlässigen ist schließlich, dass in nicht unerheblicher Weise darauf abgestellt wird, Interessen der Öffentlichkeit könnten durch Abwägungen von Verbreitungsrechten mit Datenschutzrechten beeinträchtigt werden.[20]

## *III. Das Individuum und Verantwortung*

Spricht man über Verantwortung mit rechtswissenschaftlichem Bezug, dann ist in einer freiheitlichen Gesellschaft immer der Einzelne, das Individuum, adressiert.[21] Die Rechtswissenschaft ist eine Wissenschaft von der Verantwortung;[22] Recht verteilt Verantwortung und schreibt sie zu, und zwar Rechtspersönlichkeiten. Die primäre Persönlichkeit des Rechts ist das Individuum. Dies entspricht im Übrigen auch der Vorstellung des Grundgesetzes über Art. 1 I GG: Dem Würdeprinzip ist gerade die Betonung des Einzelnen ein zentrales Anliegen.

### *1. Nicht-Wissen und Nicht-Erkennen von Technik*

Nicht-Wissen und darauf basierendes Verhalten können einem verantwortlichen Umgang mit Informationstechnologie, gerade auch der Zuschreibung von Verantwortung an ein Zurechungssubjekt, aber entgegenstehen. Dies ist bereits angelegt im Datenschutzrecht, denkt man nur an das Verdikt des Bundesverfassungsgerichts im Volkszählungsurteil, welches die Schutzbedürftigkeit des Individuums daran festmacht, dass es wissen müsse, wer was wisse.[23] Die Verantwortung wird damit rechtlich nicht allein dem Individuum zugewiesen; vielmehr stärkt das Bundesverfassungsgericht die Verpflichtung derjenigen, die automatisierte Datenverarbeitung

19 Vgl. Bretthauer, NVwZ 2012, 1144-1148.

20 Siehe etwa EuGH Urteil v. 13.05.2014, ‚Rs. C 131/12, EU:C:2014:314, Rn. 97 - *Google Spain*.

21 Zur Bedeutung siehe Klement, Verantwortung. Funktion und Legitimation eines Begriffs im Öffentlichen Recht, 2006.

22 Klement, Rechtliche Verantwortung, in: Heidbrink/Langbehn/Sombetzki (Hrsg.), Handbuch Verantwortung, i.E. 2016.

23 Vgl. BVerfGE 65, 1, 172.

betreiben und des Staates, um dafür Strukturen und Verfahren zur ergänzenden Absicherung bereitzustellen. Gleichwohl macht schon die Bezeichnung als Recht auf informationelle *Selbstbestimmung* deutlich, dass das Individuum gleichwohl verantwortlich bleiben soll.

Nicht-Wissen beeinträchtigt aber die Eigenverantwortlichkeit des Individuums. Wer Konsequenzen des Handelns nicht zu überschauen vermag, kann schwerlich Verantwortung übernehmen. Und wer nicht erfasst, dass und wie Rechtsverletzung stattfindet, kann sich ihr kaum entgegenstellen und damit Verantwortung umsetzen in rechtlich relevantes Verhalten. Und wie zu sehen sein wird, verstärkt Vernetzung diese Problematik noch.

Individuen erkennen häufig Rechtsverstöße und Eingriffe in ihre informationellen Rechte nicht, da ihnen eine bedienbare, effektive Technik zur Detektion nicht zur Verfügung steht. Es fehlt an technischem und rechtlichem Verständnis, an ausreichenden Ressourcen einschließlich der verfügbaren Zeit und auch an eindeutigen Interessen wider die informationellen Eingriffe (Schlagwort: Plattform-Nutzer)[24]. Hinzu kommen besondere Vernetzungseffekte: Die Identifikation der Verantwortlichen, der Datenverarbeiter und -nutzer ist im Zeitalter der vielfältigen Verbindungen und erst recht in der Globalisierung (zu) teuer, aufwendig und schwer. Dies liegt zum Teil daran, dass Informationseingriffe ohnehin kaum erkennbar sind: Dadurch, dass Informationen unverändert bleiben, wenn ein Dritter sie (unberechtigt) nutzt, wird für den Rechtsinhaber eine Rechtsverletzung nur dann sichtbar, wenn auf den erlangten Informationen sichtbar Entscheidungen basieren. Dies aber ist – gerade im Zeitalter von Big Data – für das Individuum zumeist nicht erkennbar. Als Zwischenfazit kann man für das Individuum festhalten: Benutzte Technik ist noch lange nicht auch erkannte und beherrschte Technik; und ein Informationseingriff ist noch lange kein erkannter und rechtsbewehrter Eingriff.

### *2. Unklarheit der rechtlichen Grundlagen*

Das Nicht-Wissen des Individuums und damit die Einschränkungen seiner Selbst-Verantwortung und Selbst-Bestimmtheit werden verstärkt durch die

---

24 Hier zeigt sich die Schwierigkeit der Trennung der Nutzer von den Diensteanbietern: Da Nutzer daran interessiert sind, diese Dienste und ihre Informationsverbreitung zu nutzen, können sie nicht eindeutig Position beziehen.

Unsicherheit über die rechtlichen Grundlagen und damit über die Normativität der Technologie.

Häufig wird, gerade von Informationsdienstleistern, der Weg der Einwilligung des Betroffenen gewählt, um sich einer rechtmäßigen weiteren Verwendung der Daten zu versichern. Diese Einwilligung setzt aber eine Reihe von Elementen für ihre Rechtswirksamkeit voraus, nicht im geringsten eine Freiwilligkeit. Diese Möglichkeit ist aber bei monopolistischen Anbietern oder sogar schon einem deutlichen Machtungleichgewicht umstritten,[25] bleibt dem Betroffenen doch regelmäßig nur die Wahl zwischen der Einwilligung und damit dem Zugang zu einer Leistung (etwa Arbeit, Wohnung, Soziales Netzwerk) einerseits oder aber der Nicht-Erteilung der Einwilligung und damit dem gänzlichen Verzicht auf die Leistung andererseits. Entsprechend verlangt die künftig geltende Europäische Datenschutz-Grundverordnung von einer wirksamen Einwilligung mehr.

Die vernetzte und effektiv organisierte Struktur vieler Datenverarbeiter macht zudem die Zuordnung der Verantwortlichkeit unklar: Nicht zuletzt war die Entscheidung des EuGH zu Google Spain auch deshalb ein solcher Paukenschlag, weil sie eine Gesamtverantwortlichkeit des Mutterkonzerns mit seinen Diensten nach EU-Recht bejahte, obwohl die datenverarbeitenden Vorgänge außerhalb der EU stattfanden und verschiedene Entitäten beteiligt waren.[26] Damit wird eine wesentliche Ursache für Rechtsunsicherheit zumindest verringert, wenn nicht sogar beseitigt: Für die Beteiligten - und darüber hinaus - ist nunmehr geklärt, unter welchen Bedingungen auch außereuropäische Unternehmen europäisches Datenschutzrecht beachten müssen und wie Zurechnung in komplexen Unternehmensstrukturen erfolgen kann.

Verantwortlichkeit setzt aber auch bei konkreten Rechten und Pflichten an, und auch hier besteht eine hohe Unsicherheit, ob und in welchem Umfang diese bestehen. Muss beispielsweise jeglicher Auskunftsanspruch erfüllt werden, auch wenn es keine Anhaltspunkte für eine bisherige Datenverarbeitung gibt und die Nachforschung für den potentiellen Datenverarbeiter erheblichen Aufwand bedeutete?[27] Wie weit reicht die Pflicht zur Einsichtnahme in die automatisierten Verarbeitungsvorgänge im Bereich

25 Siehe etwa Menzel, DuD 2008, 400, 406; Iraschko-Luscher, DuD 2006, 706, 708; Munz, in: Graf von Westphalen, Vertragsrecht und AGB-Klauselwerke, 36. EL 2015, Datenschutzklauseln, Rn. 30.

26 EuGH Urteil v. 13.05.2014, Rs. C 131/12, EU:C:2014:314, Rn. 60 - *Google Spain.*

27 Vgl. Schoch, Informationsfreiheitsgesetz, § 7, Rn. 22.

des Scoring?[28] Und wann genau - eine der umstrittensten Fragen, zumal sie entscheidend für die Anwendbarkeit des Datenschutzrechts überhaupt ist - liegt eigentlich ein personenbezogenes Datum vor?[29]

### *3. Informationsasymmetrie und Marktversagen*

Schließlich leidet das Individuum darunter, dass es datenschutzfreundliche Produkte nicht erkennen und nicht beurteilen kann. Es ist gefangen in dem Dilemma, das mit dem sog. „Market for Lemons" nobelpreiswürdig beschrieben wurde[30]: Mangels eigener Fähigkeit zur Detektion der Qualität ist der Preis eines Produkts kein Ausweis über dessen Qualität. In der Folge ist dann Marktversagen für solche Produkte zu beobachten, wie es tatsächlich auch im Bereich des „privacy-by-design" stattfindet: Es fehlen Alternativen und Wahlmöglichkeiten, die Individuen erlaubten, Präferenzen für Datenschutz überhaupt zu entwickeln und dann auch umzusetzen. In der Folge werden kaum Produkte dieser Art ausgebaut; ein echter Markt fehlt.

### *4. Individuelle Steuerungsmöglichkeiten*

Eng mit den vorherigen Punkten verknüpft ist eine weitere Schwierigkeit in der Wahrnehmung einer eigenen Verantwortlichkeit: Das Individuum ist gar nicht mehr imstande, die es betreffenden Informationsflüsse tatsächlich individuell zu steuern. Dies liegt im Online-Bereich auf der Hand,[31] geht aber darüber deutlich hinaus. Denn auch wenn der Gesetzgeber dem Individuum eine Reihe von Individualrechten zur Geltendmachung seiner Selbstbestimmtheit auch nach Preisgabe von Informationen zur Verfügung stellt, so sind diese ihrerseits oftmals nicht vollständig erfüllbar - technisch nicht, faktisch nicht und zum Teil auch rechtlich nicht.

---

28 Siehe hierzu nur BGHZ 200, 38-51.

29 Statt vieler Dammann, in: Simitis, BDSG-Kommentar, 8. Aufl., 2014, § 3 Rn. 20 f.; Vorlagebeschluss des BGH zu dynamischen IPs BGH Beschluss v. 28.10.2014, Az VI ZR 135/13, WRP 2015, 215-218.

30 Akerlof, The Quarterly Journal of Economics 84 (1970), No. 3, 488-500.

31 Zu den besonderen Gefährdungen im Online-Datenumgang Spiecker gen. Döhmann, in: Bartsch/Briner (Hrsg.), DGRI-Jahrbuch 2010, 2011, 39-51.

Besonders deutlich wird dies am sog. „Recht auf Vergessen“, also Überlegungen dazu, ob das Verlangen nach Löschung eigentlich umfassend bedient werden kann. Auch die ersten Vorschläge zu einer neuen Datenschutz-Grundverordnung der EU, die noch ein solches Recht vorsahen,[32] entsprachen nicht einem Anspruch auf Löschung einer Information aus dem gesamten Internet. Eine solche vollständige Rückholbarkeit wäre wohl auch tatsächlich kaum durchführbar, da auch für Datenübermittler zumeist nicht nachvollziehbar ist, wer Daten heruntergeladen und zwischengespeichert hat. Entsprechend begrenzt sind die vorgelagerten Auskunfts- und Berichtigungspflichten in ihrer Durchführ- und Durchsetzbarkeit. Und selbst technische Steuerungsmöglichkeiten, etwa einer systematischen Identitätsverschleierung bis hin zu Pseudonomisierung und Anonymisierung, stoßen an Grenzen, die in der Informatik hinreichend belegt sind.

## *5. Anreizstrukturen*

Hinzuweisen ist schließlich noch auf die schwierige Anreizsituation, in der sich die Individuen regelmäßig befinden. Aus dem vorherig Dargestellten wird bereits deutlich, dass die Anreize äußerst gering sind, gegen Informationseingriffe vorzugehen: Diese sind aufwendig zu ermitteln, schwer nachzuvollziehen, kaum durchsetzbar, teuer und zumeist unproduktiv.

Nun können rechtliche Regelungen durchaus verhaltenssteuernd wirken und die Anreize der Adressaten verändern, etwa indem bestimmte Restriktionen mit einer Handlungsalternative verbunden werden oder indem eine Entscheidung anders formuliert und damit die Einschätzungen verändert werden[33]. Von diesen Möglichkeiten hat das Recht allerdings bisher wenig Gebrauch gemacht. Obwohl eine Schadensersatzregelung im geltenden Recht enthalten ist, sieht dieses keine nennenswerten Regelungen für das Sonderproblem der Verletzung von Informationsrechten vor: Weder wird eine pauschalierte Schadenssumme festgesetzt noch wird für die Schadensberechnung vom Prinzip des Vermögensschadens Abstand ge-

32 Vgl. Art. 17 Entwurf der Kommission http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf.

33 Sog. Framing, siehe nur Kahneman/Tversky, Science 200 (1981), No. 4481, 453-458; Kahneman/Tversky, Choices, values and frames, 2000.

nommen. In der Konsequenz bleiben - anders als etwa im Presserecht - Verstöße gegen das Persönlichkeitsrecht aus datenschutzrechtlicher Perspektive im Kern ungeahndet und leiten daher auch nicht zu erhöhten Sorgfaltsmaßnahmen an. Verstärkt wird dieses Problem noch dadurch, dass es an Beweislasterleichterungen für den Betroffenen fehlt, dieser also - erneut ohne technisches Knowhow - dem Datenverarbeiter Verstöße nachweisen muss. Dies ist aber regelmäßig unmöglich, ohne dessen Algorithmen detektieren und nachvollziehen zu können. Die kommende Datenschutz-Grundverordnung ändert daran wenig bis nichts.

## *IV. Vernetzung und Verantwortlichkeit*

Ist also Verantwortung des Individuums schon per se problematisch unter dem gegenwärtigen technischen und rechtlichen Stand, so verstärkt die zunehmende Vernetzung diese Lage noch. Verantwortungszusammenhänge werden dadurch aufgelöst und verschoben; klassische Vorstellungen von Entscheidungshoheit als Zuschreibungsobjekt für Verantwortlichkeit gehen ins Leere.

Die gesamte jüngere Entwicklung der Informationstechnologie weist in diese Richtung. Sog. „smarte“ Steuerung - angefangen beim Energienetz, dem „smart grid“ über das energetisch effektuierte Umfeld durch „smart metering“ bis hin zum vollumfänglich vernetzten und gesteuerten Wohnumfeld, dem „smart home“ - geht davon aus, dass eine möglichst weitreichende Vernetzung verschiedenster Elemente eines Systems eine externe und sogar eine Selbststeuerung des Systems ermöglicht und damit insgesamt die Effektivität des Systems erheblich steigert. Das Individuum wird hier als störend empfunden und weitestgehend standardisiert.

Noch weiter gehen Vorstellungen davon, dass völlig neue Umwelten geschaffen werden durch Vernetzung, etwa im Bereich der Fahrer- und Mobilitätsassistenz. Mittelfristig geht es dabei nicht um Vorstellungen von Hilfestellung und Verbesserung individueller Leistungsfähigkeiten, was das Beiwort der „Assistenz“ verheißt. Denn solche assistierenden Systeme entfalten ihre Leistungsfähigkeit eigentlich erst dann, wenn der Störfaktor Mensch ausgeschaltet ist, wenn also die Fahrerassistenz zu einem selbstfahrenden Auto geworden ist. Das Individuum wird möglichst ausgeschaltet und in seinen Entscheidungsmöglichkeiten und -kompetenzen weitgehend zugunsten des Systems beschränkt.

Ähnliches ist im Bereich des Internets der Dinge und der besonderen Ausprägung in der Industrie 4.0 zu beobachten. Auch hier sollen Entscheidungsverlagerung vom Individuum in das System hin vorangebracht werden; Algorithmen sollen krisenfest entscheiden und selbstlernend reagieren können. Individuelle Entscheidungen, die womöglich nicht den algorithmisch bestimmten Wahrscheinlichkeitsaussagen im Einzelfall entsprechend, werden ausgeblendet und ersetzt durch Verhaltensprognosen, die auf der Basis von massenhafter Auswertung ohne individuellen Einschlag erstellt werden.

Wenn solche Systeme nicht nur unter externen Rationalitäten funktionieren, sondern über die inhärente Selbstlernfunktion auch veränderte Präferenzen aufweisen können und damit tatsächlich zu autonomen Systemen werden, verlieren damit die letzten Möglichkeiten traditioneller Anknüpfungspunkte für rechtliche Verantwortlichkeit ihre Bedeutung. Wer ist haftbar zu machen für Schäden, die im System auftreten? Wer kann noch nachvollziehen und dann im nächsten Schritt auch kontrollieren, welche Entscheidungen in einem solchen System gefällt werden? Welchen Stellenwert kann dann die Individualität des Menschen in einem solchen System noch einnehmen, wenn Steuerung zunehmend im Zeitalter von Big Data über Typizität und Verallgemeinerung verläuft? Wer bestimmt schließlich die Wertigkeit der Entscheidungen, die Ausgestaltung von Präferenzen und die Anpassungsreaktionen in einem solchen System? Individualität wird hier gezielt aufgelöst; systemische Interaktion ersetzt Zuschreibbarkeit von einzelnen Entscheidungen. Dies führt fast zwangsläufig in eine rechtliche Verantwortungsleere.

## *V. Verantwortung und Begrenztes Wissen*

### *1. Verantwortlichkeit trotz fehlenden Wissens*

Das Recht positioniert sich eindeutig zum Zusammenhang von Wissen/Nicht-Wissen und Verantwortlichkeit. Nicht umsonst lernt schon der Student im ersten Semester, was auch Nicht-Juristen als Lehrsatz dazu parat haben: Nicht-Wissen schützt vor Strafe nicht.

Dahinter steht die Erkenntnis, dass Verantwortlichkeit nicht dadurch abgestreift werden kann, dass sich der Verantwortliche selbiger gezielt dadurch entzieht, dass er sie nicht zur Kenntnis nimmt. Nicht das Individu-

um bestimmt seine Verantwortung, sondern das Recht.[34] Dennoch bleibt das Recht auf dieser Stufe nicht stehen. Es erkennt sehr wohl an, dass für die Erkennbarkeit von Verantwortung wiederum Wissen vorhanden sein muss. Und die Rechtswissenschaft weiß seit langem, dass die rechtlich Verantwortlichen oftmals nicht über ausreichendes Wissen verfügen. Daher wird je nach Rechtsregime durchaus unterschieden; das Strafrecht setzt einen anderen Maßstab an zur Beurteilung individuellen Fehlverhaltens als etwa das Öffentliche Recht in seiner Kontrolle (und Lenkung) des demokratischen Gesetzgebers, und auch der Fahrlässigkeitsmaßstab des Zivilrechts differenziert etwa nach Risikosphären und typischen Rollenzuschreibungen.

## *2. Arten und Gründe des Nicht-Wissens als Anknüpfungspunkt für differenzierte Verantwortlichkeiten*

Gleichwohl mag ein kleiner Ausflug erlaubt sein, sich für einen Moment einer Konkretisierung der Nicht-Wissens-Tatbestände zuzuwenden. Diese verschaffen eine größere Klarheit darüber, welche Verantwortungszusammenhänge gestört sein können.

Zu unterscheiden ist einmal objektives Nicht-Wissen von subjektivem Nicht-Wissen, und zwar in Abhängigkeit vom Akteur. Objektives Nicht-Wissen fehlt jedermann, es ist nicht vorhanden. Subjektives Nicht-Wissen dagegen ist grundsätzlich vorhanden, steht allerdings dem Entscheider nicht zur Verfügung. In diese Kategorie fällt die ökonomisch geprägte Informationsasymmetrie.[35] Verantwortung zu konstruieren bei objektiv fehlendem Wissen bedarf einer besonderen Begründung; das Technikrecht kennt es etwa auf der Basis besonders unsicherer technischer Entwicklungen, indem Gefährdungshaftung angeordnet wird - ein Beispiel ist das Atom- oder Gentechnikrecht.

---

34 Siehe Klement, Rechtliche Verantwortung, in: Heidbrink/Langbehn/Sombetzki (Hrsg.), Handbuch Verantwortung, i.E. 2016.

35 Diese stellt allerdings zumeist mehr darauf ab, dass zwischen zwei Subjekten ein Informationsgefälle besteht, also ein Subjekt mehr weiß als ein anderes. Dies ist für die Kategorie des subjektiven Nicht-Wissens nicht zwingend erforderlich, es genügt, dass das Wissen an anderer Stelle vorhanden ist. Um dieses auffinden zu können, bedarf es dann in der Regel eines weiteren Wissens, nämlich des Metawissens über die Organisation von Information.

Nicht-Wissen kann aber auch in Abhängigkeit vom Inhalt des Wissens differenziert werden. Sind andere Akteure nicht bekannt? Fehlt es an einer Kenntnis von deren Präferenzen? Können Interdependenzen nicht aufgeklärt werden? Gibt es keine Technik, die zur Detektion eingesetzt werden könnte? Handelt es sich um sozialwissenschaftliches Wissen, das benötigt wird oder eher um technisches?[36]

Hilfreich kann zudem sein, sich die Ursachen für Nicht-Wissen vor Augen zu führen. Nicht immer ist alles mögliche Wissen auch tatsächlich vorhanden; oft genug sieht beispielsweise das Recht vor, dass Wissen nicht erworben oder nicht weiter beforscht werden darf, etwa bei der Stammzellforschung oder in bestimmten Bereichen der Gentechnik. Neben solchen normativen Gründen des Nicht-Wissens können aber auch schlicht kognitive Gründe vorliegen: Das menschliche Gehirn ist nur begrenzt leistungsfähig, und auch die modernen Supercomputer können nicht alles oder jedenfalls nicht in Echtzeit bearbeiten. Schließlich kann Nicht-Wissen auch ökonomisch bedingt sein: Wenn der Wissensgewinn sich als zu teuer erweist, wird er nicht weiter verfolgt.[37]

Diese verschiedenen Arten und Ursachen für Nicht-Wissen und unsicheres Wissen finden sich wieder in den Möglichkeiten zur Verantwortungszuschreibung. Fehlt es an subjektivem Wissen, kann es in die Verantwortung des Nicht-Wissenden gelegt werden, dieses fehlende Wissen zu beschaffen. Bei normativen Verboten der Wissensgewinnung dagegen wäre es systemwidrig, wenn dies womöglich eine erhöhte Verantwortlichkeit bewirkte. Ein technisch-naturwissenschaftliches Nicht-Wissen mag ermittelbar sein, allerdings nicht für den Einzelnen, sondern nur in einer gesamtheitlichen Beforschung, so dass auch hier der Einzelne in einer anderen Verantwortlichkeit steht.

Nicht-Wissen und Verantwortungszuschreibung stehen also in einem komplexen, durchaus auch multi-normativ zu beschreibenden Zusammenhang.

36 Siehe dazu Spiecker genannt Döhmann, Staatliche Entscheidungen unter Unsicherheit, i.E. 2016.

37 Siehe dazu Spiecker genannt Döhmann, Staatliche Entscheidungen unter Unsicherheit, i.E. 2016.

### *3. Primär- und Sekundärrecht als Umgang mit Unsicherheit in vernetzten Welten*

Das Recht reagiert auf verschiedene Arten und Gründe von Nicht-Wissen zudem noch mit einer weiteren Strukturentscheidung: Es trennt zwischen Primär- und Sekundärrechtsverpflichtungen. Verantwortung wird also auf verschiedenen Ebenen zugewiesen.

#### a) Sekundärrecht

Im Sekundärrecht gilt zunächst einmal das Prinzip der Gleichstellung von Vorsatz und Fahrlässigkeit. Wer wissen könnte, wird also zur Verantwortung gezogen, und zwar im Prinzip in gleicher Weise wie derjenige, der wusste. Erweitert und gleichzeitig begrenzt wird dieser Maßstab durch die Entwicklung von Gefahren- und Risikosphären und dem Merkmal der objektiven Zurechnung.

Vernetzung und Vervielfachung von möglichen Verantwortlichen in der digitalen Welt lassen sich dadurch integrieren, dass das Sekundärrecht zunächst nicht unterscheidet, wer besonders gewichtige Bestandteile zu einer negativen Folge beigetragen hat, sondern mit dem Prinzip der Gesamtschuldnerschaft häufig eine dritte Ebene der Verteilung dem Primär- und dem Sekundärrecht nachlagert. Gleichwohl bleibt auch in dieser Konstruktion das Problem erhalten, dass eine fehlende Zurechnung aus dem System heraus nicht konstruiert werden kann. Hier könnte allerdings das Beweisrecht helfen, das vernetzte Welten als besondere Risikosphären einordnen und damit möglichen Geschädigten privilegierte Nachweispflichten über Verantwortlichkeit einräumen könnte. In diese Kategorie gehörten auch prozessuale Erleichterungen bis hin zu Verbandsklagerechten, um die Position betroffener Individuen zu stärken.[38] Dies bedarf allerdings eines gesellschaftlichen Konsenses, dass Verantwortung konstruiert werden soll.

---

38 Deutscher Richterbund, 08.08.2014, juris; Köpernik, VuR 2014, 240-243; Nietzsch, CR 2014, 272-278.

b) Primärrecht

Weitaus komplexer gestalten sich Anstrengungen des Rechts, Verantwortung in der vernetzten Welt auf der primären Ebene herzustellen und beizubehalten.

Auch hier findet sich die grundsätzliche Zuschreibung von Verantwortung nach Gefahren- und Risikobereichen als ein zentraler Steuerungsmodus im Öffentlichen Recht. Dieses Grundprinzip belässt ausreichend Raum, die konkreten rechtlichen Vorstellungen in Abhängigkeit von Arten, Qualitäten, Gründen und Situationen des Nicht-Wissens auszugestalten. Als zugrundeliegende Wertentscheidungen gilt auch hier die Verfassung: Sie belässt im Grundsatz Chancen und Risiken gleichermaßen Raum; Nicht-Wissen soll nicht zu einem Verharren im Bekannten führen können; Unsicherheit soll Gesetzgeber und Verwaltung nicht binden. Die Produktivität von Unsicherheit soll nutzbar sein für Entwicklung, Fortschritt, Innovation und neue Erkenntnisse. Gleichwohl durchzieht das Technologieregulierungsrecht das Prinzip der Vorsorge. Dieses ist angesichts der Besonderheiten von Information, allen voran der Nicht-Restituierbarkeit des Status Quo ante, auch beim Umgang mit unsicherem Wissen in diesem Bereich zu beachten. Gerade das Datenschutzrecht ist davon im Prinzip geprägt.

Eine mangelnde Ergebniskontrolle und eine unsichere Normativität, die als Folge entsteht, kann in der Konsequenz dann durch gesteigerte Verfahrensanforderungen und -kontrolle ersetzt werden; Recht trägt damit auch zur Konstruktion von Gewißheit bei und kann Rechtsunsicherheit auflösen, jedenfalls verringern.

Nicht zuletzt kann Recht durch die Ausgestaltung von Konfliktlösungsmechanismen und dem Aufbau differenzierter Entscheidungssysteme einer Weiterentwicklung Vorschub leisten.

An allen diesen Elementen kann das Informationsrecht noch gewaltige Anstrengungen unternehmen. Es fehlt an etablierten Konfliktlösungsmechanismen, die Machtungleichgewichte und Hürden der Rechtsverfolgung abmildern. Es gibt noch keine entwickelten Entscheidungsrationalitäten, die veränderten Wertvorstellungen und der Unfähigkeit des Individuums zur Selbst-Verantwortung Rechnung tragen. Es mangelt an einer Begleitung von Vernetzung und Technologieentwicklung im und durch Recht.

Erste Ansätze dazu finden sich in einigen jüngeren Entwicklungen auf europäischer Ebene. Diese sind bezeichnenderweise erste Schritte und können für sich zwangsläufig nicht beanspruchen, eine vollständige Erfas-

sung und Bearbeitung der Problemlagen zu beinhalten. Daher wäre ein enges Monitoring und Begleiten dieser Ansätze wünschenswert, um auch einen Zugewinn an Meta-Wissen strukturiert zu ermöglichen.

Als ein solcher erster Ansatz zählt etwa die Überlegung der Datenschutz-Grundverordnung[39], Meldepflichten für risikobehaftete Datenverarbeitungen vorzusehen.[40] Darin liegt eine deutliche Reaktion auf das Vorliegen von Informationsasymmetrie und subjektiver Unsicherheit, auf die Schwierigkeit des Individuums, seine Selbstverantwortung gegenüber dem Datenverarbeiter wahren zu können. Gleichzeitig geht damit auch eine Konstruktion von Sicherheit zum Abbau von Rechtsunsicherheit einher: Mit der Meldung kann auch eine Prüfung und damit auch eine rechtsverbindliche Beurteilung verlangt werden.[41]

In eine ähnliche Richtung ist auch die Entscheidung des EuGH zum Löschanspruch gegenüber einem Suchmaschinenbetreiber im Internet[42] zu werten: Zum einen wird dem Vorsorgeprinzip ein deutlicher Vorrang eingeräumt, weil man die Besonderheiten der Informationsverarbeitung akzeptiert. Gleichzeitig wird damit aber auch der Boden für neue Konfliktlösungsmechanismen bereitet,[43] wie sie der größte Anbieter auch beschritten hat, indem ein unabhängiger Beirat ins Leben gerufen wurde.[44]

## *VI. Fazit*

Verschiedene Akteure tragen Verantwortung für die Bedingungen der Informationsgesellschaft; zu beobachten sind vielfältige Macht - und Verantwortungsverschiebungen in der digitalen Welt.

Das Individuum ist ein zentraler Akteur in einer Rechtsordnung, die um subjektive Rechte herum strukturiert ist. Dies gilt erst recht für die Ausübung eines Grundrechts wie des Rechts auf informationelle Selbstbestim-

---

39 Die DSch-GVO ist keineswegs in jeder Hinsicht dem Abbau von Unsicherheit in vernetzten Welten förderlich; so ist die Beibehaltung der Technikneutralität ein großes Hindernis, angemessene Einzelregelungen gerade auch für die Problemlagen der vernetzten und autonomen Systeme zu finden.

40 Siehe Erwägungsgrund 76 ff. und Art. 35 ff. DSchGVO.

41 Art. 36 DSchGVO.

42 EuGH Urteil v. 13.05.2014, Rs. C 131/12, EU:C:2014:314 - *Google Spain*.

43 Gleichzeitig wurde vom Gericht offen gelassen, wie solche aussehen können und damit neue Rechtsunsicherheit produziert.

44 Google Beirat, vgl. https://www.google.com/intl/de/advisorycouncil/.

mung, das aktiv als Selbstbestimmungs- und damit auch als Selbstverantwortungsrecht konstruiert ist. Gleichwohl hat schon das Bundesverfassungsgericht erkannt, dass u.a. unsicheres Wissen der Ausübung dieser Selbstverantwortung entgegensteht und es daher begleitender rechtlicher Regelungen bedarf. In der digitalen Informationswelt bleibt das Individuum fast machtlos und damit auch verantwortungslos: Erhebliche Vollstreckungsdefizite von rechtlichen Regelungen, die auch durch die Technik selbst kaum aufgefangen werden können, eine fehlende Anpassung bestehender normativer Vorstellungen und vor allem aber die Verschränkung und gleichzeitige Auflösung von Verantwortlichkeiten hindern.

Es bleibt die Kernaufgabe des Rechts, Verantwortlichkeit zuzuweisen und dem Sich-Entziehen von Zuschreibung und Verantwortung entgegenzuwirken. Daher kann und muss ein modernes Rechtssystem die Verantwortung des Einzelnen unter Unsicherheitsbedingungen in der vernetzten Welt stärken durch eine kluge Rechtsgestaltung, die auch systemische Aspekte integriert.

# Zur Reichweite der staatlichen Verantwortung für Teilhabe in der digitalen Zeit

*Alexander Roßnagel*

Die Digitalisierung nahezu aller Lebensbereiche verändert die Verwirklichungsbedingungen für staatliche Verantwortung und für die Wahrnehmung von Grundrechten erheblich. Dies gilt auch für die Teilhabefunktion der Grundrechte und für die staatliche Verantwortung dafür, die gebotene Teilnahme zu ermöglichen. Welche Veränderungen eingetreten sind und eintreten werden und wie unter diesen der Staat seiner Verantwortung gerecht werden kann, sind die Themen dieses Beitrags. Er wird im ersten Teil die staatliche Verantwortung für Teilhabe in der digitalen Zeit klären und sich dann im zweiten Teil Herausforderungen und Ansätzen zuwenden, dieser Verantwortung in einzelnen beispielhaften Handlungsfeldern gerecht zu werden.

## *I. Verantwortung*

Im ersten Teil wird die These vertreten, dass die staatliche Verantwortung für Teilhabe nicht nur den gleichen Zugang zu staatlichen Monopolveranstaltungen betrifft, sondern auch die Gewährleistung von Voraussetzungen der Grundrechtsverwirklichung durch Teilhabe und Schutz.

### *1. Bezugsrahmen Internet*

Diese These soll für den Bezugsrahmen des Handelns im Internet begründet werden. Diese Beschränkung schließt vor allem die Probleme aus, die durch die Nutzung von Hardware und Software als solche – ohne Vernetzung – entstehen.

Internet bedeutet heute nicht mehr nur das Netz der Netze, das einen weltweiten und extrem schnellen Austausch von Daten ermöglicht.[1] Internet ermöglicht vielmehr auch die Kombination und den Austausch beliebiger Datenformate und damit multimediale Kommunikation.[2] Es bietet Zugang zu beliebig skalierbaren Speichern für große Datenmengen und Softwareprogrammen, die in Form des Cloud Computing von jedem genutzt werden können.[3] Es stellt vielfältige Plattformen für soziale Interaktionen in Form von Social Netzworks und anderen Web 2.0-Anwendungen bereit.[4] Wer diese Angebote im Internet nutzt, hinterlässt jedoch bei jeder Handlung Datenspuren, die durch Big Data-Analyseinstrumente, die ebenfalls im Internet angeboten werden, trotz ihre großen Menge und trotz unterschiedlicher Formate in hoher Geschwindigkeit ausgewertet werden können.[5]

Das Internet weist spezifische Eigenschaften auf, die die Wahrnehmung staatlicher Verantwortung sehr erschweren. Dies betrifft zum einen die räumliche Dimension: Das Internet kann weltweit genutzt werden – sowohl von dem, der digitale Informationen und Handlungsmöglichkeiten anbietet, als auch von demjenigen, der diese nachfragt. Diese Globalität des Regelungsgegenstands erschwert die Wahrnehmung von Verantwortung für Nationalstaaten oder den regionalen Zusammenschluss von Staaten ungemein. Dies betrifft zum anderen die Konsistenz digitaler Daten. Sie sind unkörperlich und ermöglichen ein virtuelles Leben im Cyberspace. Die körperliche Ausübung staatlicher Macht, ist nur sehr schwer möglich. Dies hat drittens Auswirkungen auf die zeitliche Dimension. Das Handeln im Internet ist in dreierlei Hinsicht zeitlos. Einerseits benötigt die Überbrückung von Raum so gut wie keine Zeit. Digitale Daten sind gleichzeitig überall auf der Welt verfügbar. Andererseits sind digitale Daten ohne Geschichte, Veränderungen sind nicht erkennbar.[6] Schließlich

1 S. hierzu Roßnagel, ZRP 1997, 26 ff.
2 S. z.B. die Beiträge in Kubicek/Klumpp/Fuchs/Roßnagel (Hrsg.), Internet@Future, Jahrbuch Telekommunikation und Gesellschaft 2001.
3 S. z.B. BITKOM, Cloud-Computing – Evolution in der Technik, Revolution im Business, 2009; Kroschwald, Informationelle Selbstbestimmung in der Cloud, 2015.
4 S. z.B. Dörfel/Hotho/Kartal-Aydemir/Roßnagel/Stumme, Informationelle Selbstbestimmung im Web 2.0, 2013.
5 S. z.B. Roßnagel/Nebel, DuD 2015, 455 f. m.w.N.
6 Roßnagel, in: ders. (Hrsg.), Recht der Telemediendienste, 2013, Einl. ins SigG, Rn. 8.

sind Daten im Internet praktisch nicht zu löschen. Irgendwo sie sie immer gespeichert: „Das Internet vergisst nichts“. Schließlich zeichnet sich als vierte spezifische Eigenschaft des Internet die Ausweitung seines Wirkungsbereichs ab, indem es die körperliche und die virtuelle Welt verbindet.[7] Dies erfolgt in beiden Richtungen. Durch das Internet der Dinge werden Handlungen in der körperlichen Welt im Internet abgebildet.[8] Umgekehrt wird die körperliche Welt durch „Augmented Reality“ mit digitalen Informationen angereichert.[9]

Die Entwicklungen im Internet sind hochdynamisch. Niemand weiß verlässlich, wohin sich das Internet und seine gesellschaftlichen Folgen entwickeln. Derzeit sind viele unterschiedliche Entwicklungstrends möglich, die die Rahmenbedingungen der Wahrnehmung staatlicher Verantwortung erheblich beeinflussen. Das Internet bietet viele Ansatzpunkte für eine „Civil Information Society“, in der demokratische Teilhabe, Mitbestimmung der Bürger in öffentlichen Entscheidungen und Selbstbestimmung der Bürger über die Wahrnehmung ihrer Freiheitsbereiche gefördert werden.[10] Das setzt allerdings das vielfältige selbstbewusste Ergreifen von Handlungsmöglichkeiten im Internet durch die Bürger mit Unterstützung vieler staatlicher Stellen voraus. Verstärkt sich dagegen die Ökonomisierung des digitalen Lebens wird das Internet durch den Globalkapitalismus von Internetgiganten geprägt werden. Die Enthüllungen von Edward Snowden zeigen aber noch eine weitere Entwicklungsmöglichkeit auf, nämlich das Internet als globalen Überwachungsraum eines Hegemonialstaats, der alle Regungen im Internet kontrolliert.

## *2. Verantwortung*

Wenn nach der staatlichen Verantwortung gefragt wird, sollte unter Verantwortung das Einstehen für bestimmte Handlungen oder Entwicklungen verstanden werden.[11] Dieses Einstehen kann nur erwartet werden, wenn

7 S. z.B. Roßnagel/Sommerlatte/Winand, Digitale Visionen, 2008.
8 S. z.B. Fleisch/Mattern, Internet der Dinge, 2005. Zu den Auswirkungen von Ubiquitous Computing auf den Datenschutz s. z.B. Roßnagel, Datenschutz in einem informatisierten Alltag, 2007.
9 S. z.B. für das vernetzte Automobil Hansen, DuD 2015, 367.
10 S. hierzu Roßnagel, ZRP 1997, 26 ff.; Schaar, Das digitale Wir, 2015.
11 S. z.B. Saladin, Verantwortung als Staatsprinzip, 1984.

derjenige, der Verantwortung tragen soll, über ausreichendes Wissen[12] und relevante Möglichkeiten des Handelns verfügt.

Wird nach der Reichweite staatlicher Verantwortung gefragt, sind daher mehrere Begrenzungen zu beachten: Zum einen bestehen Begrenzungen hinsichtlich des Trägers der Verantwortung: „Staat" bezeichnet nicht ein einziges homogenes Gebilde, sondern ist ein Sammelbegriff, der viele selbstständige Körperschaften und deren unselbständige organisatorische Untergliederungen umfasst. Diese haben zwar eine einheitliche Rechtsordnung und vergleichbare und abgestimmte Funktionen, die sie arbeitsteilig erfüllen. Sie verfolgen aber vielfach unterschiedliche Interessen, so dass es schwer fällt, diesen allen eine einheitliche Verantwortung zuzuordnen. Sinnvoller erscheint es, von einer staatlichen Verantwortung des Bundes oder eines Landes oder einer ausgegliederten organisatorischen Einheit zu sprechen. Zum anderen bestehen für die staatliche Verantwortung sachliche Begrenzungen: Die Träger der staatlichen Verantwortung haben bestimmte Staatsaufgaben, für deren Erfüllung sie einstehen müssen. Diese Staatsaufgaben sind begrenzt, um die Freiheit der Staatsbürger zu gewährleisten, und damit auch die aus diesen Aufgaben folgende Verantwortung. Drittens besteht eine personelle Begrenzung: Die Verantwortung eines staatlichen Verantwortungsträgers besteht nur gegenüber seinen Staatsbürgern und Einwohnern. Eng mit der sachlichen Begrenzung ist viertens die modale Begrenzung der Verantwortung zu sehen: Je nach Staatsaufgabe trifft den Staat eine Erfüllungs-, Gewährleistungs-, Folgen- oder Auffangverantwortung, so dass der Staat für verschiedene Entwicklungen in unterschiedlicher Weise Verantwortung trägt.[13] Fünftens besteht eine zeitliche Begrenzung staatlicher Verantwortung: Sie besteht zwar verfassungsrechtlich nicht nur für die drei gegenwärtigen Generationen, sondern auch für künftige Generationen. Doch muss der Anspruch, durch staatliches Handeln auch der Verantwortung für künftige Generationen gerecht zu werden, mit dem zeitlichen Abstand zu diesen abnehmen. Je größer dieser ist, umso weniger Wissen ist über die Auswirkungen heutigen Handels auf künftige Lebensbedingungen und die Erwartungen künftiger Generationen verfügbar. Die stärkste Begrenzung staatlicher Verantwortung besteht jedoch in der Diskrepanz zwischen der weltweiten Entwicklung der Infor-

12 Zum Problem mangelnden Wissens s. den Beitrag von Spiecker in diesem Band.

13 S. z.B. Schulze-Fielitz, Grundmodi der Aufgabenwahrnehmung, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band I, 2. Aufl. 2012, 893 ff.

mations- und Kommunikationstechnik und der räumlichen Begrenzung staatlicher Handlungsmacht auf das jeweilige Staatsgebiet. Diese wird zwar dadurch reduziert, dass sich viele Staaten in Europa zur Europäischen Union zusammengeschlossen haben. Diese kann in einem weiteren räumlichen Umfeld staatliche Verantwortung wahrnehmen als ihre Mitgliedstaaten. Dennoch ist auch der Handlungsbereich der Europäischen Union auf einen begrenzten Raum beschränkt.

### *3. Teilhabe*

Um zu beurteilen, welche Verantwortung staatliche Stellen für die Teilhabe am Internet haben, kann eine enge oder eine weite Sicht rechtlich verbürgter Teilhabe eingenommen werden. Eine enge Sicht fragt nach der Teilhabe als originäres subjektives öffentliches Recht. Ein solches hat das Bundesverfassungsgericht seit dem Numerus-Clausus-Urteil für staatliche Ausbildungsleistungen mit Monopolcharakter anerkannt. Danach besteht zum Beispiel ein Teilhabeanspruch aus dem Grundrecht auf freie Wahl der Ausbildungsstätte nach Art. 12 Abs. 1 Var. 3 GG und dem Sozialstaatsprinzip nach 20 Abs. 1 GG für die Teilnahme am Hochschulstudium oder der Referendarausbildung.[14] Das Grundrecht auf Wahl der Ausbildungsstätte ist ohne die tatsächlichen Voraussetzungen, staatliche Ausbildungsleistungen in Anspruch nehmen zu können, wertlos. Dieser Teilhabeanspruch gilt jedoch immer nur im Rahmen des Möglichen.[15]

Eine weite Sicht fragt nach den Leistungsverpflichtungen des Staates, die sich auch aus vielen anderen Grundrechten ergeben können. Sie knüpft an dem objektiven Gehalt der Grundrechte an. Diese zielen darauf ab, dem Grundrechtsträger reale Freiheit zu gewährleisten. Mit Blick auf ihre objektiven Gehalte lassen sich auch primär abwehrrechtlichen Grundrechtsbestimmungen im Sinn einer Gewährleistung realer Freiheit leistungsrechtliche Zusatzelemente abgewinnen.[16] Diese Gewährleistung setzt oft „Realisierungshilfen“ durch staatliche Vorleistungen oder den Schutz des Staates vor einer Beeinträchtigung durch Dritte voraus, wenn Grundrechte tatsächlich verwirklicht werden sollen. Wenn aus dieser Perspektive der

14 S. BVerfGE 33, 303 ff.; 43, 291 (313 f.).
15 S. z.B. BVerfGE 33, 303 (333).
16 S. hierzu die Nachweise in Murswiek, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts, Band IX, 3. Aufl. 2011, § 192 Rn. 91 ff.

Staat einen objektiven Schutz- oder Leistungsauftrag hat, schließt sich die Frage an, ob einzelne einen grundrechtlichen Anspruch darauf haben sollen, an diesen Leistungen teilzuhaben. Teilhabe kann so als Funktion der Grundrechte angesehen werden, die auf staatliche Leistungen angewiesen sind.

## *4. Verantwortung für Teilhabe*

Zur Bestimmung der Verantwortung für Teilhabe in der digitalen Zeit kommt man also, indem man fragt, welche Gewährleistung der Verwirklichungsbedingungen von Grundrechten durch den Staat notwendig sind, um durch die Nutzung von Informations- und Kommunikationstechniken tatsächlich realisierte Freiheit zu erreichen.[17] Dabei sind folgende Aspekte zu beachten: In der digitalen Welt sind vor allem die technische Bedingungen der Grundrechtsverwirklichung zu berücksichtigen und zu gestalten. Viele dieser Bedingungen werden von Privaten angeboten, so dass sich die Frage stellt, zu welchen Bedingungen eine Teilhabe an Grundrechtsvoraussetzungen in privaten Angeboten möglich sein soll. Zwar ist die Vertragsfreiheit aller Parteien am Markt zu achten. Diese darf aber nicht nur die Durchsetzung des Rechts des Stärkeren fördern und zu unfairen Vertragsbedingungen führen. Der Staat muss daher die Bedingungen der Teilhabe an diesen Angeboten überprüfen und unter Umständen für diese einen Rahmen setzen, der Fair Play gewährleistet. In extremen Fällen muss er vor Privaten, die in Grundrechte eingreifen, Schutz bieten, die Grundrechtsbereiche der widerstreitenden Interessen im Sinn praktischer Konkordanz gegeneinander abgrenzen und alle an einem Grundrechtsausgleich zwischen den widerstreitenden privaten Interessen teilhaben lassen. Soweit Informations-, Ressourcen- und Machtasymmetrien bestehen, kann Grundrechtsverwirklichung auf einen Ausgleich mit anderen Grundrechten angewiesen sein. Im Ergebnis besteht eine Verantwortung staatlicher Stellen für den Zugang, den Schutz und den Ausgleich für private Veranstaltungen im Internet, die für die Grundrechtsverwirklichung kritisch sind.

17 S. z.B. Roßnagel, Rechtswissenschaftliche Technikfolgenforschung, 1993, 19, 241 ff.

### 5. Verantwortungswahrnehmung

Für die Verantwortungswahrnehmung ist dabei der Regelungsgegenstand und seine Bedeutung für die Grundrechte zu beachten:

Soweit es um Marktangebote geht, muss der Staat eine Marktverantwortung wahrnehmen. Er muss die Marktgesetze beachten und die Grundrechte der Marktteilnehmer respektieren, zugleich aber die Verwirklichungsbedingungen dieser Grundrechte sichern und die Voraussetzungen gewährleisten, dass der Markt mit konkurrierenden Angeboten und freier Nachfrage überhaupt funktionieren kann.

Die Wahrnehmung der Grundrechte im Internet setzt viele funktionierende Infrastrukturen voraus. Die Infrastrukturverantwortung des Staates fordert von ihm, die notwendigen Infrastrukturen selbst zur Verfügung zu stellen oder zu gewährleisten, dass andere dies tun. Dies gilt vor allem für kritische Infrastrukturen, die für das Zusammenleben in einer Gesellschaft von entscheidender Bedeutung sind. Sie sind zu sichern und zu schützen. Diese Infrastrukturverantwortung umfasst aber auch die Aufgabe, die Teilhabe an diesen Infrastrukturen zu ermöglichen und sicherzustellen sowie gerechte Bedingungen für ihre Nutzung zu gewährleisten.

Schließlich kommt dem Staat auch eine Innovationsverantwortung zu.[18] Innovationen sind für die Anpassung der Gesellschaft an sich ändernde Umstände entscheidend. Der Staat muss Innovationen ermöglichen, sozialnützliche Innovationen anreizen, Innovationsfolgen abschätzen und steuern und sozialschädliche Innovationen verhindern, erschweren oder ausgleichen.[19]

## II. Verantwortungsfelder

Im zweiten Teil des Beitrags wird die These vertreten, dass die staatliche Verantwortung für Teilhabe in der digitalen Zeit viele unterschiedliche

---

18 S. Hoffmann-Riem, Innovationen durch Recht und im Recht, in: Schulte (Hrsg.), Technische Innovation und Recht – Antrieb oder Hemmnis?, 1996, 3 ff.; Eifert/Hoffmann-Riem (Hrsg.), Innovationsfördernde Regulierung, 2009; Eifert/Hoffmann-Riem (Hrsg.), Innovationsverantwortung, 2009.

19 Roßnagel, Innovation als Gegenstand der Rechtswissenschaft, in: Hof/Wengenroth (Hrsg.), Innovationsforschung – Ansätze, Methoden, Grenzen und Perspektiven, 2. Aufl. 2010, 9 ff.; Hornung, Grundrechtsinnovationen, 2015, 161 ff.

Handlungsfelder betrifft. Sie fordert Angebote zur Grundrechtsverwirklichung, die staatliche Verantwortungsträger inzwischen auch schon weitgehend erbringen. Einige Beispiele für Herausforderungen und Lösungen werden dargestellt.

## *1. Infrastrukturen*

Entscheidende Voraussetzung für das Leben in der digitalen Zeit ist der Zugang und die Nutzung von Infrastrukturen, auf denen diese technisch geprägte Welt aufbaut. Notwendig hierfür sind die Gewährleistung des Zugangs zu den unverzichtbaren Infrastrukturen zu fairen Bedingungen, die Sicherstellung der Marktkonkurrenz zwischen den Anbietern solcher Infrastrukturen und die Gewährleistung von realer Vertragsfreiheit nicht nur für den Anbieter der Infrastrukturleistungen, sondern auch für den Nutzer. Dabei muss die Grundregel gelten, dass den Anbieter von Infrastrukturdienstleistungen umso höhere Verpflichtungen treffen, je höher sein Marktanteil ist. Denn wegen der Netzwerkeffekte ist die Teilhabe an diesen Dienstleistungen für die Grundrechtsverwirklichung umso wichtiger, je mehr Teilnehmer diese Infrastruktur nutzen.

Die staatliche Verantwortung richtet sich auf die Gewährleistungen des fairen Zugangs und der sinnvollen Nutzung der für die Grundrechtsverwirklichung unverzichtbaren Infrastrukturen.[20] Hierfür ist eine Unterscheidung zwischen Grundfunktionen der Infrastrukturen und darüberhinausgehenden Zusatzfunktionen erforderlich. Der grundrechtliche Teilhabeanspruch kann nur für Grundfunktionen bestehen. Die staatliche Gewährleistung beschränkt sich auf die fairen Bedingungen ihrer Inanspruchnahme, etwa durch eine geeignete und wirksame Kontrolle Allgemeiner Geschäftsbedingungen.

Ein Beispiel für unverzichtbare Infrastrukturen in der digitalen Zeit sind Suchmaschinen. Sie bieten in der Überfülle von Daten die Grundfunktionen für das Finden und Gefundenwerden von bestimmten Informationen. Ihre freie und faire Nutzung ist daher die notwendige Voraussetzung für die wirksame Ausübung der Informationsfreiheit (Finden von Informationen) und der Meinungs- und Pressefreiheit (Gefundenwerden von Berich-

20 S. z.B. Roßnagel, Infrastrukturverantwortung des Staats und Eigenverantwortung des Bürgers, in: Kubicek/Klumpp/Büllesbach/Fuchs/Roßnagel (Hrsg.), Innnovation@Infrastruktur, Jahrbuch für Telekommunikation und Gesellschaft 2002, 269 ff.

ten und Meinungsäußerungen). Notwendige Anforderungen an Suchmaschinen sind daher objektive Suchalgorithmen und die Verhinderung von Diskriminierung. Staatliche Verantwortung erstreckt sich somit auf die Gewährleistung eines Teilhabeanspruch für Grundfunktionen zu fairen Bedingungen und des Schutzes von Persönlichkeitsrechten[21] sowie eines geeigneten rechtlichen Rahmens, um diese Rechte (unter Umständen in Form eines Kontrahierungszwangs) auch durchsetzen zu können.[22]

Ein weiteres Beispiel unverzichtbarer Infrastrukturen sind inzwischen auch Soziale Netzwerke. Sie bieten die Grundfunktionen für soziale Interaktionen in der digitalen Welt. Die Verwirklichung von Grundrechten, die diese sozialen Interaktionen schützen sollen, wie zum Beispiel die freie Entfaltung der Persönlichkeit, die Informationsfreiheit, die Meinungsfreiheit, die Wissenschaftsfreiheit, die Vereinigungsfreiheit und die Berufsfreiheit, ist auf die Nutzung dieser Infrastrukturen angewiesen. Auch bei ihnen erstreckt sich die staatliche Verantwortung auf die Gewährleistung einer Teilhabe zu fairen Bedingungen und des Schutzes von Persönlichkeitsrechten. Ebenso wie bei Suchmaschinen muss auch bei Sozialen Netzwerken gewährleistet werden, dass diese Ansprüche bezogen auf Grundfunktionen durchgesetzt werden können.[23]

### *2. Informationen*

Für nahezu jede Grundrechtsausübung sind Informationen notwendig – in der Informationsgesellschaft in gesteigerter Form. Daher ist eine Informations- und Kommunikationsordnung, die den Zugang zu Informationen und ihre Nutzung regelt, für die digitale Welt unabdingbar.

Dies gilt vor allem für Informationen, über die der Staat selbst verfügt. Auf sie zugreifen zu können und sie nutzen zu können, ist Grundvoraussetzung für demokratische Meinungs- und Willensbildung, für rechtsstaatliche Kontrolle und für die Grundrechtsausübung gegenüber staatlicher Macht. Aufgabe staatlicher Verantwortung ist daher, diese Informationen aktiv zur Verfügung zu stellen, den Zugang zu diesen Informationen zu

21 S. EuGH vom 13.5.2914, C-131/12 (Google).

22 S. hierzu Jandt, Technikadäquate Grundrechtsentwicklung, Habilitationsschrift Kassel, 2015, 326 ff.

23 S. EuGH vom 6.10.2015, C-362/14 (Facebook); Jandt, Technikadäquate Grundrechtsentwicklung, Habilitationsschrift Kassel, 2015, 371 ff.

gewährleisten und ihre Nutzung zu ermöglichen. Zugleich muss aber sichergestellt werden, dass schützenswerte Geheimnisse gewahrt und Persönlichkeitsrechte geschützt werden.[24] Diesen Aufgaben ist der Staat in der Bundesrepublik Deutschland weitgehend gerecht geworden, indem er Informationspflichten staatlicher Stellen, den Zugang zu staatlichen Informationen und die Möglichkeit ihrer Weiternutzung in den Informationsfreiheitsgesetzen,[25] dem Informationsweiterverwendungsgesetz[26] und dem E-Government-Gesetz[27] geregelt hat.

Auf freien Zugang zu Informationen und freien Umgang mit ihnen sind auch Wissenschaft und Kultur angewiesen. Freiheit von Forschung und Lehre setzten sowohl die freie Veröffentlichung wissenschaftlicher Ergebnisse und der ihnen zugrundeliegenden Forschungsdaten als auch den freien Zugang zu wissenschaftlichen Publikationen und veröffentlichen Forschungsdatensammlungen voraus. Das Internet hat diese Möglichkeiten rein technisch erheblich verbessert. Die Qualitätssicherung wissenschaftlicher Ergebnisse setzt allerdings über die rein technischen Möglichkeiten der Publikation im Internet hinaus Verfahren der Selbstkontrolle durch die Wissenschaft voraus. Die Publikation wissenschaftlicher Ergebnisse und der Zugang zu diesen dürfen nicht durch die Monopolisierung und die ökonomische Macht großer Verlage gefährdet werden. Vielmehr muss die Informationsversorgung der Wissenschaft zu vertretbaren Bedingungen gewährleistet werden. Staatliche Verantwortung für die Grundrechtsverwirklichung kann sich daher auch darauf erstrecken, „Open Access" zu Wissenschaftspublikationen zu fairen Bedingungen und unter wissen-

24 S. Roßnagel, MMR 2007, 16 ff.; 2006; Der Hessische Datenschutzbeauftragte/Der Präsident des Hessischen Landtags (Hrsg.), Informationsfreiheit und Datenschutz, 2007.

25 S. z.B. Informationsfreiheitsgesetz vom 5.9.2005, BGBl. I, 2722; s. hierzu Gallwas, NJW 1992, 2785; Sokol, Informationszugang und Datenschutz, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 1803; Kugelmann, NJW 2005, 3609; Schnabel, ZD 2012, 493; Schoch, NJW 2009, 2987; ders., Informationsfreiheitsgesetz, 2009.

26 S. z.B. Informationsweiterverwendungsgesetz vom 13.12.2006, BGBl. I, 2913; Schoch, NVwZ 2006, 872.

27 S. z.B. E-Government-Gesetz vom 25.7.2013, BGBl. I, 2749; s. zu diesem z.B. Roßnagel, NJW 2013, 2710; Albrecht/Schmid, KuR 2013, 529.

schaftlicher Selbstkontrolle zu gewährleisten[28] und den Zugang und den Schutz von Forschungsdaten zu regeln.

In ähnlicher Weise ist in der digitalen Zeit eine staatliche Verantwortung für den freien Zugang zu einer kulturellen Grundversorgung[29] zu begründen. Diese manifestiert sich in erster Linie in einer staatlichen Beobachtungspflicht hinsichtlich der kulturellen Angebote in den Medien und in einer punktuellen Intervention, wenn Missbräuche von Informations- oder ökonomischer Macht zu erkennen sind. Diese Verantwortung kann auch die Förderung bestimmter unterrepräsentierter kultureller Angebote umfassen. In der digitalen Welt, die auf der Nutzung technischer Systeme beruht, muss sich die Informationsverantwortung auch auf den ausreichenden Zugang zu technischen Informationen erstrecken, die für die technische Verwirklichung von Grundrechtsausübungen erforderlich sind.

Von hoher Bedeutung für die Grundrechtsausübung sind Suchinformationen. Um sie auf den Suchenden abzustimmen, nutzen die Suchalgorithmen das Persönlichkeitsprofil, das sie aufgrund früherer Anfragen angelegt haben, sowie die ihnen bekannten Umstände der Suche (z.B. Ort und technische Ausstattung des Suchenden). Dies kann dazu führen, dass dem Suchenden nur solche Informationen angeboten werden, die zu seinem Weltbild und seinen Präferenzen passen. Eine Auseinandersetzung mit „störenden" Informationen oder anderen Meinungen wird dadurch vermieden. Dies kann zur Bestärkung bereits bestehender Meinungen und Weltsichten führen. Dieser „Kreislauf" beeinflusst die individuelle Meinungsbildung und die kollektive demokratische Willensbildung. Wie für andere Medien[30] kann sich daher auch für Suchmaschinen eine staatliche Verantwortung für Vielfaltsicherung und Diskriminierungsfreiheit ergeben.[31]

---

28 S. z.B. die Berliner Erklärung über offenen Zugang zu wissenschaftlichem Wissen vom 22.10.2003, https://de.wikipedia.org/wiki/Berliner_Erkl%C3%A4rung_%C3%BCber_offenen_Zugang_zu_wissenschaftlichem_Wissen.

29 Zur kulturellen Grundversorgung durch den öffentlich-rechtlichen Rundfunk s. BVerfGE 73, 118 (157 f.); 74, 297 (324 f.); 83, 238 (297 f.).

30 S. BVerfG 73, 118 (158 f.); 83, 238 (315); 87, 181 (199); 97, 228 (257); 114, 371 (387).

31 S. hierzu Jandt, Technikadäquate Grundrechtsentwicklung, Habilitationsssschrift Kassel, 2015, 363 f.

### 3. Instrumente des Rechtsverkehrs

Die staatliche Verantwortung erstreckt sich auch darauf, die rechtssichere Kommunikation in der digitalen Zeit zu ermöglichen. Es geht vor allem um die Instrumente, die Willenserklärungen und ihre Übermittlung so absichern, dass an ihre Verwendung Rechtsfolgen geknüpft und mit ihnen Beweismittel erzeugt werden können. Hierzu bedarf es geeigneter rechtlicher Regelungen.[32]

Für eine rechtsverbindliche Kommunikation unter Abwesenden ist eine sichere Identifizierung der Beteiligten notwendig. Dies erfordert in der digitalen Zeit elektronische Identitätsnachweise. Ihre Erzeugung, ihr Einsatz und ihre Verwaltung setzen eine geeignete Identitätsinfrastruktur und ein wirksames Identitätsmanagement voraus.[33] Technische Instrumente dafür sind elektronische Ausweise. Die staatliche Verantwortung für die Identitätsinfrastruktur und das Identitätsmanagement ist bisher dadurch erfüllt worden, dass die Ausstellung und Verwendung elektronischer Ausweise in §§ 18 ff. PAuswG,[34] § 78 Abs. 5 Aufenthaltsgesetz[35] und § 6 De-Mail-G[36] geregelt wurden und ihre rechtswirksame Verwendung zum Beispiel in § 3 a Abs. 2 VwVfG ermöglicht wurde. Eine gegenseitige Anerkennung amtlicher Identitätsnachweise der Mitgliedstaaten im europäischen Markt regelt die Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-VO)[37] in Art. 6 bis 12.

Über die Identifizierung der Kooperationspartner hinaus sind weitere (beweis)sichere Instrumente zur Teilnahme am elektronischen Rechtsverkehr notwendig, die nachweisbar die Abgabe von Willenserklärungen und

---

32 S. z.B. Roßnagel/Hornung/Knopp, Verfassungsrechtliche Visionen für E-Government, in: Bundesministerium für Wirtschaft und Technologie (Hrsg.), Dritter Nationaler IT-Gipfel – Arbeitsgruppe 3 – Szenarien für die Zukunft – Anregungen für eine „Deutsche E-Government-Gesamtstrategie“, 2008, 11 ff.

33 Reichl/Roßnagel/Müller, Digitaler Personalausweis. Eine Machbarkeitsstudie, 2005; Hornung, Die digitale Identität, 2005.

34 Personalausweisgesetz vom 18.6.2009, BGBl. I, 1346), geändert durch Art. 1 des Gesetzes vom 20.6.2015, BGBl. I, 970, s. näher Hornung/Möller, PassG – PAuswG, Kommentar, 2011.

35 Aufenthaltsgesetz vom 25.2.2008, BGBl. I, 162, geändert durch Art. 2 des Gesetzes vom 28.10.2015, BGBl. I, 1802.

36 De-Mail-Gesetz vom 28.4.2011, BGBl. I, 666; s. Roßnagel, NJW 2011, 1473.

37 Verordnung Nr. 910/2014, EU ABl. L 257 vom 28.8.2014, 73; s. z.B. Hoffmann, DuD 2014, 765 ff.; Roßnagel, NJW 2014, 3686; ders., MMR 2015, 359.

deren Zustellung ermöglichen.[38] Solche technischen Instrumente bilden elektronische Signaturen, elektronische Siegel, elektronische Zeitstempel und elektronische Absende- und Zustellbestätigungen. Ihre Erzeugung und Verwaltung setzen eine Vertrauensinfrastruktur voraus, in der Vertrauensdiensteanbieter zusammenarbeiten und ihre Vertrauensdienste anbieten. Die staatliche Verantwortung umfasst Regelungen zu Anforderungen an die Sicherheit und Qualität dieser Dienste sowie die Kontrolle dieser Angebote und die Durchsetzung der Qualitätsanforderungen. Solche Regelungen zu Vertrauensinfrastrukturen, Anforderungen an Anbieter und Rechte der Nutzer enthalten Art. 13 bis 46 der eIDAS-VO,[39] das Signaturgesetz und die Signaturverordnung[40] sowie das De-Mail-G.[41]

Die staatliche Verantwortung erstreckt sich auch auf die Rechtsfolgen, die mit der Verwendung dieser Instrumente im elektronischen Rechtsverkehr verbunden sein sollen. Die Rechtsfolgen beim Einsatz elektronischer Identitätsnachweise und gesicherter elektronischer Willenserklärungen in der digitalen Welt sollen gleichwertig sein mit Identitätsnachweisen und Willenserklärungen in der körperlichen Welt. Dieser Verantwortung ist der Gesetzgeber nachgekommen, indem er gleichwertige Rechtsfolgen bei Einsatz sicherer Informationstechnik im Rechtsverkehr geregelt hat. Er hat in vielen Regelungen die elektronische Form unter Verwendung von elektronischen Ausweisen oder qualifizierten elektronischen Signaturen mit der Schriftform mit eigenhändiger Unterschrift gleichgestellt – etwa in § 126 Abs. 3 BGB, in § 3 a Abs. 2 VwVfG, in § 87 a AO oder in § 35 SGB I.[42] Vorschriften, die in besonderer Weise gesicherte elektronische Dokumente in vergleichbarer Weise regeln wie den Urkundenbeweis, fin-

38 S. hierzu Roßnagel, in: ders. (Hrsg.), Recht der Telemediendienste, 2013, Einführung ins SigG, Rn. 7 ff.

39 S. Roßnagel, NJW 2014, 3686; ders., MMR 2015, 359.

40 S. hierzu die Kommentierung von SigG und SigV in: Roßnagel (Hrsg.), Recht der Telemediendienste, 2013; in: Manssen (Hrsg.), Telekommunikations- und Multimediarecht, Loseblatt; in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015.

41 S. hierzu Roßnagel, NJW 2011, 1473.

42 S. hierzu z.B. Jandt und Roßnagel, in: Roßnagel (Hrsg.), Recht der Telemediendienste, 2013, § 126 BGB, Rn. 8 ff., § 3 a VwVfG, Rn. 20 ff.

den sich in § 371 a und b ZPO[43] sowie in Art. 35 Abs. 2, 41 Abs. 2 und 42 Abs. 2 eIDAS-VO.[44]

### 4. Elektronische Verwaltung

Ein spezieller Bereich des elektronischen Rechtsverkehrs betrifft die elektronische Verwaltung. In der digitalen Zeit soll der Staat selbst auch in der elektronischen Welt präsent sein und in seinen Verwaltungseinheiten und zwischen diesen sowie mit seinen Bürger auf elektronische Weise kommunizieren.

Die Bürgerkommunikation setzt nicht nur eine Präsenz der Verwaltung im Internet und eine einseitige Kommunikation mit dem Bürger voraus, indem die Verwaltung im Netz elektronische Mitteilungen und Verkündungen zum Abruf bereithält. Vielmehr erfordert sie von der Verwaltung auch kompatible gesicherte Kommunikationsstrukturen, die einen bilateralen Austausch von Informationen und Willenserklärungen ermöglichen.[45] Dies bedeutet nicht nur, dass sie elektronische Nachrichten empfangen und versenden kann, sondern dass sie auch qualifizierte elektronische Signaturen erstellen und prüfen kann sowie elektronische und gescannte Dokumente akzeptiert und verarbeiten kann.[46] Wie im allgemeinen elektronischen Rechtsverkehr müssen auch in der Kommunikation mit der Verwaltung als Sicherungsinstrumente elektronische Signaturen, De-Mail und elektronische Ausweise eingesetzt werden können. Die staatliche Verantwortung besteht darin, die Verwaltungsbehörden zur elektronischen Bürgerkommunikation zu verpflichten und ihnen rechtlich, technisch und finanziell die Verwendung der notwendigen Sicherungsmittel zu ermöglichen. Dies ist bereits im Grundsatz durch das 3. Verwaltungsverfahrensänderungsgesetz 2003[47] ermöglicht und durch das E-Government-Gesetz 2013 bestärkt worden.[48]

---

43 S. z.B. Roßnagel, in: ders. (Hrsg.), Recht der Telemediendienste, 2013, § 371 a ZPO, Rn. 15 ff.
44 S. näher Jandt, NJW 2015, 1205.
45 S. z.B. Johannes, MMR 2013, 694.
46 S. z.B. Roßnagel/Nebel, NJW 2014, 886.
47 3. VwVfÄG vom 21.8.2002, BGBl. I, 3322; s. zu diesem Roßnagel, NJW 2003, 469.
48 S. Roßnagel, NJW 2013, 2710.

Die interne Verwaltungskommunikation innerhalb und zwischen Behörden muss ebenfalls vollständig elektronisch möglich sein, um einen durchgehenden Arbeitsprozess ohne Medienbruch in der Verwaltung und über die Institutionen hinweg zu ermöglichen. Die schnelle elektronische Bearbeitung von Verwaltungsaufgaben setzt eine elektronische Aktenführung und eine elektronische Vorgangsbearbeitung vom ersetzenden Scannen von Eingangspost bis hin zur elektronischen Archivierung der Akten voraus. Der Staat ist seiner Verantwortung bereits insoweit gerecht geworden, als er die Verwaltungsbehörden 2013 durch das E-Government-Gesetz zur rechtssicheren verwaltungsinternen elektronischen Vorgangsbearbeitung verpflichtet hat. Seiner Verantwortung für die finanzielle, personelle und technische Umsetzung dieser Verpflichtung muss er in den nächsten Jahren nachkommen.

### *5. Sicherheit in der Informationstechnik*

Die Schutzpflicht des Staats, sich schützend und fördernd vor die Grundrechte zu stellen,[49] begründet in der digitalen Zeit vor allem eine Verantwortung für sichere Informations- und Kommunikationstechnik. Dies bedeutet nicht, dass staatliche Stellen alle Sicherheitsaufgaben selbst erfüllen müssen. Doch besteht eine staatliche Verantwortung, für geeignete Rahmenbedingungen zu sorgen, dass sich alle auf sichere Informations- und Kommunikationstechnik verlassen können.

Sicherheit in der Informations- und Kommunikationstechnik soll sich vor allem über den Markt herstellen. Die Verantwortung des Staats ist daher in erster Linie eine Marktverantwortung. Er muss den Markt beobachten und bei Marktversagen die Bedingungen des Markts so verändern, dass die erforderlichen Sicherheitsziele durch Marktangebote erreicht werden. Dies erfordert punktuelle Korrekturen und zusätzliche Anreize. Faktisch kann derzeit Software – auch Sicherheitssoftware – durch die verwendeten Vertragsklauseln ohne Haftungsrisiken angeboten werden. Um die Vertrauenswürdigkeit von Sicherheitssoftware zu steigern sollten berechtigte Sicherheitserwartungen festgelegt und eine Haftung beim Verfehlen dieser Erwartungen sichergestellt werden. Für besonders riskante oder sicherheitsrelevante Systeme sollten Sicherheitsanforderungen an die

49 S. z.B. BVerfGE 38, 1; 49, 89; 57, 295; 73, 118; 90, 60; 114, 371; 119, 181.

Hersteller definiert werden, die diese zu einer Berücksichtigung des Grundsatzes „Security by Design“ zwingt. Da der Bürger, aber auch kleine und mittelständige Unternehmen bei der Beurteilung von Informations- und Kommunikationstechniksicherheit überfordert sind, ist es notwendig staatliche Technikexpertise dem Markt als neutrale Informationsquelle zur Verfügung zu stellen. Die Befugnis für das Bundesamt für die Sicherheit in der Informationstechnik in § 7 BISG, Hard- und Softwaresysteme ohne Anlass auf ihre Sicherheit untersuchen zu dürfen, ist hierfür ein erster Schritt in die richtige Richtung.[50] Die Zertifizierung von Produkten und die Auditierung von Informationstechnik-Angeboten wären notwendige weitere Schritte. Diesen müsste eine ausdrückliche Berücksichtigung der Sicherheit von Informations- und Kommunikationstechnik und der Bezugnahme auf Zertifikate und Audits in Vergabeverfahren folgen.

Die Marktverantwortung muss durch eine Infrastrukturverantwortung ergänzt werden. Für die Verwirklichung vieler Grundrechte ist ein ausreichender Schutz kritischer Infrastrukturen notwendig.[51] Dieser Verantwortung ist die Bundesrepublik Deutschland in einem ersten Schritt durch das Informationstechniksicherheitsgesetz (IT-SiG) vom 17.7.2015 gerecht geworden.[52] In diesem werden Einrichtungen in den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen erfasst. Sie werden dann als kritische Infrastrukturen definiert, wenn sie von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. In diesem Fall werden den Betreibern dieser Infrastrukturen besondere Sicherungspflichten hinsichtlich der eingesetzten Informationstechnik auferlegt.[53]

Die staatliche Infrastrukturverantwortung drückt sich aber noch in einer weiteren Aufgabe aus, nämlich in der Gewährleistung ausreichender Sicherheitsinfrastrukturen und ihrer Nutzungsmöglichkeiten. Sicherheits-

50 S. Roßnagel, DVBl. 2015, 1211.

51 S. hierzu bereits die Anmerkungen zum ersten BSIG 1990 in Roßnagel/Bizer/Hammer/Pordesch, DuD 1990, 178 ff. und Roßnagel/Bizer, KritJ 1990, 436 ff.

52 IT-Sicherheitsgesetz, BGBl. I, 1324; s. zu diesem z.B. Roßnagel, DVBl. 2015, 1206; Gitter/Meißner/Spauschus, ZD 2015, 512; Hornung, NJW 2015, 3334; Roos, MMR 2015, 636.

53 S. hierzu näher Roßnagel, DVBl. 2015, 1208 f.; Hornung, NJW 2015, 3336.

techniken wie Verschlüsselung oder elektronische Zertifikate, die die Grundlage für die Nutzung von Sicherungsmaßnahmen wie elektronische Signaturen, elektronische Siegel, elektronische Zeitstempel, elektronische Bestätigungen, Vertraulichkeitsschutz oder das Management elektronischer Identitätsnachweise sind, setzen Vertrauensdienste und Vertrauensdiensteanbieter voraus. Deren Angebote müssen insgesamt eine funktionierende und verlässliche Vertrauensinfrastruktur bilden.[54] Rahmenregelungen für diese Vertrauensinfrastruktur bestehen durch die Verordnung über elektronische Identifizierung und Vertrauensdienste (eIDAS-VO) und das Signaturrecht.[55] Es sollte durch die Infrastruktur und die notwendigen Infrastrukturregelungen für eine „Volksverschlüsselung" ergänzt werden.[56]

Schließlich besteht hinsichtlich der Sicherheit der Informations- und Kommunikationstechnik eine Informationsverantwortung des Staates. Über Sicherheitsrisiken und Schutzmöglichkeiten besteht eine hohe Unkenntnis. Der Schutz der Grundrechte, die in der digitalen Zeit auf die Sicherheit von Informations- und Kommunikationstechnik angewiesen sind, erfordert daher, die Grundrechtsträger über Risiken und Schutzmöglichkeiten zu informieren, damit sie ihre Grundrechte selbst schützen oder schützen lassen können. Teil der staatlichen Sicherheitsverantwortung ist deshalb, Sicherheitsinformationen zu verbreiten, die Angriffsrisiken darzustellen, Produktbewertungen zur Verfügung zu stellen, Programme zur Risikoerkennung zu empfehlen und Sicherungsmöglichkeiten zu beschreiben. In diesem Zusammenhang ist es hilfreich, dass das Informationstechniksicherheitsgesetz in § 8 b BSIG und weiteren ähnlichen Vorschriften ein Informationssystem aufbaut, in dem die Betreiber von kritischen Infrastrukturen sicherheitsrelevante Vorfälle an das Bundesamt für Sicherheit in der Informationstechnik melden müssen und dieses Amt aus den verschiedenen Meldungen einen Lagebericht erstellt und diesen sowie Sicherheitsempfehlungen an die Betreiber zurückmeldet.[57]

Zu kritisieren ist allerdings, dass die Information von Nutzern der kritischen Infrastrukturen sehr restriktiv geregelt ist. Ebenso ist die Bekanntmachung von erkannten Schwachstellen in Informationstechnikprodukten

---

54 S. hierzu Roßnagel, in: ders. (Hrsg.), Recht der Telemediendienste, München 2013, Einl. ins SigG, Rn. 18 ff.

55 S. hierzu näher Roßnagel, NJW 2014, 3686; ders., MMR 2015, 359.

56 S. www.volksverschluesselung.de.

57 S. näher Hornung, NJW 2015, 3336 f.; Roßnagel, DVBl. 2015, 1209 f.

gegenüber der Öffentlichkeit zu zurückhaltend geregelt. Notwendig ist ein Ausgleich zwischen den Sicherheitsinteressen der Bürger und Unternehmen, die auf Sicherheitsinformationen angewiesen sind, und gegenläufigen Sicherheitsinteressen sowie den Individualinteressen der Betreiber kritischer Infrastrukturen und den Herstellern informationstechnischer Produkte. Dabei muss aufgrund der grundrechtliche Schutzpflicht des Staats die bisherige Grundregel umgedreht werden: Das Bundesamts für Sicherheit in der Informationstechnik sollte auf berechtigte Anfragen hin Auskünfte erteilen oder von sich aus wichtige Erkenntnisse mitteilen und diese im Einzelfall nur aufgrund einer Abwägung der widerstreitenden Interessen verweigern können. [58]

### *6. Schutz der Grundrechte*

Die Schutzpflicht des Staates für gefährdete Grundrechte[59] wird in der digitalen Zeit für viele Grundrechte akut, weil die Digitalisierung ihre Verwirklichungsbedingungen zum Teil radikal verändert und sie neuen Gefährdungen aussetzt. Dies soll im Folgenden aus Platzgründen nur für drei Grundrechte näher ausgeführt werden, indem für diese zusätzliche Gefährdungen und Schutzaufgaben des Staats beschrieben werden.

Das Grundrecht auf informationelle Selbstbestimmung, das das Bundesverfassungsgericht aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG ableitet,[60] wird durch viele Entwicklungen verletzt oder gefährdet. Die größte Herausforderung besteht derzeit wohl in der Ausspähung aller elektronischen Kommunikationsvorgänge durch fremde und eigene Geheimdienste. Insbesondere die US-Geheimdienste streben an, alle Datenspuren im Internet zu erfassen, um sie bei Bedarf kontrollieren und auswerten zu können.[61] Diese Ausspähung durch Geheimdienste wird ermöglicht, weil die großen Internetdiensteanbieter mit ihnen zusammenarbeiten (müssen).[62] Aufgrund ihrer Geschäftsmodelle versuchen diese, möglichst viele Daten über

58 S. Roßnagel, DVBl. 2015, 1210 f.
59 S. Fn. 49.
60 S. z.B. BVerfGE 65, 1 (41 ff.); 67, 100 (142); 103, 23 (33); 113, 29 (46); zur Entwicklung s. z.B. Geminn/Roßnagel, JZ 2015, 703.
61 S. z.B. Greenwald, Die globale Überwachung, 2014.
62 S. hierzu näher EuGH vom 6.10.2015, C-362/14 (Facebook), Rn. 11 ff.; Roßnagel/Jandt/Richter, DuD 2014, 545.

ihre Nutzer zu protokollieren, durch den Zugriff auf Dateien der Nutzer zu erheben und durch Analysetools aus ihrem Verhalten im Internet abzuleiten.[63] Das Problem dieser Grundrechtsverletzungen wird dadurch verschärft, dass viele mögliche Schutzmaßnahmen gegen das Ausspähen von Verkehrs- und Inhaltsdaten zunehmend unwirksam werden. Die riesengroßen Datenmengen, die durch die Digitalisierung vieler Lebensbereiche entstehen (Ubiquitous Computing), und die neuen Analysemöglichkeiten dieser heterogenen Datenmassen durch Big Data-Techniken ermöglichen immer besser die Deanonymisierung von personenbezogenen Daten. Die Schutzpflicht des Staats begründet dessen Verantwortung auch gegenüber Angriffen auf Grundrechte durch fremde Staaten. Dieser muss er dadurch gerecht werden, dass er seinen Bürgern technische Schutzmöglichkeiten bietet, die die Auswertung von Daten durch ausländische Geheimdienste erschweren. Gegenüber der Ausspähung durch Internetanbieter muss er Schutz vor unfairen Allgemeinen Geschäftsbedingungen bieten. Auf die zunehmende Unwirksamkeit von Anonymisierungsmaßnahmen muss er durch Vorsorgeregelungen für den Umgang mit anonymen Daten reagieren.

Das Grundrecht auf Gewährleistung der Vertraulichkeit und der Integrität eigener Techniksysteme (IT-Grundrecht), das das Bundesverfassungsgericht ebenfalls aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG ableitet,[64] wird in der digitalen Zeit vor allem dadurch gefährdet, dass Hersteller von Geräten und Anbieter von Diensten immer stärker auf die Nutzungsmöglichkeiten des eigenen Endgeräts Einfluss nehmen. Dies ist zum Teil Voraussetzung oder Folge neuer Geschäftsmodelle wie „Product as a Service", zum Teil entspringt dies einem Wunsch oder Bedarf, den Nutzer zu kontrollieren, oder ist vielfach auch das Ziel „bösartiger" Apps, die irgendeine Leistung anbieten, deren Hauptzweck aber in der unbemerkten Übertragung von Dateien des Nutzers an den App-Anbieter besteht. In all diesen Fällen ist das Ergebnis, dass der Nutzer des Geräts nicht dessen Herr ist und dieses Handlungen ausführt, die der Nutzer nicht erfährt und nicht beeinflussen kann. Da dies im Regelfall eine Verletzung des IT-Grundrechts ist, besteht eine staatliche Verantwortung, dem Nutzer eine Selbsthilfe dadurch zu ermöglichen, dass er Software auf seinem Gerät, die etwas ande-

63 S. hierzu näher Roßnagel, Regulierung – was leistet unser Datenschutzrecht (nicht)? in: Hill (Hrsg.), E-Transformation. Veränderung der Verwaltung durch digitale Medien, 2014, 78 ff.

64 BVerfGE 120, 274 (306 ff.).

res tut, als er möchte, durch entsprechende Entdeckungs- und Schutzsoftware modifizieren darf. Da dies urheberrechtlich umstritten ist, wäre eine entsprechende Klarstellung des Gesetzgebers dringend geboten.[65]

Die schwierigste Aufgabe aus heutiger Sicht ist die Gewährleistung der Entscheidungs- und Verhaltensfreiheit in der digitalen Zeit. Diese wird künftig vor allem durch statistische Auswertungen im Rahmen von Big Data-Analysen gefährdet. Soweit diese personenbezogenen Daten auswerten oder auf personenbezogene Profile zielen, ist dies ein Problem der informationelle Selbstbestimmung und des Datenschutzes. Dies dürfe in beiden Fällen nicht mit geltendem Datenschutzrecht vereinbar sein.[66] Aber auch, wenn personenbezogene Daten weder der Ausgangspunkt noch das Ziel von Big Data-Analysen sind, gefährden diese die Entscheidungs- und Verhaltensfreiheit. In dieser Hinsicht sind zwei zu unterscheidende Problembereiche erkennbar.[67]

Das erste Problem besteht darin, dass hinsichtlich der statistischen Vorhersage von Emotionen und Verhalten die Gefahr besteht, dass der Einzelne trotz sorgfältiger und bedachter Entscheidung, welche Daten er über sich preisgeben will, die Kontrolle darüber verliert, über welche Daten und welches Wissen jemand verfügt. Dass diese Daten nur Prognosen sind und zudem falsch sein können, bleibt häufig außer Acht, wenn diesen Prognosen echte Entscheidungen folgen. Damit kollektiviert Big Data das Risiko für die Selbstbestimmung und Entscheidungsfreiheit.[68] Durch Big Data findet eine anonyme Vergemeinschaftung[69] statt: Statistik gilt für alle. Wer seine Daten für Big Data-Auswertungen bereitstellt, erzeugt nicht nur Risiken für sich selbst, sondern immer auch Risiken für andere, die sich in einer vergleichbaren Situation befinden. Die aus den Daten der Einwilligenden erzeugten Auswertungen gelten auch für diejenigen, die ihre Daten verweigert haben. Auf diese Weise untergräbt Big Data datenschutzbewusstes Verhalten. Wenn Daten anderer vergleichbarer Personen ausgewertet werden können, wenn sie diese preisgegeben haben, wird die

65 S. zu dieser Gefährdung und möglichen Schutzmaßnahmen Bodden/Rasthofer/Richter/Roßnagel, DuD 2013, 720.

66 S. z.B. näher Roßnagel, ZD 2013, 566; Ohrtmann/Schwiering, NJW 2014, 2984; Weichert, ZD 2013, 251; Richter, (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data, 2015.

67 S. hierzu Roßnagel/Nebel, DuD 2015, 455.

68 S. auch Weichert, ZD 2013, 254; Roßnagel, ZD 2013, 566.

69 S. Hubig, in: Roßnagel/Sommerlatte/Winand (Hrsg.), Digitale Visionen – Zur Gestaltung allgegenwärtiger Informationstechnologien, 2008, 165 ff.

Möglichkeit untergraben, über den eigenen Datenstrom durch bewusste Auswahl von publizierten Daten selbst zu bestimmen. Big Data umgeht die individuelle Datenaskese, indem aus den Daten ähnlicher Personen auf durchschnittliche oder individuelle Verhaltensweisen geschlossen wird. Selbst wenn ein Betroffener keine Daten zur Verfügung stellt, kann über Durchschnittswerte sein künftiges Verhalten prognostiziert werden.

Das zweite Problem besteht darin, dass die durch Big Data-Analysen erzeugten statistischen Muster Grundlagen von Entscheidungen und Maßnahmen sind und dadurch normbildend und verhaltensbestimmend wirken. Wer positive Wirkungen erreichen und negative vermeiden will, passt sein Verhalten diesen Mustern an. Big Data-Analysen können durch diese Normbildung indirekt, aber wirkungsvoll die Wahrnehmung von Grundrechten beeinflussen. Die anonymen Big Data-Muster wirken auf diese Weise genauso negativ auf die Persönlichkeitsentfaltung des Einzelnen und die freie Kommunikation und Willensbildung in der Gesellschaft insgesamt ein, wie dies das Bundesverfassungsgericht bereits im Volkszählungsurteil als Auswirkungen personenbezogener Überwachung festgestellt hat.[70] Durch die Fähigkeit von Big Data-Analysen, ständig neue korrelierende Muster zu finden und damit auch auf den ersten Blick völlig zusammenhanglos erscheinende Verhaltensmerkmale als positiv oder negativ erscheinen zu lassen, kommt hinzu, dass niemand mehr einschätzen kann, welche Verhaltensweisen die gewünschten Wirkungen erzielen. Dadurch entstehen ein diffuses Gefühl nicht-normkonformen Verhaltens und das Bestreben, durch normkonformes Verhalten nicht aufzufallen.[71] Solche statistischen Muster verstärken die Normativität der Normalität und reduzieren „Soziodiversität“. Diese ist jedoch für die Gesellschaft ebenso wichtig wie Biodiversität für die Natur. Sie ist die Voraussetzung für Innovationen und Demokratie.[72]

Für eine freie, demokratische Gesellschaft, die auf die selbstbestimmte und ungezwungene Mitwirkung ihrer Bürger angewiesen ist, ist eine solche Einschränkung der Grundrechte nicht akzeptabel. Es obliegt daher der staatlichen Schutzpflicht, die ungehinderte Ausübung der Grundrechte zu gewährleisten. Ansätze, um der staatliche Verantwortung gerecht werden zu können, könnten darin liegen, bestimmte Datenkategorien mit mögli-

70 BVerfGE 65, 1 (43).
71 S. Weichert, ZD 2013, 258; s. das Beispiel in Roßnagel, ZD 2013, 566.
72 Helbing, Neue Zürcher Zeitung, 20.3.2013, 31, mit Verweis auf das Konzept der „Weisheit der Vielen“.

cher diskriminierender Wirkung auszuschließen, Anforderungen an die Wissenschaftlichkeit von Big Data-Analysen und an die Erheblichkeit der Ausgangsdaten für die zulässige Zielsetzung der Analysen zu stellen[73] und Einwilligungen, die negative Konsequenzen für Dritte haben können, zu beschränken. Um Beeinträchtigungen der Entscheidungs- und Verhaltensfreiheit zu verhindern und um demokratisches Engagement zu sichern, sind grundsätzlichere Lösungsansätze zu bedenken. Der Schutz der Persönlichkeit soll gewährleisten, dass dem Einzelnen – „auch unter den Bedingungen moderner Informationsverarbeitungstechnologien" – die „Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten".[74] Um dieses Ziel zu erreichen, bedarf ihre „lückenschließenden Funktion"[75] einer weiteren, über die informationelle Selbstbestimmung hinausgehenden Konkretisierung. Da es „mit der Menschenwürde … nicht zu vereinbaren (ist), … den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch *in der Anonymität einer statistischen Erhebung*, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist",[76] muss diese darauf zielen, Big Data-Analysen auf verfassungsverträgliche Zwecke zu begrenzen.[77]

## *III. Fazit*

Die Untersuchung zur Reichweite der staatlichen Verantwortung für Teilhabe in der digitalen Zeit ergab viele Handlungsfelder, in denen eine staatliche Verantwortung festgestellt werden konnte. Diese ergibt sich vor allem aus der Schutzpflicht des Staats für die Grundrechte seiner Bürger. Werden diese neuen Gefährdungen ausgesetzt, mobilisiert dies die Verantwortung staatlicher Stelle, sich schützend und fördernd vor diese Grundrechte zu stellen. Wie die staatlichen Stellen ihrer Schutzaufgabe gerecht werden, können diese bis zu einem Mindestmaß an notwendigem Schutz im Rahmen eines weiten Entscheidungsspielraums bestimmen. Wenn sie

73 S. hierzu § 28 b Nr. 1 BDSG für Scoring.
74 BVerfGE 65, 1 (42 f.).
75 BVerfGE 120, 274 (313).
76 BVerfGE 27, 1 (6) – Hervorhebung durch Verfasser.
77 S. Roßnagel/Nebel, DuD 2015, 459.

aber Schutzmaßnahmen ergreifen, hat der einzelne Bürger einen grundrechtlichen Anspruch, an diesen teilhaben zu können. Es gibt aber noch einen zweiten Begründungsstrang für die staatliche Verantwortung für Teilhabe in der digitalen Zeit. Grundrechtliche Abwehrrechte wollen reale Freiheit gewährleisten. Für die Wahrnehmung dieser intendierten Freiheit sind die jeweiligen Verwirklichungsbedingungen des Grundrechts entscheidend. Diese können sich durch die Digitalisierung nahezu aller Lebensbereiche radikal verändern. Um auch unter den neuen Verwirklichungsbedingungen Freiheit zu gewährleisten, kann den Staat die Verantwortung treffen, neue Rahmenbedingungen herzustellen, die Freiheit auch unter den veränderten Verwirklichungsbedingungen gewährleisten.

Eine Verantwortungserfüllung konnte in der Untersuchung für die Handlungsfelder „Instrumente des elektronischen Rechtsverkehrs“ und „elektronische Verwaltung“ festgestellt werden. In beiden Handlungsfeldern ist der Staat seine Verantwortung weitgehend gerecht geworden. Im Handlungsfeld des elektronischen Rechtsverkehrs hat er geeignete Regelungen erlassen, die einen vertrauenswürdigen Rahmen bilden, um Vertrauensdienste in ausreichender Qualität am Markt anzubieten und das Entstehen einer verlässlichen Vertrauensinfrastruktur zu fördern. Im Handlungsfeld elektronische Verwaltung hat er einen Rechtsrahmen zur Verfügung gestellt, innerhalb dessen Möglichkeiten und Verpflichtungen bestehen, eine elektronische Verwaltung aufzubauen, die alle Verwaltungsfunktionen in der digitalen Zeit erfüllen kann.

Noch verbleibende Verantwortungsaufgaben konnte in der Untersuchung zumindest für die Handlungsfelder „Infrastrukturen“, „Informationen“, „Informationstechniksicherheit“ und „Schutz von Grundrechten“ festgestellt werden. In diesen Handlungsfeldern bestehen noch herausfordernde Aufgaben, denen sich staatliche Stellen in der kommenden Zeit intensiv widmen müssen.

Unabhängig von einzelnen Handlungsaufgaben bedarf es einer organisatorischen Absicherung in der Wahrnehmung staatlicher Verantwortung. Zur Erfüllung seiner Aufgaben bedarf der Staat geeigneter Institutionen und Verfahren. Gerade in der digitalen Zeit ist die Fähigkeit entscheidend, immer wieder neue Herausforderungen zu erkennen und ihnen geeignet zu begegnen. Daher muss organisatorisch vor allem die Beobachtungs- und Nachbesserungspflicht des Gesetzgebers und anderer staatlicher Stellen – entsprechend ihrer Funktion im staatlichen Informations- und Handlungsgefüge – gesichert werden.

# Ist der digitale Staat ein besserer Staat?

*Utz Schliesky*

## *I. Einführung: Digitaler Staat*

Ein besserer Staat setzt einen guten Staat voraus - ist das Bessere doch bekanntlich der Feind des Guten. Die Verbindung des Staates mit einer ethischen Kategorie scheint allerdings ein wenig aus der Mode gekommen zu sein, wenn es doch dem Staatsdenken auch nicht fremd ist. Im 19. Jahrhundert war diese Verbindung eher Allgemeingut - man denke nur an *Hegel*: »Der Staat ist die Wirklichkeit der sittlichen Idee (…)«.[1] Letztlich beschäftigt sich die Staatslehre schon seit gut 2000 Jahren mit der Frage nach dem guten oder besseren Staat; die Literaturgattung der sog. Fürstenspiegel liefert seit jeher den Herrschern Handlungsanleitungen für eine gute Herrschaft und vereint insoweit verfassungsrechtliche, staatsphilosophische und ethische Grundnormen. Seit dem Konstitutionalismus sind die Fürstenspiegel den Verfassungen gewichen, die nun die rechtliche und - zumindest in sehr allgemeinen Grundzügen auch - ethische Grundordnung des Staates bilden. Dementsprechend will ich den digitalen Staat nachfolgend an derartigen Grundaussagen messen. Einige wesentliche Grundaussagen unserer Verfassung sollen daraufhin überprüft werden, ob sie in der digitalen Welt Bestand haben können (II) oder wie sie weiterzuentwickeln sind, damit ein besserer Staat entsteht (III).

---

1 *Hegel*, Grundlinien der Philosophie des Rechts oder Naturrecht und Staatswissenschaft im Grundrisse, 1820, hrsgg. von *Lakebrink*, 2002, § 257. *Hegel*, aaO. § 142, definiert die Sittlichkeit wie folgt: »Die Sittlichkeit ist die *Idee der Freiheit*, als das lebendige Gute, das in dem Selbstbewusstsein, sein Wissen, Wollen und durch dessen Handeln seine Wirklichkeit sowie dieses an dem sittlichen Sein seine an und für sich seiende Grundlage und bewegenden Zweck hat - der *zur vorhandenen Welt und zur Natur des Selbstbewusstseins gewordene Begriff der Freiheit.*« - Rezipiert etwa durch *Friedrich Julius Stahl*, Die Philosophie des Rechts, Zweiter Band - Zweite Abteilung, 5. Aufl. 1878/6. Aufl. 1963, § 36 (S. 130): »Der Staat ist daher nach Art und Form seines Bestandes d e r V e r b a n d e i n e s V o l k e s u n t e r e i n e r H e r r s c h a f t ( O b r i g k e i t ) . Nach Gehalt und Bedeutung ist er e i n s i t t l i c h e s R e i c h . Er ist schlechthin d i e s i t t l i c h e W e l t (…).«

Dabei ist der Begriff des »digitalen Staates« leicht irreführend: Er beschreibt nicht ein anderes, völlig neuartiges Staatsgebilde in der virtuellen Welt, sondern die prozesshafte Entwicklung der Digitalisierung staatlicher Verfahren und Strukturen. Die Informations- und Kommunikationstechnik erobert nicht nur alle gesellschaftlichen Lebensbereiche, sondern eben längst auch alle Staatsgewalten. Während die Gesellschaft in einem hohen Innovationstempo über das Internet der Dinge, selbstfahrende Autos oder die Nutzung von Big-Data[2], z.B. in Gestalt der stetigen Übermittlung von Gesundheitsdaten an Krankenkassen als Grundlage der Beitragsbemessung, diskutiert, beschäftigt sich der Staat mit elektronischem Regieren und Verwalten (E-Government), der Koordinierung staatlicher Infrastrukturen via Internet, der Entwicklung von Möglichkeiten digitaler Demokratie, der Cyber-Sicherheit (z.B. zur Abwehr von Hacker-Angriffen auf die Homepage der Bundeskanzlerin), mit der Digitalisierung parlamentarischer Abläufe, Strategien für eine virtuelle Kriegsführung oder dem elektronischen Rechtsverkehr. Allen Beispielen gemeinsam ist, dass sie aufgrund der technikgestützten Enträumlichung und Entgrenzung[3] und den zwangsläufig global vernetzten Ablaufstrukturen zu bisherigen Denk- und Regulierungsmodellen nicht (mehr) passen und daher einer (neuen) rechtlichen Regulierung bedürfen, wenn der staatliche Steuerungs- und Gestaltungsanspruch nicht aufgegeben werden soll. Langsam, aber sicher setzt sich daher die Auffassung durch, dass E-Government und digitale Strukturen insgesamt einer rechtlichen Normierung bedürfen[4].

2 Zu den datenschutzrechtlichen Fragen des Big Data *Ohrtmann/Schwiering,* Big Data und Datenschutz – Rechtliche Herausforderungen und Lösungsansätze, NJW 2014, 2984 ff.; s. auch *Hofstetter*, Verkannte Revolution: Big Data und die Macht des Marktes, APuZ 11-12/2015, S. 33 ff.

3 Dazu bereits *Schliesky*, in: Hill/Schliesky (Hrsg.), Die Vermessung des virtuellen Raums, E-Volution des Rechts- und Verwaltungssystems III, 2012, S. 14 ff.

4 Dazu bereits *Schliesky*, Regelungsbedarf für elektronische Verwaltungsstrukturen, in: Henneke (Hrsg.), Kommunale Verwaltungsstrukturen der Zukunft, 2006, 50 ff.; *ders.*, ZRP 2015, 56 ff.; zu Teilaspekten auch *Fischer-Lescano*, *JZ* 2014, 965 ff.; *Hoffmann-Riem,* JZ 2014, 53 ff.

## *II. Maßstäbe für einen guten Staat - Kernaussagen des Grundgesetzes*

### *1. Menschenwürde und Persönlichkeitsrecht*

Den archimedischen Punkt aller grundgesetzlichen Maßstabsnormen bildet die Menschenwürde, die in Art. 1 Abs. 1 GG an die Spitze der Verfassung gestellt ist und als Basis des Verfassungssystems das normative Fundament der Bundesrepublik Deutschland und das Wesen seiner Staatlichkeit beschreibt[5]. Aus dem Zusammenspiel der Menschenwürdegarantie in Art. 2 Abs. 1 GG hat das Bundesverfassungsgericht im Wege richterlicher Rechtsfortbildung das allgemeine Persönlichkeitsrecht kreiert, das seine Grundlage in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG findet[6]. Das allgemeine Persönlichkeitsrecht schützt zum einen die Möglichkeit autonomer Selbstentfaltung durch Abschirmung eines privaten Bereichs, zum anderen aber auch die nach außen gerichtete Selbstdarstellung der Person in der Öffentlichkeit; darüber hinaus schützt es als dritte große Kategorie die vorgelagerten Grundbedingungen für die freie Entfaltung der Persönlichkeit[7]. Die besondere Würdeerheblichkeit der individuellen Persönlichkeitsentfaltung auf Grundlage der geschützten, enger umgrenzten Voraussetzungen personaler Identität wird durch den Bezug auf die Menschenwürdegarantie in Art. 1 Abs. 1 GG besonders betont und in einem herausgehobenen Sinne, eben im Sinne eines allgemeinen Persönlichkeitsrechts, geschützt.

In der digitalen Welt sind das allgemeine Persönlichkeitsrecht und ab und an sogar die Menschenwürdegarantie in großer Verletzungsgefahr. Allerdings drohen die meisten Gefahren von privater Seite, so dass in der digitalen Welt zahlreiche neue Drittwirkungsproblematiken für diese zentrale Grundrechtsgarantie entstehen. Die Beispiele reichen vom sog. Cyber-Mobbing in sozialen Netzwerken bis zur Zurschaustellung von erniedrigenden Folterpraktiken durch Terroristen. Viele dieser neuen Herausforderungen lösen staatliche Schutzpflichten aus, die zu - auch gesetzgeberischen - Handlungsaufträgen führen. Der technische Fortschritt zwingt je-

---

5 BVerfGE 5, 85 (204); 30, 173 (193); 50, 166 (175); 87, 209 (228); *Heun,* Die Verfassungsordnung der Bundesrepublik Deutschland, 2012, S. 235.

6 St Rspr., etwa BVerfGE 35, 202 (219); 72, 155 (170); 82, 236 (296); 90, 263 (270); s. ferner BVerfGE 65, 1 (41 ff.); 120, 274 (303 ff.), im IT-Kontext.

7 Statt vieler *Dreier*, in: ders. (Hrsg.) Grundgesetz-Kommentar, Bd. I, 3. Aufl. 2013, Art. 2 I Rn. 69 ff., 78; *Kube,* in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. VII, 3. Aufl. 2009, § 148 Rn. 36 ff.; *Schliesky*, Ein Recht auf Heimat?, 2014, S. 21.

denfalls dazu, auch sehr grundlegende Kategorien wie etwa das Menschsein als Anknüpfungspunkt von Menschenwürde, Persönlichkeitsrecht und anderen Grundrechten zu hinterfragen: Zunehmend werden Menschen elektronische, von Computern gesteuerte Bauteile implantiert, so dass Krankheiten wie Epilepsie, Parkinson etc. gelindert werden können oder etwa Blinde wieder sehen können[8]. Der Einfluss dieser digitalen Hilfsmittel auf die Persönlichkeit und Hirnleistung der Betroffenen ist nachgewiesen, und weder Fremdsteuerung noch erhebliche selbst veranlasste Leistungssteigerungen sind medizinisch-technisch ausgeschlossen.[9]

Das Recht auf »Vergessenwerden« in Suchmaschinen hat der EuGH vor Kurzem konturiert[10] - dennoch bleiben Fragen offen, weil zum einen das kulturelle Erbe, zumindest die Archivierung von Medienerzeugnissen etc. nicht mehr vollständig überliefert werden kann und zum anderen auch Grundrechte von Medienunternehmen und Suchmaschinenbetreibern in Rede stehen. Hier besteht eine bi-, tri- oder multipolare Interessenkollision, die vom Gesetzgeber aufzulösen wäre. Eng damit verbunden sind Fragen der Sicherung des digitalen Nachlasses[11].

Ein zentrales Thema der Zukunft wird die Frage sein, wie Daten als Handelsware rechtlich zu behandeln sind[12]. Bei zahlreichen Geschäftsmodellen von Anbietern sozialer Netzwerke etc. werden Leistungen im Austausch gegen persönliche Nutzerdaten zur Verfügung gestellt. Nach deutschem Recht ist die persönliche »Datensouveränität« Ausfluss des allgemeinen Persönlichkeitsrechts in Gestalt des Rechts auf informationelle Selbstbestimmung[13]. Auch das ebenfalls auf das allgemeine Persönlichkeitsrecht gestützte Grundrecht auf Vertraulichkeit und Integrität informa-

8 Weltweit sind bereits 120.000 sog. Hirnschrittmacher implantiert worden, in Deutschland sind es 400 - 500 Fälle jährlich. Näher dazu Wirtschaftswoche Nr. 7 vom 09.02.2015, S. 62 ff.

9 *Meckel*, APuZ 7/2012, 33 ff.

10 EuGH, Urt. v. 13.05.2014 – C-131/12; dazu u. a. *Kühling*, EuZW 2014, 527 ff.; *Sofiotis*, Das Recht auf Vergessen im Spannungsfeld von Datenschutz und Informationsfreiheit, VR 2015, 84 ff.; *Spindler*, JZ 2014, 981 ff.;

11 Dazu eingehend *Martini*, »Wenn ich einmal soll scheiden«: Der digitale Nachlass und seine unbewältigte rechtliche Abwicklung, in: Hill/Martini/Wagner (Hrsg.), Facebook, Google & Co. Chancen und Risiken, 2013, S. 77 ff.; *Brisch/Müller-ter Jung*, CR 2013, 446 ff.

12 Dazu *Reiners,* ZD 2015, 51 ff.

13 BVerfGE 65, 1 ff.

tionstechnischer Systeme[14] kann hier eine Rolle spielen. Die rein wirtschaftliche Nutzung persönlicher Daten kollidiert jedenfalls mit diesem Grundkonstrukt des deutschen Datenschutzes und dementsprechend auch mit seinen einfachgesetzlichen Ausprägungen im Datenschutzrecht.

### *2. Grundrechte*

Längst sind auch die anderen Grundrechte im digitalen Zeitalter angekommen. Welch ein großer Bedarf an Weiterentwicklung hier besteht, zeigt allein die richterliche Rechtsfortbildung des Bundesverfassungsgerichts mit dem Recht auf informationelle Selbstbestimmung und nun besonders mit dem Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. An dieser Rechtsfortbildung durch das Bundesverfassungsgericht zeigt sich auch, dass nicht für jede neue Herausforderung gleich eine Verfassungsänderung erforderlich ist. Die digitale Dimension der Grundrechte kann vielmehr in der Regel durch zeitgemäße Auslegung herausgearbeitet werden, da grundrechtliche Normgehalte in Abhängigkeit von konkreten Grundrechtsgefährdungen entwicklungsfähig und wandelbar sind[15]. Allerdings bedürfen auch die Rechtsfiguren der Schutzpflicht und der Drittwirkung von Grundrechten einer Weiterentwicklung, wenn typische grundrechtliche Gefährdungslagen in der digitalen Welt erfasst werden sollen[16].

Dennoch wäre es auch für das Grundgesetz wünschenswert, den Schutz der digitalen Privatsphäre ausdrücklich in die Verfassung aufzunehmen, wie es jüngst Art. 15 LVerf SH als erste deutsche Verfassung getan hat. Der Verfassunggeber würde so eine Vorgabe für Abwägungsentscheidungen des einfachen Gesetzgebers zwischen Persönlichkeitsrecht auf der einen Seite und Wirtschafts- und Unternehmerfreiheit auf der anderen Seite treffen. Denn neu ist in der virtuellen Welt, dass Informationen aus der Privatsphäre sozusagen zur Währung zahlreicher Geschäftsmodelle wer-

---

14 BVerfGE 120, 274 (303 ff).

15 *Hoffmann/Luch/Schulz/Borchers*, Die digitale Dimension der Grundrechte, 2015, S. 15 ff.; *Schliesky/Hoffmann/Luch/Schulz/Borchers*, Schutzpflichten und Drittwirkung im Internet - Das Grundgesetz im digitalen Zeitalter, 2014, S. 80 ff. insbes. S. 89 ff.; ferner *Luch/Schulz*, MMR 2013, 88 ff.; zu anderweitigem Änderungsbedarf am Grundgesetz *Schliesky*, in: Hill u.a. (Hrsg.), Brauchen wir eine neue Verfassung?, 2014, S. 215 ff.

16 *Schliesky/Hoffmann/Luch/Schulz/Borchers* (Fn. 15), S. 98 ff.

den. Eine Normierung der digitalen Privatsphäre würde die Schutzpflicht des einfachen Gesetzgebers verstärken.

Eine weitere Frage ist, inwieweit automatisierte Verhaltensweisen in die Grundrechtsdogmatik eingepasst werden können. Die Grundrechte des Grundgesetzes basieren auf dem Gedanken individueller Freiheit und setzen menschliche Verantwortungsbetätigung voraus. Die Informations- und Kommunikationstechnik ermöglicht es heutzutage aber bereits, dass beispielsweise ein Börsenhandel mit zum Teil erheblichen Auswirkungen auf die »Realwirtschaft« und möglicherweise sogar auf Staatshaushalte ausschließlich durch Computerprogramme erfolgt. Die Verfassung muss insoweit Antworten darauf geben, ob derartige Betätigungen (noch) den Schutzbereichen der Berufs- und Eigentumsfreiheit unterfallen können.

Noch einen Schritt weiter geht die Diskussion, inwieweit auch Avataren ein Grundrechtsschutz zukommen soll. Ein Staatsrechtler mag angesichts des individualrechtlichen Charakters der Grundrechte hier an einen schlechten Aprilscherz denken, doch zeigen einschlägige Internetforen, dass derartige Diskussionen längst geführt werden[17]. Da nach Art. 19 Abs. 3 GG der Grundrechtsschutz auch auf juristische Personen ausgedehnt wird, kann eine derartige Diskussion in Kürze auch mit staatsrechtlicher Ernsthaftigkeit drohen.

### *3. Staatliches Gewaltmonopol*

Klassischer Maßstab für einen guten Staat ist seit jeher das staatliche Gewaltmonopol, da Frieden und Sicherheit zu den vornehmsten Staatszwecken gehören. Der eigentliche Siegeszug des staatlichen Gewaltmonopols begann mit der Herausbildung des Territorialstaates und hat im Nationalstaat des 20. Jahrhunderts seine bis heute akzeptierte und ganz überwiegend gewollte Form gefunden. Das Gewaltmonopol beruht allerdings auf einer physischen Möglichkeit in einer räumlich definierten Zuständigkeit,

17 S. etwa http://forum.hypergrid.org/opensin-general/grundrechte-eines-avatars-t3615-10.html, zuletzt aufgerufen am 08.01.2015. Gefordert werden dort u.a. das Recht auf freie Wahl der Erscheinungsform, das Recht auf Bannlinien-Freiheit, das Recht auf fehlenden Gruppenzwang, die Pflicht zur angemessenen Reaktion auf IMs anderer und die Pflicht zur Hilfeleistung anderen gegenüber. Ausdrücklich gefordert wird jedenfalls eine Unterscheidung zwischen dem »User« und dem Avatar.

es setzt die souveränitätstheoretische Einzigkeit der Staatsgewalt voraus[18]. Das Internet, die Möglichkeiten der Informations- und Kommunikationstechnik und alle Prozesse der Digitalisierung sind aber wesensimmanent grenzüberschreitend, staatliche Akteure spielen in diesem weltweiten Netzwerk nur eine untergeordnete Rolle und sind - streng genommen - verzichtbar. Da auf der anderen Seite die kulturelle Errungenschaft des staatlichen Gewaltmonopols nach wohl ganz überwiegender Auffassung nicht leichtfertig aufgegeben werden sollte, stellt sich die große Herausforderung, das staatliche Gewaltmonopol wenigstens partiell auch in digitalen Kontexten durchzusetzen. Alle Staaten dieser Welt versuchen dies in unterschiedlichem Maße und mit unterschiedlichem Umfang. Die immer wieder suggerierte Gleichrangigkeit aller Akteure und damit die Möglichkeit des Verzichts auf das staatliche Gewaltmonopol ist eine Chimäre, da gerade auch im digitalen Netzwerk sehr wohl (oftmals auch illegitime) Macht ausgeübt wird und Verbrechen begangen werden.

## *4. Demokratie*

### a) Digitaler Strukturwandel der Öffentlichkeit

Das Parlament ist in der repräsentativen Demokratie der Ort zur Herstellung demokratischer Öffentlichkeit und zur Fokussierung der öffentlichen Meinung[19]. Die öffentliche Meinung im normativen Sinn ist dabei das Ergebnis eines durchaus komplexen Meinungsbildungsprozesses nach Maßgabe bestimmter Qualitätskriterien, zu denen etwa die freie und gleiche Teilhabe und ein gleicher, möglichst hoher Informationsstand der Beteiligten gehören[20]. Nun ist die klassische Öffentlichkeitsfunktion des Parlaments[21] zu einer Zeit und unter gesellschaftlichen Umständen konzipiert und beschrieben worden, die sich in den vergangenen Jahrzehnten gravie-

---

18 Dazu näher *Schliesky,* Souveränität und Legitimität von Herrschaftsgewalt, 2004, S. 92.

19 Zur Begriffsgeschichte der »Öffentlichkeit« eingehend *Hölscher*, in: Geschichtliche Grundbegriffe Bd. 3, 1972, Art. Öffentlichkeit, S. 413 ff.; kritisch gegenüber dem deutschen Begriff der Öffentlichkeit *Bourdieu*, Über den Staat, 2014, S. 532.

20 *Schulze-Fielitz*, in: Evangelisches Staatslexikon, Art. Öffentlichkeit (2006), S. 1655 (1656).

21 Dazu eingehend *Schliesky*, Parlamentsfunktionen, in: Morlok/Schliesky/Wiefelspütz (Hrsg.), Handbuch des Parlamentsrechts, 2015, § 5 Rn. 35 ff.

rend verändert haben. Die Vorstellungsbilder der demokratischen öffentlichen Meinung sind letztlich noch immer mit der griechischen Agora oder dem römischen Forum verbunden, auch wenn die zunehmende gesellschaftliche Größe und Komplexität durch Staatsbildung, durch die Einführung eines repräsentativen Systems und erst recht ergänzt und ersetzt durch Massenmedien wie Bücher, Zeitungen, Flugschriften oder dann Hörfunk, Fernsehen schon lange einen Strukturwandel der Öffentlichkeit und der öffentlichen Meinung bewirkt haben[22] und sich eben – wie gleich noch zu zeigen ist – letztlich in einem permanenten Entwicklungs- und Veränderungsprozess befinden. Eine zum Teil durchaus neue Art des Strukturwandels mit gravierenden Auswirkungen auf die Öffentlichkeitsfunktion des Parlaments bewirken elektronische Medien bzw. das Internet und soziale Netzwerke. Zugleich verändert sich der relevante politische Raum durch Europäisierung und Globalisierung, so dass das Volk als Legitimationssubjekt der demokratischen Herrschaftsordnung nicht mehr mit der relevanten Öffentlichkeit oder öffentlichen Meinung deckungsgleich ist. Zugleich schwindet die bisher als zentraler demokratischer Faktor vorhandene und als erforderlich angesehene »bürgerliche Öffentlichkeit«[23]. So nimmt es nicht wunder, dass *Habermas* schon vor gut 50 Jahren den durch gezielte Beeinflussung der Öffentlichkeit (Öffentlichkeitsarbeit; PR-Kampagnen etc.) verursachten »Strukturwandel der Öffentlichkeit« beschrieben hat[24].

Längst findet ein weiterer Strukturwandel der Öffentlichkeit statt, der durch das Internet und die digitalen Medien in Gang gesetzt worden ist[25]. Gerade in sozialen Netzwerken entstehen neue segregierte »Club-Zirkel« als geschlossene Benutzergruppen, die in der Regel nur zur Bestätigung vorgefertigter Meinungen dienen, da »Andersdenkende« schnell aus diesem Zirkel ausgeschlossen werden. Ein großes Problem für die klassische

22 Dazu instruktiv *Luhmann*, Die Politik der Gesellschaft, 2002, S. 274 ff.

23 Dazu *Schulze-Fielitz*, in: Evangelisches Staatslexikon, Art. Öffentlichkeit (2006), S1655; s. auch *Jarren*, ZfP 24 (2014), 317 ff.; *Michelsen/Walter*, Unpolitische Demokratie, 2013, S. 105 ff., 373 ff.

24 *Habermas*, Strukturwandel der Öffentlichkeit, 1962; kritisch gegenüber Habermas *Bourdieu*, Über den Staat, 2014, S. 29 ff.; *Luhmann*, Die Politik der Gesellschaft, 2002, S. 288.

25 Dazu eingehend Siebter Zwischenbericht der Enquete-Kommission »Internet und digitale Gesellschaft«, Demokratie und Staat, BT-Drucks. 17/12290, 91 ff.; jüngst auch *Jarren*, Erfüllen die Medien heute einen demokratischen Auftrag?, in: ZfP 24 (2014), 317 ff.

Öffentlichkeitsfunktion des Parlaments besteht heute bereits darin, dass während der Plenartagungen Paralleldiskussionen in sozialen Netzwerken stattfinden, die den Kreis der repräsentativ zur Meinungsbildung Berechtigten weit überschreiten, die Aufmerksamkeit aus dem Plenum in den digitalen Raum verlagern und zum Teil auf einem Niveau stattfinden, das nicht annähernd Parlamentsgebräuchen und damit auch nicht parlamentarischem Ordnungsrecht entspricht.[26] Zugleich verlieren »klassische« Medien wie Zeitungen und Fernsehen dramatisch an Nutzern, da diese sich nur noch mithilfe von kostenlosen Inhalten des Internets ihre Meinung bilden. Da Öffentlichkeit bekanntlich durch Kommunikation entsteht, entstehen angesichts dieses neuen Kommunikationsverhaltens neue Herausforderungen von den Kommunikationsgrundrechten bis hin zur Öffentlichkeitsarbeit des Parlaments. Auch bei der gesellschaftlichen und erst recht rechtlichen Erfassung der digitalen Entwicklung besteht das Problem darin, dass alte Vorstellungsbilder zugrunde gelegt werden, die in der virtuellen Welt keine Berechtigung haben. Ein Kernproblem der digitalen Welt ist eben, dass wir uns keine zutreffenden Bilder machen können wie in der realen Welt. Die virtuelle Welt gaukelt uns Bilder vor, doch die eigentlichen digitalen Rechenoperationen bleiben unsichtbar. Der Börsen-Onlinehandel bildet derzeit ein abschreckendes Beispiel: Rechner und komplizierte Algorithmen wickeln in Bruchteilen von Sekunden milliardenschwere Transaktionen ab – ohne jede menschliche Mitwirkung[27]. Dies hat mit dem »Publikumshandel«, den man für die Idee der Börse als öffentlicher Marktplatz zur Preisbildung für Aktien etc. kreiert hat, nichts mehr gemein. Angesichts nachgewiesener und vermuteter Manipulationen ermitteln längst Staatsanwaltschaften weltweit. Soweit sind wir bei der Herstellung oder eben Manipulation der politischen öffentlichen Meinung[28] (noch) nicht, doch drohen parallele Gefahren durch die Digitalisierung der Öffentlichkeit. Dies liegt vor allem auch daran, dass es bislang kaum Qualitätskontrollen für politische Inhalte, Bilder, Videos etc. im Internet gibt. Klassischen Medien konnte aufgrund redaktioneller Qualitätskontrollen und eines zu erwartenden journalistischen Berufsethos ein ge-

---

26 Ohne dass in der Regel Ordnungsmaßnahmen möglich sind, da die Ordnungsgewalt des Präsidenten sich nur auf das eigentliche Plenum und allenfalls noch auf das Parlamentsgebäude bezieht.

27 Dazu populärwissenschaftlich *Schirrmacher*, Ego − Das Spiel des Lebens, 2013; s. auch *Han,* Psychopolitik, 2014, S. 77 ff.

28 Dazu *Luhmann*, Die Politik der Gesellschaft, 2002, S. 288, 295 f.

wisses Grundvertrauen entgegengebracht werden, das bei vielen digitalen Inhalten nicht angebracht ist. Diese Gefahr bewusster Manipulation wird unterstützt durch die als Errungenschaft gepriesene Anonymität des Netzes[29]. Wie gering der Schutz vor bewussten Meinungsmanipulationen heutzutage ist, zeigen abschreckende Beispiele eines digitalen Mobs bei irrtümlich einer Straftat Verdächtigten oder jüngst bei der russischen Kriegspropaganda im Ukraine-Konflikt. Diese Möglichkeiten der Steuerung der neuen (angeblich) öffentlichen Meinung werden zunehmend auch von politischen Parteien entdeckt und bewusst bedient.

b) Veränderungen der parlamentarischen Demokratie

Mit der Digitalisierung der Öffentlichkeit wird zugleich die Kontrollfunktion des Parlaments gegenüber der Regierung tangiert und bedroht, die angesichts geringer eigener Sanktionsinstrumente die Öffentlichkeit für ihre Wirksamkeit benötigt[30]. Diese Wahrheitskontrolle erweist sich für das Parlament dann als kaum noch leistbar, wenn die relevante Öffentlichkeit sich in digitale Medien und soziale Netzwerke verlagert. Die vorgebliche Medienvielfalt ist heute letztlich nur eine gewachsene Vielfalt an Zugangskanälen zu Informationen. Das Internet und dessen Inhalte bewirken wenig Verbesserung der redaktionellen Qualität und führen zu einer Segregierung der Öffentlichkeit in verschiedenen »Benutzergruppen«, die eben nicht demokratischen Maßstäben und Wertvorstellungen genügen (müssen).

Die Informations- und Kommunikationstechnik bietet durchaus erhebliche Chancen für die Weiterentwicklung der parlamentarischen Demokratie: Zunächst einmal bietet Informations- und Kommunikationstechnik dem Parlament sowie auch den einzelnen Abgeordneten neue Möglichkeiten zur Erschließung von Informationen und Informationsquellen, durch die das strukturelle Informationsdefizit gegenüber der Exekutive bei geschickter Nutzung der neuen Medien durchaus verringert werden kann. Zum anderen können – wie in der Verwaltung – auch parlamentarische

29 Dazu kritisch *Frank*, Meute mit Meinung, 2013, S. 44 f.

30 Schon *Adorno*, Eingriffe. Neun kritische Modelle, 1963, S. 164, hat erkannt: »Soll öffentliche Meinung legitim jene Kontrollfunktion ausüben, welche seit Locke die Theorie einer demokratischen Gesellschaft zuschreibt, dann muss sie selber in ihrer Wahrheit kontrollierbar sein.«

Arbeitsabläufe optimiert werden[31], die in vielen Diskussionen unter dem Schlagwort »papierloses Parlament« erörtert werden. Darüber hinaus bietet die Informations- und Kommunikationstechnik einfach und relativ kostengünstig zusätzliche Instrumente der Öffentlichkeitsarbeit wie z. B. Live-Übertragungen der Parlamentsdebatten im Internet, elektronische Newsletter oder sog. RSS-Feeds von Pressemitteilungen, Parlamentsdrucksachen etc. In der Regel wird mithilfe derartiger Instrumente allerdings nur die Quantität von Informationen, nicht aber zwingend die Qualität der parlamentarischen Öffentlichkeitsarbeit erhöht. Und schließlich bietet die Informations- und Kommunikationstechnik neue Formen der Interaktion mit Bürgerinnen und Bürgern auch zwischen den Wahlterminen, die zur Erhöhung bzw. Verstärkung der Responsivität führen können. Entscheidungs- und Beteiligungsverfahren bei komplexen Rechtsetzungsprozessen oder gar der Verfassunggebung, die Einrichtung von Bürgerforen oder auch die öffentliche Petition über das Internet sind lediglich Beispiele eines noch längst nicht ausgeschöpften Spielraumes. Die von vielen Bürgern und auch Politikern gepriesenen sozialen Netzwerke sind nach hier vertretener Auffassung für die Parlamentsarbeit eher ungeeignet, da die im Parlament behandelten Themen für soziale Netzwerke eher sperrig sind, eine prägnante und einheitliche Parlamentsmeinung systembedingt nur schwer zu formulieren ist und die Spontaneität eines Parlaments im Netz kaum zu gewährleisten ist. Fraglos müssen sich Parlamente aber noch mehr als bislang für die Digitalisierung der Gesellschaft und vor allem der Kommunikationsprozesse öffnen – dies wird allerdings nicht ohne finanzielle Ressourcen und ohne geeignetes Personal möglich sein. An beidem fehlt es jedoch. Der Deutsche Bundestag hat sich zwischenzeitlich in vorbildlicher Weise mit den Auswirkungen der Digitalisierung im Rahmen einer Enquetekommission beschäftigt, die auch neue Wege der Beteiligung von netzaffinen Bürgerinnen und Bürgern gegangen ist[32]. Im Hinblick auf die Weiterentwicklung der parlamentarischen Demokratie empfiehlt die Enquetekommission die Einführung von neuen Formen der digitalen politischen Partizipation[33].

---

31 Für die Verwaltung dazu *Schliesky u. a.*, Arbeitsteilung 2.0, 2013, S. 1 ff.

32 Dazu umfassend Siebter Zwischenbericht der Enquete-Kommission »Internet und digitale Gesellschaft«, Demokratie und Staat, BT-Drucks. 17/12290.

33 Siebter Zwischenbericht der Enquete-Kommission »Internet und digitale Gesellschaft«, Demokratie und Staat, BT-Drucks. 17/12290, S. 97 ff., auch zu Handlungsempfehlungen an die Legislative.

Manche Aspekte der Digitalisierung und insbesondere bestimmte Vorschläge zum Einsatz der Informations- und Kommunikationstechnik führen zu nicht zu vernachlässigenden Bedrohungsszenarien für die parlamentarische Demokratie. Dies gilt vor allem für Vorschläge einer permanenten technikgestützten diskursiven Mitwirkung oder sogar einer technikgestützten Entscheidungsmitwirkung aller Interessierten. Derartige Vorschläge tangieren die Repräsentationsfunktion des Parlaments und bedrohen letztlich das repräsentative System insgesamt. Hier ist insbesondere das Konzept der sog. »Liquid Democracy«[34] bzw. des »Liquid Feedback«, bei dem eine stetige Mitwirkung an demokratischen Entscheidungsprozessen via Internetpräsenz suggeriert wird. So charmant die Idee, interessierten Bürgerinnen und Bürgern mithilfe entsprechender IT-Programme an staatlichen Entscheidungsprozessen permanent zu beteiligen, auf den ersten Blick auch klingen mag, so bedenklich erscheint dies bei näherem Hinsehen. Denn viele Internet-Artikulationsmöglichkeiten stellen eine Form der »Scheinpartizipation« dar, mit denen letztlich nicht das Maß an politischer Partizipation, sondern die Frustration der Bürger gegenüber ihren demokratischen Institutionen erhöht wird[35]. Das sachbezogene Abstimmen im Online-Modus ist nicht mehr – wie im herkömmlichen parlamentarischen Entscheidungsprozess – das Ergebnis eines oftmals durchaus langwierigen Diskurses, sondern in der Regel nur noch Ausdruck einer spontanen Stimmung[36]. Jedermann, auch ein sonst nicht Wahl- oder Abstimmungsberechtigter, könnte an politischen Entscheidungsprozessen teilnehmen, ohne die Last der Verantwortung zu spüren oder gar zu tragen[37]. Vielmehr können Bürgerinnen und Bürger ihre Anstrengungen zur demokratischen Mitwirkung – die von der Online-Petition über Meinungsumfragen bis hin zu Online-Abstimmungen reicht – ohne jeglichen Aufwand dabei sein und der Illusion erliegen, durch einen Mausklick bereits politische Aktivität zu entfalten[38]. Der Fehler im Denkmodell von Liquid Democracy-Konzepten besteht insoweit darin, dass Partizipati-

34 Dazu *Buck*, ZParl. 2012, 626 ff.; *Seckelmann,* Wohin schwimmt die Demokratie? – »Liquid Democracy« auf dem Prüfstand, in: Hill u. a. (Fn. 15), S. 67 ff.; *Vogelmann*, APuZ 48/2012, 40 ff.

35 *Salzborn*, Politische Teilhabe im Netz ist überschätzt – das WWW ist nicht die Welt, in: Kemper u.a. (Hrsg.), Wirklichkeit 2.0, 2012, S. 276 (276 f.; 278).

36 Prägnant *Guggenberger*, APuZ 38-39/2012, 10.

37 *Guggenberger*, a.a.O.

38 *Salzborn* (Fn. 35), S. 276 (278); zur Gefahr permanenter Volksentscheide *Guggenberger*, a.a.O., (12 f.).

onsmöglichkeiten mit demokratischer Inklusion gleichgesetzt werden, wodurch ein Mangel an tatsächlicher Inklusion von derartigen Konzepten noch nicht einmal als Problem wahrgenommen werden kann[39]. Dementsprechend werden Erwartungen an das bestehende politische System geweckt, die dieses in technischer Hinsicht und strukturell weder erfüllen kann noch erfüllen darf. Und umgekehrt wird neuen technischen Konzepten problemlos die Erfüllung von demokratischen Integrationsleistungen des »alten« repräsentativen Systems zugeschrieben, die von den neuen Konzepten schon systembedingt nicht erreicht werden können.

### c) Grundlegender Reformbedarf

Zahlreiche Rechtsprobleme der Digitalisierung liegen darin begründet, dass die geltende Verfassungs- und Gesetzesordnung bestehende, an physischer Präsenz sowie Schriftlichkeit orientierte Strukturen abbildet. Das Erschließen des demokratischen Potenzials der Informations- und Kommunikationstechnik setzt ein anderes Theoriegebäude und an manchen Stellen auch veränderte rechtliche Vorgaben voraus. Die gänzlich anders strukturierte Informations- und Kommunikationstechnik darf nicht einfach bestehenden Theorien resp. gesetzlichen Regelungen aufgepfropft werden. So sind noch manche Ideen des Informations- und Kommunikationstechnik-Einsatzes etwa mit der Raum- und Zeitfunktion der repräsentativen Demokratie nicht vereinbar: Das Parlament ist der Ort der demokratischen Öffentlichkeit und damit der repräsentativen Demokratie. Es kann daher nicht ohne weiteres hingenommen werden, wenn »die Öffentlichkeit« sich in das Internet verlagert. Hinzu kommt, dass die Netzöffentlichkeit nichts mehr mit der etwa von *Habermas* beschriebenen Öffentlichkeit[40] zu tun hat. »Mit dem Zerfall des öffentlichen Raumes verschwindet das Fundament für jene Demokratie, die auf der Herausbildung eines gemeinsamen Willens im öffentlichen Raum beruht.«[41] Und auch der Zeitaspekt darf

---

39 Zutreffend *Buck*, ZParl. 2012, 626 (632).

40 *Habermas*, Strukturwandel der Öffentlichkeit, 1962, S. 122 ff.

41 *Han*, Digitale Rationalität, 2013, S. 11; zur Bedeutung und Veränderung des Raumes im Kontext moderner Informations- und Kommunikationstechnik *Schliesky*, Einführung: Die Vermessung des virtuellen Raumes, in: Hill/Schliesky (Hrsg.), Die Vermessung des virtuellen Raumes, E-Volution des Rechts- und Verwaltungssystems III, 2012, 659 (10 f.).

nicht übersehen werden: Die Beratungszeit für Anhörung, Nachdenken, politische Abstimmungen, Debatten, Einschaltung von Sachverständigen etc. fehlt bei einer stetigen »Gefällt mir«-Demokratie, bei der eine demokratische Teilhabe per Mausklick suggeriert wird[42]. Und welcher Bürger hat schon Zeit, den ganzen Tag über im Internet politische Diskussionen zu verfolgen und über diese abzustimmen? Demokratische Entscheidungsprozesse, die zugleich auch rechtstaatlichen Anforderungen wie insbesondere dem Gebot der Rationalität zu genügen haben, benötigen weitaus mehr Zeit als »einen Klick«. Vor allem aber ist die physische Präsenz in der Demokratie unverzichtbar[43], denn Diskussions-, Überzeugungs- und Entscheidungskultur setzt mehr als eine bloße Informationsbereitstellung im Netz voraus[44]. Körpersprache, Rhetorik oder überhaupt die Darbietung der eigenen politischen Meinung gehören zum Parlamentarismus[45].

## *5. Rechtsstaat*

Digitale Netzwerke, arbeitsteilige Prozesse und grenzüberschreitende Zusammenarbeit sind in der an strikten sachlichen und örtlichen Zuständigkeiten orientierten deutschen Kompetenzordnung, die durch das Bundesstaatsprinzip eine vertikale Potenzierung erfährt, nur schwer zu vereinbaren. Dieses Phänomen ist schon oft beschrieben worden[46] und bis heute nicht zufriedenstellend gelöst. Viele E-Government-Konzepte verstanden sich als »Generalangriff auf die Zuständigkeiten«, die - nicht ganz zu Unrecht - als veritables Hindernis für die Staats- und Verwaltungsmodernisierung ausgemacht wurden. Dabei wurde jedoch regelmäßig übersehen, dass die Zuständigkeitsordnung ihre Grundlage im Rechtsstaats- und Demokratieprinzip findet. Auch der politische Impetus zur Realisierung von E-Government-Anwendungen kurz nach der Jahrtausendwende hat letztlich nicht zu grundlegenden Änderungen im deutschen Zuständigkeitsdenken geführt, so dass sich viele Hoffnungen des E-Government nicht erfüllt

42 Gleiche Bedenken bei *Bull*, Netzpolitik: Freiheit und Rechtsschutz im Internet, 2013, S. 109.
43 *Guggenberger*, APuZ 38-39/2012, 10 (13).
44 Zutreffend *Kleinert*, APuZ 38-39/2012, 18 (21).
45 Dazu *Sarcinelli*, Politische Kommunikation in Deutschland, 2011, S. 230 ff.; s. auch *Gerhardt*, Öffentlichkeit, 2012, S. 548 f.
46 S. bereits *Schliesky*, NVwZ 2003, 1322 ff.

haben. Dies beruhigt aus Sicht der überkommenen Zuständigkeitsordnung und damit des klassischen Rechtsstaats- und Demokratieverständnisses, doch kann der digitale Staat vor diesem Hintergrund bislang weder als realisiert noch erst recht als bessere Alternative zu den klassischen Rechtsstaats- und Demokratieverbürgungen gesehen werden.

## *6. Gemeinwesen und Gemeinwohl*

Schon *Cicero* hat das Gemeinwesen als die »Sache des Volkes« definiert[47]. Er stellt dabei aber klar, dass Volk nicht jede Vereinigung von Menschen ist, die auf jede nur denkbare Weise sich wie eine Herde zusammengescharrt hat, sondern der Zusammenschluss einer größeren Menschenzahl, der auf der Grundlage einer Rechtsvereinbarung und einer Interessengemeinschaft erfolgt ist[48]. Die Gemeinwohlkonkretisierung bzw. -verwirklichung ist einer der ursprünglichen Staatszwecke[49].

Ein Gemeinwesen entsteht also nicht durch zufällige Zusammenballung von Individuen in einem digitalen Netzwerk: Der Schwarm ist kein Volk und kann keinen Staat bilden[50]. Und die bloße Summe der im Netz verfolgten Einzelinteressen begründet auch noch kein Gemeinwohl. Hier gilt insoweit das, was *Thomas von Aquin* festgestellt hat: »Wenn also eine Gesellschaft von Freien von ihrem Führer auf das Gemeinwohl der Gesellschaft hingelenkt wird, so wird diese Regierung recht und gerecht sein, wie es Freien angemessen ist. Wenn aber die Führung sich nicht das Gemeinwohl der Gesellschaft, sondern den persönlichen Vorteil des Führers zum Ziel setzt, so wird die Herrschaft ungerecht und wider die Natur sein.«[51]

---

47 *Cicero*, Über den Staat, I 25 (39): res publica - res populi.

48 *Cicero*, aaO.

49 Sie findet sich bereits bei *Aristoteles*, Politik, 1252 a I, S. 47; für den deutschen Verfassungsstaat BVerfGE 42, 312 (332); *Link*, VVDStRL 48 (1990), 7 (18, 19 ff.).

50 Dazu aus philosophischer Perspektive jüngst eingehend *Byung-Chul Han,* Im Schwarm - Ansichten des Digitalen, 2013.

51 *Von Aquin*, Über die Herrschaft der Fürsten, übers. von Friedrich Schreyvogl, Nachwort von Ulrich Matz, 1971, I 1 (s. 8).

### *7. Zwischenergebnis*

Die Summe dieser Einzelergebnisse führt zu dem ernüchternden Zwischenergebnis, dass die Maßstäbe des guten Staates in ihrer herkömmlichen verfassungsrechtlichen Ausprägung in der digitalen Welt nicht eingehalten werden. Dies liegt daran, dass die Maßstäbe, d.h. Verfassung und einfachgesetzliche Rechtsordnung, auf den Menschen und bestimmte technische Möglichkeiten und Interaktionsmedien ausgerichtet sind. Der digitale Staat muss daher nicht zwangsläufig ein schlechterer Staat sein - er erfüllt aber weniger gut die für die analoge Welt aufgestellten Maßstäbe.

## *III. Wege zu einem digitalen und besseren Staat*

Zugleich dürfte deutlich geworden sein, dass ein besserer Staat nicht allein dadurch entsteht, dass der überkommene Nationalstaat einfach »digitalisiert« wird. Die Digitalisierung ist kein Selbstzweck und hat für sich genommen nicht einmal einen Eigenwert. Ein rechtlich relevantes Interesse kommt ihr erst dann zu, wenn ein Parlament einem digitalen Aspekt einen rechtlichen Wert verleiht oder sie als Instrument einem vorhandenen Rechtswert zu besserer Geltung verhelfen kann. Für all dies ist eine Weiterentwicklung der Maßstabsnormen erforderlich, an denen die Digitalisierung dann wiederum zu messen ist, um Auswüchse und Beschneidungen von rechtlich geschützten Interessen zu vermeiden.

### *1. Überwindung der Staatlichkeit?*

Zunächst muss allerdings noch hinterfragt werden, ob »Staatlichkeit« überhaupt noch die passende Kategorie für die digitale Welt bildet. Jedenfalls das Internet als globales Netzwerk ist mit staatlichen Kategorien nicht zu erfassen: Staatsgebiet, Staatsvolk und Staatsgewalt im *Jellinek'schen* Sinne[52] lassen sich im »World Wide Web« nicht mehr identifizieren. Verschwörungstheoretiker, Sozialrevolutionäre und »digital nati-

52 *Jellinek,* Allgemeine Staatslehre,1914, zur Definition: S. 193, zum Staatsgebiet: S. 394 ff., zum Staatsvolk: S. 406 ff., zur Staatsgewalt: S. 427 ff.

ves« tragen daher bereits längst den Abgesang auf den Staat vor[53]. Die Diskussion erinnert allerdings an die Debatte über die Europäisierung des Staates, die ebenfalls nicht zu einer Abschaffung, wohl aber zur grundlegenden Veränderung der Staatlichkeit geführt hat[54]. Dementsprechend sind das Internet und globale (Handels-)Netzwerke zweifelsohne neue Phänomene, aber doch letztlich nur bestimmte Handlungsinstrumente und -modalitäten, die aufgrund von Enträumlichung und Entgrenzung schwerer zu regulieren sind. Die Staaten bleiben daher auch in der digitalen Welt zunächst einmal die entscheidenden Herrschaftsakteure. Allerdings ist eine größer gewordene Gefahr der Selbstreferentialisierung bestimmter Systeme nicht von der Hand zu weisen: So entziehen sich globale Handelssysteme mit den von ihnen installierten Schiedsgerichtsbarkeiten zunehmend staatlicher Normierung und staatlicher Rechtsprechung. Und der Computer-Börsenhandel nimmt bereits einen erheblichen Anteil des täglichen Wertpapierumsatzes ein und findet weitestgehend ohne aktuelles menschliches Zutun statt. Neben der Qualität der Algorithmen entscheiden nun bereits physische Gegebenheiten wie die Länge der Verbindungsleitungen über den nur noch in Millisekunden gemessenen Erfolg oder Misserfolg an Börsen. Und auch das zunehmend »autonome« Handeln von Robotern[55], die von Pflegeheimen bis zu selbstständigem Autofahren in immer mehr Bereichen zum Einsatz kommen, führt zu Entwicklungen, die nicht mehr in jedem Moment von Menschen gesteuert sind und für die es an Handlungsmaßstäben fehlt.

## *2. Ethik des digitalen Staates und der digitalen Gesellschaft*

Gerade an dem Beispiel verselbstständigter Maschinen wird deutlich, dass wir neue moralische Handlungsanleitungen für neue Konstellationen von Interessenkollisionen sowie für neue Möglichkeiten menschlichen oder eben auch roboterischen Handelns benötigen. Dazu ist eine philosophische und gesellschaftspolitische Diskussion erforderlich, die in rechtliche Re-

53 Für eine Ablösung der Demokratie vom Staat auch *Boehme-Neßler*, Von der Euro-Krise zur globalen Demokratie, ZRP 2012, 237 ff.

54 Dazu grundlegend *Schliesky* (Fn. 18), S. 445 ff.

55 S. etwa *Decker*, Roboter und Moral, in: Süddeutsche Zeitung Nr. 7 vom 10./11. Januar 2015, S. 5.

gelungen und ggf. auch verfassungsrechtliche Normierungen führt[56]. Fast noch trivial sind Haftungsregelungen für selbstfahrende Autos oder Pflegeroboter - doch fehlen auch sie bislang. Viel gravierender sind die eingangs skizzierten medizinischen Fortschritte, aufgrund derer zunehmend digitale Bauteile kranken Menschen implantiert werden. Die Diskussion über mögliche Grenzen digitaler Eigen- oder Fremdsteuerung sind dringend erforderlich und bedürfen einer ethischen Fundierung, da sie zentrale rechtliche Kategorien wie das Menschsein, das Persönlichkeitsrecht und auch andere Grundrechte tangieren. Die Staatshaftung für E-Government[57] gehört schließlich zu diesen Regelungsdesideraten ebenso wie die parlamentarische Interessenabwägung zwischen den Interessen eines Suchmaschinenanbieters, dem Persönlichkeitsrecht des von einer Veröffentlichung Betroffenen und den Interessen von Drittbetroffenen[58] bei dem Recht auf Vergessenwerden.

Erste Überlegungen zu einem »Digitalen Kodex«[59] zeigen, dass derartige Diskussionen langsam ihren Anfang nehmen. Mit Blick auf den Staat ist allerdings eher ein »digitaler Fürstenspiegel« erforderlich, der dem Staat und seinen Organen die Maßstäbe für einen guten bzw. besseren digitalen Staat an die Hand gibt. Die Arbeit an einem derartigen digitalen Fürstenspiegel umfasst nicht nur alle Bereiche des geltenden Verfassungsrechts, die auf die Auswirkungen der Digitalisierung hin zu überprüfen sind, sondern vor allem auch all die Bereiche des staatlichen und gesellschaftlichen Lebens, die mit der Digitalisierung neu entstehen. Nicht ohne Grund finden derartige ethisch getriebene Diskussionen gerade im Bereich

56 S. *Decker*, Roboter und Moral, Süddeutsche Zeitung Nr. 7 vom 10./11. Januar 2015, S. 5; *Omand*, Regeln für die schöne neue Welt, Frankfurter Allgemeine Zeitung Nr. 66 vom 19. März 2015, S. 6.

57 Dazu *Stelkens,* Staatshaftung und E-Governement: Verwaltungsorganisationsrechtliche Gestaltungsmöglichkeiten, in: Hill/Schliesky (Hrsg.), Auf dem Weg zum digitalen Staat – auch ein besserer Staat?, 2015, S. 189 ff..

58 Dazu *Schulz*, Abwägung und Schieflage: Vorrang des Rechts auf Vergessenwerden gegenüber anderen Interessen?, in: JuWissBlog vom 06.01.2015, www.juwiss.de/1-2015/#more-9710, zuletzt abgerufen am 12.01.2015.

59 Deutsches Institut für Vertrauen und Sicherheit im Internet (Hrsg.), Braucht Deutschland einen digitalen Kodex?, 2014.

des »cyberwar« statt, wie sowohl militär-[60] als auch friedenspolitische[61] Diskussionen zeigen.

Die Aufgabe ist alles andere als trivial: Verfassung, Rechtsordnung und Gesellschaft müssen in die digitale Welt geführt werden. Ohne direkten menschlichen Kontakt drohen allerdings Maßlosigkeit und Verrohung - wie man an zahlreichen Inhalten des Internets ablesen kann, für die es vorher kein Medium gegeben hätte und die man dem direkten Gegenüber nicht zu sagen gewagt hätte. Am Beispiel des demokratischen Diskurses wurde bereits oben gezeigt, dass »Like-Buttons« und Leserbriefforen der Zeitung den klassischen demokratischen Diskurs nicht ersetzen können[62]. Hoffnungsfroh stimmt insoweit, dass bereits Schulbücher existieren, die für den ethischen Diskurs in der digitalen Welt gedacht sind[63].

### *3. Neubestimmung der Maßstabsnormen*

Auf der Grundlage dieser ethischen Debatten und eines möglichst weitreichenden Konsenses bedarf es einer Weiterentwicklung der Maßstabsnormen für einen guten Staat. Dies mag auf dem ersten Blick nach einem Taschenspielertrick klingen, wenn man die Maßstabsnormen verändert, um dann am Ende den digitalen Staat als den besseren Staat bewerten zu können. Dieses Vorgehen ist aber zwingende Folge der neuen Ethik des digitalen Staates und der grundlegend veränderten Gesellschaft, für die eine »analoge Rechtsordnung« nicht mehr ausreicht. Diese Neubestimmung betrifft auch die Staatsfundamentalnormen und sichert uns Themen für viele weitere Tagungen. So wird man beispielsweise um eine Weiterent-

---

60 S. etwa die strategische Problemanalyse »cyberwar« des früheren Brigadegenerals *Kriesel* und das Anfang Mai 2014 eröffnete Forschungszentrum Cyber Defense (CODE) der Bundeswehr-Universität Neubiberg, s. dazu www.bundeswehr-journal.de/2013/ganzheitlicher-ansatz-in-der-cyber-abwehr/#more-1706, zuletzt abgerufen am 08.01.2015; s. ferner die Ausgabe 2014/2 des E-Journals Ethik und Militär, www.ethikundmilitaer.de/fileadmin/Journale/2014-12/Ausgabe_2014_2_DE.pdf, zuletzt aufgerufen am 12.01.2015.

61 S. etwa »Cyberpeace - Ein Gegenentwurf zur informatikgestützten Kriegsführung, Spionage und Überwachung« des Forums Informatikerinnen und Informatiker für Frieden und gesellschaftliche Verantwortung e.V. (FIfF), www.ag-friedensforschung.de/themen/Infowar/fiff2013-neu.html, zuletzt aufgerufen am 08.01.2015.

62 S. auch *Han*, Digitale Rationalität, 2013, S. 40 f.

63 Standpunkte der Ethik - Brisant: Digitale Welt.

wicklung des Demokratieprinzips nicht umhin kommen, wenn die digitale Welt nicht irrelevant für den demokratischen Diskurs bleiben soll. Über die Neubestimmung der Öffentlichkeit ist genauso nachzudenken wie über eine Bausteinlegitimation für staatliche Maßnahmen, die dann auch modulhaftes und arbeitsteiliges Handeln staatlicher Organe rechtfertigen kann. Wenn vor allem diese Weiterentwicklung des Demokratieprinzips gelingt, dann braucht der Pessimismus von *Helmut Willke* nicht geteilt zu werden: »Die Entzauberung der Demokratie als Steuerungsregime hochkomplexer Gesellschaften ist bereits unterwegs, weil (…) ihre Intelligenz nicht mehr ausreicht, um die wirklich gravierenden Probleme auch nur einigermaßen adäquat anzugehen.«[64]

Auch das Bundesstaatsprinzip und die konkrete Gestalt des deutschen Föderalismus sind erneuerungsbedürftig; die Kompetenzordnung des Grundgesetzes in ihrer herrschenden Auslegung im Sinne einer strikten Kompetenztrennung, wie sie das Bundesverfassungsgericht annimmt und die Föderalismusreform I verfassungspolitisch bekräftigt hat, werden einem arbeitsteiligen Zusammenwirken im digitalen Netzwerk nicht gerecht. Das Netzwerk bedarf einer verfassungsrechtlichen Absicherung, um über eine entsprechende institutionelle Legitimation zu verfügen, die dem Demokratieprinzip Stand hält. Ganz konkret sollte darüber hinaus nachgedacht werden, bundeseinheitlich grundlegende Basisinfrastrukturen zu ermöglichen und dafür eine (ggf. sogar ausschließliche) Bundeskompetenz in die Verfassung aufzunehmen. Diese sollte durch eine entsprechende Kompetenz für IT-Sicherheit[65] ergänzt werden. Und auch die punktuellen Antworten des Verfassunggebers auf die strikte Rechtsprechung des Bundesverfassungsgerichts in Art. 91 b, 91 c, 91 d und 91 e GG werden auf Dauer nicht ausreichen. Eine allgemeinere Regelung für IT-gestützte Verwaltungskooperation ist geboten, um längst praktizierte Kooperationen verschiedenster Akteure, die regelmäßig nur schwer mit der sachlichen Zuständigkeitsordnung vereinbar sind, nicht in vernetzter Beliebigkeit enden zu lassen.

Und schließlich ein drittes Beispiel: Staatliche Informationsverarbeitung und Wissensgenerierung entsprechen in Zeiten zahlreicher gemeinschaftsrechtlicher Vorgaben und moderner Informations- und Kommunikationstechnik nicht mehr den unterkomplexen linearen staatlichen Ent-

64 *Willke*, Demokratie in Zeiten der Konfusion, 2014, S. 162.

65 Zum Referentenentwurf für ein IT-Sicherheitsgesetz des Bundes *Roth*, ZD 2015, 17 ff.

scheidungsprozessen. Die Verfassung sollte auch an dieser Stelle die tatsächlich praktizierte Komplexität vernetzter Informationsbeziehungen zulassen, damit dem Staat und seinen Organen ein zeitgemäßes Informations- und Wissensmanagement möglich ist[66].

### *4. Digitalisierung als Schlüssel zur Staats- und Verwaltungsmodernisierung*

Mit entsprechenden ethischen und anschließend verfassungsrechtlichen Rahmenbedingungen kann dann auch endlich der Durchbruch bei der Staats- und Verwaltungsmodernisierung gelingen. Mehr als zehn Jahre Bemühungen um E-Government in Deutschland sind ohne durchgreifenden Erfolg geblieben, wenn auch zahlreiche Veränderungen durchaus bewirkt worden sind. Der »bessere Staat« ist hier allerdings meist noch nicht erreicht worden, weil zum einen die rechtlichen Rahmenbedingungen störten und zum anderen die herkömmlichen Denkansätze den neuen Möglichkeiten nicht gerecht werden konnten. Die zwar bereits bei dem Neuen Steuerungsmodell propagierte Bürger- bzw. Kundenorientierung[67] ist in der Regel nur Lippenbekenntnis geblieben, weil auch die elektronische Verwaltung meist nur im Rahmen von Zuständigkeiten entsteht und dementsprechend auch nur aus Sicht der Verwaltung gedacht wird. Bürgerinteressen kommen hier zu kurz, denn es kann wohl kaum als attraktiv gelten, wenn der Bürger für jede elektronisch nachgefragte Verwaltungshandlung ein neues Programm einer anderen Verwaltung »lernen« muss[68]. Das verwaltungspolitische Handwerkszeug in Gestalt von Prozessdenken[69], neuartiger Arbeitsteilung, Standardisierung oder neuen Figuren wie der Zuständigkeitsverzahnung[70] steht zur Verfügung, doch fehlt es an einem strategischen Ansatz zur Umsetzung im deutschen Bundesstaat. Aber den-

---

66 Dazu *Schliesky*, in: Hill u.a. (Hrsg.), Brauchen wir eine neue Verfassung?, 2014, S. 215 ff.

67 Dazu bspw. *Schedler/Proeller*, New Public Management, 2011, S. 71 ff.

68 S. dazu auch *Schliesky*, Wann wird das Rathaus völlig elektronisch?, in: 65 Jahre Kommunal- und Schulverlag, 2014, S. 103 ff.

69 Dazu *Hill*, Prozessflexibilisierung und adaptive Prozessentwicklung, DÖV 2012, 249 ff.; *Schliesky*, in: Schliesky (Hrsg.), Die Umsetzung der EU-Dienstleistungsrichtlinie in der deutschen Verwaltung, Teil 3, 2010, S. 91 (113 f.).

70 Vorgeschlagen von *Schliesky* (Fn. 69), S. 91 ff. (114 f.); aufgegriffen von *Ziekow*, in: Schliesky (Fn. 69), S. 141 ff.

noch besteht begründeter Optimismus, dass auf diesem Weg der Staats- und Verwaltungsmodernisierung ein funktional besserer Staat erreichbar ist.

## *IV. Fazit*

»Das Internet manifestiert sich heute nicht als ein öffentlicher Raum, als ein Raum des gemeinsamen, kommunikativen Handelns. Es zerfällt vielmehr zu Privat- und Ausstellungsräumen des Ich.«[71] Diese Aussage *Byung-Chul Hans* verdeutlicht, wie sehr die Digitalisierung staatliche Grundstrukturen erschüttert und gerade auch zentrale demokratische Grundvoraussetzungen wie etwa die diskursorientierte demokratische Öffentlichkeit infrage stellt. Wir leben zweifelsohne in einer Transitionsphase, bei der wir nicht sicher wissen können, wohin sich der Staat entwickelt. Eines aber wissen wir sicher: Die herkömmlichen Maßstäbe für einen guten (analogen) Staat passen nicht mehr, neue müssen erst entwickelt werden. Die Ethik der digitalen Gesellschaft und des digitalen Staates steht noch aus, der digitale Fürstenspiegel muss erst noch geschrieben werden. Grundlegende Verfassungsfunktionen bedürfen der Überprüfung, und mit ihnen die Herrschafts- und Steuerungsinstrumente. Die Notwendigkeit einer grundlegenden Staats- und Verwaltungsmodernisierung wächst stetig, weil eben die Kluft zwischen digitaler Realität und analoger Normativität von Tag zu Tag größer wird. Eine solche Modernisierung wird allerdings mit dem rasanten Bröckeln unserer bisherigen gesellschaftlichen Gewissheiten nicht einfacher. Dennoch kann der Staat im digitalen Zeitalter ein besserer Staat werden, wenn die geforderte Ethik entsteht und auf ihrer Basis die faszinierenden Möglichkeiten der Informations- und Kommunikationstechnik, der künstlichen Intelligenz und der neuen arbeitsteiligen Möglichkeiten in den Dienst der Menschen und ihrer Grundwerte gestellt werden. »Die erste Bürgerpflicht ist, seinem Vaterlande zu dienen.«[72] Mit diesem Satz beginnt *Friedrich der Große* sein »Politisches Testament«, und auch diese ethische Forderung kann in die digitale Welt übersetzt werden. Wenn es gelingt, die Möglichkeiten der neuen Techniken in den Dienst der Menschen zu stellen, und der Staat ihre Ge-

71 *Byung-Chul Han*, Digitale Rationalität und das Ende des kommunikativen Handelns, 2013, S. 7.

72 *Friedrich der Große*, Das Politische Testament von 1752, 1974/2001, S. 3.

fahren für Menschenwürde, Freiheit und Sicherheit der Bürgerinnen und Bürger im Griff behalten kann - dann ist der digitale Staat tatsächlich ein besserer Staat.

# Informational Privacy im Spiegel unterschiedlicher Rechtskulturen*

*Michael Fehling*

## *I. Einführung*

Die digitale Welt ist ohne breite transatlantische Datenströme nicht vorstellbar. Europa wird sich zwar bei der Internet-Sicherheitsarchitektur stärker von den USA emanzipieren und mittelfristig auch gewisse Gegengewichte zur Allmacht von Google und Facebook aufbauen können und müssen.[1] Ein weitreichendes Entkoppeln wäre indes nicht nur ökonomisch wenig realistisch, sondern stünde auch diametral im Gegensatz zum Versprechen weltweiter Vernetzung, zur Hoffnung auf die »eine Welt«, wenn schon nicht in der Realität, dann doch wenigstens virtuell.

So sehr uns dieses Anliegen auf beiden Seiten des Atlantiks eint, so deutlich unterscheidet sich allerdings das Verständnis von *Privacy* im Allgemeinen und *Informational Privacy* im Besonderen zwischen Deutschland und Kontinentaleuropa (wenngleich mit erheblichen Unterschiede zwischen den Mitgliedstaaten) einerseits und den USA andererseits. Im Grundsatz durchaus zu Recht betonen viele, der Datenschutz sei in den USA jedenfalls im Privatrechtsverkehr weitaus schwächer ausgeprägt als in Kontinentaleuropa; dafür genieße der freie Informationsfluss in den USA einen höheren Stellenwert.[2] Bei näherem Hinsehen wird das Bild

---

* Meinem studentischen Mitarbeiter Philipp Fritsche sowie meiner früheren wiss. Mitarbeiterin Barbara Schunicht danke ich für wertvolle Unterstützung vor allem bei den Nachweisen.

1 Gestützt auf grundrechtliche Schutzpflichten und Art. 87 f Abs. 1 GG Hoffmann-Riem, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, JZ 2014, 53 ff.; Lenski, Alter Datenschutz und neue Datenströme im Lichte der NSA-Affäre, ZG 2014, 324, 336 ff.

2 Besonders pronounciert Whitman, The Two Western Cultures of Privacy: Dignity Versus Liberty, 113 Yale L.J. 1161 ff. (2004); ferner etwa Fehling, Evolving Law and Economics in the Evolving Technological Environment – Comment on Haksoo Ko –, in: Eger/Oeter/Voigt (Hrsg.), Economic Analysis of International Law, 2014, S. 99, 100, 102; vgl. auch Hanschmann, Das Verschwinden des Grundrechts auf

freilich vielschichtiger, werden unterschiedliche Perspektiven auf das Thema deutlich, die sich teilweise überlappen, in Teilbereichen aber auch ausschließen.

## II. Übergreifender versus sektorspezifisch punktuellem Schutz von Informational Privacy

Nimmt man den Normtext als Ausgangspunkt, so zeigt sich schon hier ein gewichtiger Unterschied. In Deutschland ist das Datenschutzrecht in entsprechenden Bundes- und Landesgesetzen, auf europäischer Ebene in einer Datenschutz-Richtlinie[3] und künftig vor allem in einer EU-Grundverordnung[4] allgemein und übergreifend normiert. Zwar finden sich vereinzelt auch bereichsspezifische Bestimmungen, die teilweise besondere einwilligungsunabhängige Datenverarbeitungsermächtigungen enthalten,[5] teilweise aber auch einen erhöhten Geheimnisschutz für als besonders sensibel eingestufte Daten oder Informationsbeziehungen anordnen.[6] Aber die zentralen Regeln für die Macht- und Verantwortungsstrukturen in der digitalen Welt sind auf personenbezogene Daten aller Art anwendbar, mit Regelungen sowohl für die Datenverarbeitung durch den Staat als auch im privaten Bereich. Ein solches allgemeines Datenschutzrecht (*omnibus le-*

---

Datenschutz gegen hoheitliche Maßnahmen in der Pluralität von Rechtsregimen, in: Matz-Lück/Hong (Hrsg.), Grundrechte und Grundfreiheiten im Mehrebenensystem, 2012, S. 293 (328 ff.).

3 Rl 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Warenverkehr, ABl. 2001 Nr. L 281, S. 31.

4 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 11. Juni 2015, abrufbar unter: http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf (Stand: 21. August 2015).

5 Grundrechtsdogmatisch liegt dem vielfach die Erwägung zu Grunde, dass den speziellen Verhältnissen auch andere Grundrechte mitbetroffen sind und insoweit mit der informationellen Selbstbestimmung praktische Konkordanz hergestellt werden muss. Dies betrifft etwa bei der Forschung die Wissenschaftsfreiheit. Simitis, Privacy – An Endless Debate?, 98 Cal. L. Rev. 1989, 2000 (2010), sieht darin schon eine Annäherung an den US-amerikanischen Ansatz.

6 Schutzverstärkend wirkt etwa beim Informantenschutz die Pressefreiheit, im Verhältnis von Anwalt und Mandanten sind es die Justizgrundrechte, zwischen Gläubigen und Geistlichen greift die Religionsfreiheit ein.

*gislation*) existiert in den USA nicht und ist auch künftig nicht zu erwarten.[7] Man beschränkt sich auf wenige sektorspezifische Regelungen vor allem zum Geheimnisschutz dort, wo man bestimmte Daten für besonders sensibel hält und deshalb in der Datenweitergabe typisierend eine Gefahr für den Bürger in seiner Privatheit gegenüber dem Staat sieht. Den weitesten Anwendungsbereich besitzt dabei der *Federal Privacy Act*, der die Offenlegung (*disclosure*) von eng verstandenen persönlichen Informationen, die bei einer Bundesbehörde vorliegen, von der schriftlichen Einwilligung des Betroffenen abhängig macht.[8] Zwar werden auch in den USA für die *Informational Privacy* (mehr als für *Privacy* allgemein[9]) vereinzelt umfassendere Schutzkonzepte diskutiert;[10] in Gesetzgebung und Rechtsprechung sind solche Konzepte jedoch zumindest auf Bundesebene[11] nicht durchgedrungen.

Das *Common Law* vermag die Lücken in der Gesetzgebung nur punktuell zu schließen. Im Lichte der Privatautonomie basiert die Datennutzung im Privatrechtsverkehr auf *notice and choice*. Die Information über die *privacy policy* des Unternehmens kann jedoch unspezifisch bleiben oder umgekehrt extrem umfangreich und dadurch kaum mehr lesbar sein: Die Alternative beschränkt sich oft darauf, auf den Abschluss eines Vertrags mit dem entsprechenden Unternehmen zu verzichten. Wo eine darüber hinausgehende Wahlmöglichkeit eröffnet wird, genügt meist ein bloßes Widerspruchsrecht.[12] Das *Tort Law* kennt im Gegensatz zu § 823 BGB keinen allgemeinen Schadensersatzanspruch bei *Privacy*-Verletzungen, vielmehr werden nach herrschender Auffassung (im maßgeblichen *Restate-*

---

7 Betont etwa von Schwartz, The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures, 126 Harv.L.Rev. 1966, 1974 (2013); Schwarz/Solove, Reworking Information Privacy Law. A Memorandum Regarding Future ALI Projects About Information Privacy Law, 2012, S. 34 f.

8 Überblick bei Strahilewitz, Reunifying Privacy Law, 98 Cal. L. Rev. 2007, 2224 ff. (2010); vgl. auch NASA v. Nelson, 562 U.S. 134 (2011), S. 156; Aufzählung weiterer Regelungen bei Determann, NVwZ 2016, 561, 564.

9 Dies betont Eifert, Autonomie und Sozialität: Schutz durch informationelle Selbstbestimmung, Ringvorlesung an der Bucerius Law School am 17.3.2015 (Veröffentlichung in Vorbereitung).

10 Berühmt und grundlegend Warren/Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 ff. (1890).

11 Nachweise über zum Teil weiterreichende Entscheidungen der Gerichte der Bundestaaten in NASA v. Nelson, 562 U.S. 134, dortige Fn. 9 (2011).

12 Kurzüberblick bei Schwarz/Solove, Reworking Information Privacy Law (Fn. 7), S. 31 ff.

*ment of Torts*[13]) nur vier spezifische eng ausgelegte Beeinträchtigungen erfasst: (1) Eindringen in die innere Privatsphäre, (2) Veröffentlichung von peinlichen privaten Fakten, (3) unzutreffende Darstellung in der Öffentlichkeit sowie (4) Namens- und Identitätsdiebstahl.[14] Ein übergreifender Schutz legitimer Privatheitsinteressen wird nicht zuletzt deshalb abgelehnt, weil dies zur Uferlosigkeit tendiere.[15]

Der Unterschied zwischen übergreifendem Schutz und fragmentierten Einzelregelungen pflanzt sich auf Verfassungsebene fort. In Deutschland sorgt bekanntlich das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) mit den Gewährleistungen der informationellen Selbstbestimmung[16] sowie der Vertraulichkeit und Integrität informationstechnischer Systeme[17] für einen gegenständlich umfassenden Schutz, gegebenenfalls überlagert durch den spezielleren Schutz des Telekommunikationsgeheimnisses (Art. 10 GG) und der Unverletzlichkeit der Wohnung (Art. 13 GG). Zwar mag dieser Selbstbestimmungsschutz wiederum akzessorisch auf speziellere grundrechtliche Gewährleistungen ausgerichtet sein, um diese bereits im Vorfeld gegen einzelne spezifische Gefährdungen abzusichern.[18] Doch ändert dies nichts daran, dass dem Grundgesetz in seiner Auslegung durch das Bundesverfassungsgericht zunächst einmal ein übergreifendes grundrechtliches Schutzkonzept für die Selbstentfaltung im Umgang mit personenbezogenen Daten zugrunde liegt. Auf europäischer Ebene ist über die allgemeine Privatsphäre-Gewährleistung (Art. 7 GrCh, Art. 8 EMRK) hinaus das Recht auf Schutz personenbezogener Daten in der Grundrechte-Charta (Art. 9) sogar explizit aufgeführt.

---

13 Restatement (Second) of Torts §§ 652B-652E (1977).

14 Zurückgehend auf Prosser, z.B. Privacy, 48 Cal. L. Rev. 383 ff. (1960); für eine Verteidigung dieses Ansatzes in jüngerer Zeit aus rechtsvergleichender Perspektive Schwartz/Peifer, Prosser´s Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Approach?, 98 Cal. L. Rev. 1925, 1937 ff. (2010); kritisch etwa Strahilewitz (Fn. 8), 98 Cal. L. Rev. 2007, 2236 ff. (2010); vgl. auch Schwarz/Solove, Reworking Information Privacy Law (Fn. 7), S. 7 ff.

15 Besonders deutlich Gerety, Redefining Privacy, 12 Harv.C.R-C.L L Rev. 233, 234 (1977); Schwartz/Peifer (Fn. 14), 98 Cal. L. Rev. 1925, 1963 (2010).

16 Grundlegend BVerfGE 65, 1 – Volkszählung.

17 Grundlegend BVerfGE 120, 274 – Online-Durchsuchung.

18 Britz, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, 2010, S. 561, 563 u. 573 f. Näher dazu unten III. 3.

In den USA gibt es dagegen kein kodifiziertes allgemeines Grundrecht auf *Informational Privacy*. Der *Supreme Court* hat jüngst erneut offen gelassen, ob eine *Privacy*-Verbürgung, den Schutz gegen die Offenlegung gesammelter personenbezogener Daten betreffend, im Wege der Rechtsfortbildung konstruierbar wäre,[19] etwa wie teilweise vorgeschlagen in Gestalt eines *Substantive Informational Due Process*.[20] Von einem solchen bloßen Schutz gegen Offenlegung (*disclosure*) wäre die Datenerhebung wohl ohnehin nicht erfasst.[21] Anleihen nimmt man vielmehr bei der räumlichen Privatheit. *Privacy* wird deshalb in Parallele zu der im *Fourth Amendment* garantierten Unverletzlichkeit der Wohnung (*home*)[22] und dem Schutz vor Durchsuchungen allgemein (*search*) konstruiert und auch nur in diesem Umfang verfassungsrechtlich anerkannt. Der dazu von der Judikatur entwickelte Standard der »*resonable expectations of privacy*«[23] war zwar ursprünglich durchaus auf Erweiterung des Privatheitsschutzes gegenüber dem Staat auch im Sinne eines gewissen Datenschutzes angelegt, wurde vom *Supreme Court* indes später wieder zunehmend enger auf den räumlichen Herrschaftsbereich zurückgeführt.[24] Erst in jüngster Zeit fand wieder eine vorsichtige Ausweitung statt.[25] Die *Privacy*-Verbürgung

---

19 Zuletzt in NASA v. Nelson, 562 U.S. 134 (2011), S. 138 u. 148 f., explizit dagegen mangels Verankerung von *Privacy* im Verfassungstext die abw. Meinung von Scalia. Die Frage war zuvor vom Supreme Court nur zweimal in den 1970er Jahren überhaupt aufgeworfen und damals ebenfalls offen gelassen worden, nämlich in Whalen v. Roe, 429 U.S. 589, 599, 605 (1977) und in Nixon v. Administrator of General Services, 433 U.S. 425, 457 (1977); dazu auch Wittmann, Der Schutz der Privatsphäre vor staatlichen Überwachungsmaßnahmen durch die US-amerikanische Bundesverfassung, 2014, S. 44 ff.

20 Chlapowski, The Constitutional Protection of Informational Privacy, 71 Boston University L. Rev. 133 (1991).

21 NASA v. Nelson, 562 U.S. 134 (2011), S. 155 f. rechtfertigt die Datenerhebung nicht zuletzt mit der Erwägung, der Schutz gegen unberechtigte Offenlegung reiche aus.

22 Zu den britischen Wurzeln der sogenannten „Castle-Doctrine“ Geminn/Roßnagel, „Privatheit“ und „Privatsphäre“ aus der Perspektive des Rechts – Ein Überblick, JZ 2015, 703, 704.

23 Grundlegend Katz v. United States (1967), 389 U.S. 347, 361.

24 Die Entwicklung wird ausführlich nachgezeichnet und analysiert bei Wittmann, Der Schutz der Privatsphäre (Fn. 19), S. 61 ff., zusammenfassend S. 789 ff.; Slobogin, Die Zukunft des Datenschutzes in den USA, Die Verwaltung 44 (2011), 465, 467 ff.

25 Zuletzt Riley v. California, No. 13-132 (2014) die Auswertung eines Smartphones bei einem Verhafteten betreffend.

wird zusätzlich dadurch verringert, dass in Kollisionsfällen der Schutz, den die freie Informationsweitergabe durch Private ihrerseits durch die *Free Speech*-Garantie des *First Amendment* genießt, regelmäßig Vorrang erhält.[26] In Deutschland dagegen – und vergleichbar auf EU-Ebene[27] – ist in solchen Konstellationen eine einzelfallbezogene Abwägung vorzunehmen, worin der im Ansatz durchaus vergleichbare Schutz des Art. 5 Abs. 1 GG weit seltener eine solch hohe Gewichtung erfährt.[28]

### *III. Unterschiedliche Traditionen und Blickwinkel als Hintergrund*

Hinter dem skizzierten positiv-rechtlichen Befund verbergen sich rechtskulturell fundierte Unterschiede, die sich schlagwortartig verkürzend in verschiedene Gegensatzpaare einkleiden lassen.

#### *1. Menschenwürde versus Liberty und im Privatrechtsverkehr Property Rights*

Wie schon die dogmatische Verankerung in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG deutlich macht, basiert die deutsche Vorstellung von informationeller Selbstbestimmung (wie im Übrigen auch das Urheberpersönlich-

---

26 Besonders betont von Volokh, Freedom of Speech and Information Privacy, 562 Stanford L. Rev. 1049 ff. (2000). Der *Supreme Court* hat z.B. ein Gesetz von Vermont, das den Verkauf und die Veröffentlichung von Medikamenten-Verschreibungslisten mit Personenbezug eingeschränkt hatte, wegen Verstoßes gegen die Free Speech-Garantie aufgehoben, siehe Sorell v. IMS Health, 131 S.Ct. 2653 (2011); dazu Schwarz/Solove, Reworking Information Privacy Law (Fn. 7), S. 38 f.

27 Vgl. EuGH Rs. C-101/01 (Lindqist), Slg. 2003, I-12971, Rn. 79 ff.; EuGH Rs. C-73/07 (Satakunnam), Slg. 2008, I-09831, Rn. 52 ff.; zusammenfassend Schneider, Stand und Perspektiven des europäischen Datenverkehrs- und Datenschutzrechts, Die Verwaltung 44 (2011), 499, 511. Besondere Probleme bereitet die Abwägung bei dem in der Google-Entscheidung des EuGH, Urt. v. 13.5.2014, Rs. C-131/12 (Google), JZ 2014, 1009 ff. kreierten Recht auf Vergessen; dazu Spindler, JZ 2014, 981 ff. und Boehme-Neßler, NVwZ 2014, 825 ff.

28 Eine Ausnahme bildet Masing, Herausforderungen des Datenschutzes, NJW 2012, 2305, 2306. Zu sich abzeichnenden Veränderungen bei Informationszugangsrechten siehe unten III. 4. mit Fn. 117.

keitsrecht[29]) wesentlich auf der Menschenwürde. Das Recht, selbst zu bestimmen, welche persönlichen Lebensumstände man Dritten offenbart, erscheint als Ausfluss der Personalität und Autonomie des Menschen. Die Ausrichtung auf die Menschenwürde als historische Reaktion auf Diktatur und Nationalsozialismus prägt, nicht zuletzt aufgrund deutschen Einflusses, zumindest im Ansatz nun auch die EU-Grundrechtecharta und die dortige sinngemäße Verbürgung informationeller Selbstbestimmung.[30] Ohnehin spielte das deutsche Vorbild für das dortige Recht in der Genese wohl eine wichtige Rolle.[31]

Den US-amerikanischen Grundrechten und der *Privacy*-Konzeption ist demgegenüber, wie schon oft vergleichend betont,[32] eine Verankerung in einem übergreifenden Würdekonzept fremd. Menschenwürde gilt als rechtlich zu wenig fassbar, wird insoweit sogar in eine Reihe mit *happiness* gestellt.[33] Teilweise setzt man dort Menschenwürde auch zu sehr mit Ehrschutz gleich, den man aus US-Sicht wegen der aristokratischen Wurzeln in Europa für übersteigert hält.[34] *Whitman* versteigt sich sogar zu der These, der Nationalsozialismus habe mit der Betonung der »Ehre« jedes »Volksgenossen« um seines »deutschen/arischen Blutes« willen einen wichtigen Beitrag zur Verbreiterung des zuvor auf den Adel beschränkten

---

29 Parallele bei Mayer-Schönberger, Beyond Privacy. Beyond Rights – Toward a „Systems" Theory of Information Governance, 98 Cal. L. Rev. 1853, 1857 ff. (2010).

30 Borowsky, in: Meyer (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Aufl. 2014, Art. 1 Rn. 28. anders Kranenborg, in: Peers/Hervey/Kenner/Ward (Hrsg.), The EU Charter of Fundamental Rights, 2014, Rn. 08.24 ff. wonach das Recht auf informationelle Selbstbestimmung gerade nicht explizit in Art. 8 GrCh enthalten, sondern lediglich ein Bestandteil des in Art. 8 GrCh verbürgten europäischen Datenschutzrechts sei: „The proposal to formulate it as a right to informational self-determination was rejected."

31 Die „konzeptionelle Vergleichbarkeit" betonend Siemen, Datenschutz als europäisches Grundrecht, 2006, S. 293, vgl. auch S. 132, 211, 231; zusammenfassend Schneider (Fn. 27), Die Verwaltung 44 (2011), 499, 502; relativierend Kranenborg, in: Peers/Hervey/Kenner/Ward (Fn. 30), Rn. 08.24 ff.

32 Aus US-Sicht übergreifend etwa Eberle, Human Dignity, Privacy and Personality in German and American Constitutional Law, 1997 Utah L. Rev. 963, 1048 ff.

33 Schwartz/Peifer (Fn. 14), 98 Cal. L. Rev. 1925, 1982 (2010). Eine seltene Ausnahme bildet Bloustein, Privacy as an Aspect of Human Dignity: An Answer to Dean Posser, 39 N.Y.U. L. Rev. 962 (1964).

34 Whitman (Fn. 2), 113 Yale L.J. 1161, 1169 f. (2004).

Würdekonzepts geleistet.[35] Das deutsche Denken in solch unbestimmten Großformeln wie Menschenwürde oder informationeller Selbstbestimmung widerspricht vor allem im Privatrecht dem *Case Law*-Ansatz, der sich auch und gerade bei *Privacy* typischerweise auf Fallgruppen mittlerer Abstraktionshöhe stützt.[36] Wenn man überhaupt nach einem tieferen konzeptionellen Hintergrund des vorhandenen fragmentierten Schutzes von *Informational Privacy* in den USA sucht, so ist dies eher der Freiheitsschutz (*liberty*), vor allem gegenüber dem Staat[37] mit dem *Fourth Amendment* im Zentrum. Das Schutzniveau bleibt freilich niedrig, was der *Supreme Court* nicht zuletzt mit den angeblich[38] geringen Privatheitserwartungen der US-Bürger[39] rechtfertigt. *Liberty* spielt in Gestalt der Privatautonomie auch im Privatrechtsverkehr eine zentrale Rolle. Dort erscheint indes, ausgehend vom *Tort Law*, eine Parallele zu den *Property Rights* noch wirkmächtiger.[40] Dazu trägt nicht zuletzt die weit verbreitete ökonomische Analyse des Rechts bei, die das Konzept der *Property Rights* vom Eigentum im engeren Sinne gelöst und auf Verfügungsrechte aller Art erweitert hat.[41] Manche wollen mit dem *Property Rights*-Ansatz die wirtschaftliche

35 Whitman (Fn. 2), 113 Yale L.J. 1161, 1187 f. (2004); demgegenüber richtigstellend Schwartz/Peifer (Fn. 14), 98 Cal. L. Rev. 1925, 1949 (2010).

36 Zu den vier *Privacy-Torts* siehe oben II. mit Fn. 14.

37 Whitman (Fn. 2), 113 Yale L.J. 1161, 1169 f. (2004); kritisch wegen der zu einseitigen und tendenziell datenschutzfeindlichen Betonung des Freiheitsschutzes in den USA Bignami, European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining, B.C. L. Rev. 48 (2007), 609 (681 ff.); Wittmann, Der Schutz der Privatsphäre (Fn. 19), S. 444 ff.; siehe auch Diggelmann, Grundrechtsschutz der Privatheit, VVDStRL 70 (2011), 50, 70 mit dortiger Fn. 82.

38 Eingehende Kritik daran, auf einer intensiven Auswertung der US-Literatur fußend, bei Wittmann, Der Schutz der Privatsphäre (Fn. 19), insb. S. 452 ff.; Slobogin (Fn. 24), Die Verwaltung 44 (2011), 465, 478 ff.

39 Zum Standard der „reasonable expectations of privacy“ siehe oben II. mit Fn. 23, 24.

40 Dies geht über die Law and Economics-Anhänger im engeren Sinne hinaus, grundlegend für einen „national information market“ insoweit Laudon, Markets and Privacy, 39 Comm. of the ACM 92 (1996); dem europäischen würdebasierten Ansatz gegenübergestellt bei Mayer-Schönberger (Fn. 29), 98 Cal. L. Rev. 1853, 1862 f. (2010).

41 Im vorliegenden Zusammenhang grundlegend Posner, The Right of Privacy, 12 Georgia L. Rev., 393 ff. (1978); aus jüngerer Zeit etwa Murphy, Property Rights in Personal Information: An Economic Defense of Privacy, 84 Georgetown L.J., (1996), 2381 ff.; Varian, Economic Aspects of Personal Privacy, in: National

Verfügungsmacht des Einzelnen über seine Daten ausbauen.[42] Doch häufiger (vor allem bei den Anhängern der ökonomischen Analyse) führt dieser Ansatz nicht zu einem erhöhten Datenschutz, sondern gerade umgekehrt zu einer weitreichenden Nutzungsbefugnis auch für fremde persönliche Daten. Wie noch näher zu betrachten,[43] begünstigt die Ökonomisierung eine Sichtweise, wonach Datenschutz tendenziell als Hindernis für eine durch Verträge optimierte individuelle Nutzenmaximierung erscheint. Ein freier Informationsfluss vermeidet aus diesem Blickwinkel in erster Linie Transaktionskosten.

Man kann sich freilich fragen, ob diese unterschiedlichen Konzepte auch in ihren Auswirkungen wirklich so weit voneinander entfernt sind, wie es zunächst den Anschein hat. So ist der würdebasierte Ansatz schon im deutschen Verständnis nicht konkurrenzlos. Vereinzelt wird, von einigen missverständlichen Formulierungen im Volkszählungsurteil ausgehend, informationelle Selbstbestimmung sogar als eigentumsähnliches Verfügungsrecht über die eigenen Daten beschrieben.[44] Doch verbindet sich damit im Gegensatz zu den USA eher eine übersteigerte Vorstellung von individueller Daten-Hoheit. [45] Letztlich sind es Autonomie und Sozialität des Menschen,[46] denen beide Rechtsordnungen gleichermaßen Rechnung tragen müssen. Wie das Bundesverfassungsgericht klargestellt hat, besitzt der Einzelne kein Recht, allein darüber zu bestimmen, wie er in der Öffentlichkeit dargestellt wird und welches Bild sich Dritte von seiner Person machen können.[47] Ferner ist auch im deutschen Verfassungsver-

---

Telecommunications and Information Administration, Privacy and Self-Regulation in the Information-Age, 1996.

42 So etwa Laudon (Fn. 40), 39 Comm. of the ACM 92 (1996); Lessig, Code and other Laws of Cyberspace, 1999, S. 122 ff.

43 Siehe unten III. 4.

44 Vgl. Kilian, Informationelle Selbstbestimmung und Marktprozesse, CR 2002, 921, 925 ff.; vgl. auch Götting, Persönlichkeitsrechte als Vermögensrechte, 1995, insb. S. 139 ff.

45 Grundlegend zur Kritik an einer eigentumsanalogen Konstruktion Albers, Zur Neukonzeption des grundrechtlichen „Daten"schutzes, in: Haratsch/Kugelmann/Repkewitz (Hrsg.), Herausforderungen an das Recht der Informationsgesellschaft, 1996, S. 113; vgl. auch Schoch, Das Recht auf informationelle Selbstbestimmung in der Informationsgesellschaft, in: FS Stern, 2012, S. 1491, 1495 f.

46 So das Oberthema für die Vorträge von Britz und Eifert in der Ringvorlesung an der Bucerius Law School am 17.3.2015 (Veröffentlichung in Vorbereitung).

47 BVerfGE 65, 1, 42 f.; hervorgehoben von Britz, in: Hoffmann-Riem (Fn. 18), S. 561, 566.

ständnis informationelle Selbstbestimmung keineswegs auf Abschottung fixiert, sondern beinhaltet auch das Recht, seine Persönlichkeit gerade mittels Austausch von Daten mit Dritten zu entfalten.[48] Dies schließt die Befugnis zur eigenen ökonomisierten Datennutzung grundsätzlich mit ein.[49] Umgekehrt finden sich auch in den USA einzelne als besonders sensibel angesehene Bereiche, in denen die Schutzbedürftigkeit der Daten (etwa bestimmte Gesundheitsdaten betreffend)[50] typisierend das Interesse an Senkung von Transaktionskosten im Geschäftsverkehr überwiegt. Im Übrigen spielt der klassische Freiheitsschutz gegenüber dem Staat auch in der Judikatur des Bundesverfassungsgerichts zur informationellen Selbstbestimmung eine zentrale Rolle,[51] worauf noch zurückzukommen sein wird.[52]

Im deutschen und teilweise wohl auch europäischen Denken verbindet sich der würdebasierte Ansatz ein Stück weit mit dem Gleichheitsgedanken.[53] Jeder besitzt die gleiche unverfügbare Würde und genießt dadurch tendenziell auch im Ergebnis das gleiche Persönlichkeitsschutzniveau, was wiederum Diskriminierungen in der »realen Welt« vorbeugen soll. Nach US-Vorstellungen gibt es zwar gleiche Ausgangsbedingungen, doch trägt dann jeder, zugespitzt formuliert, seine Daten freier »zu Markte«; in der Konsequenz differiert dann das Leistungsangebot im Privatrechtsverkehr stärker je nach individuellem, aus den verfügbaren Daten herausdestillierten Persönlichkeitsprofil. Dennoch bliebe es vor dem skizzierten Hintergrund zu unterkomplex, wenn man das deutsche (und partiell auch das europäische) Konzept als gleichheitsorientiert, das US-amerikanische Denken dagegen als freiheits- und wettbewerbsorientiert charakterisieren

48 Dies betonen etwa Hoffmann-Riem, Informationelle Selbstbestimmung in der Informationsgesellschaft, AöR 123 (1998), 513, 527 ff.; Masing (Fn. 28), NJW 2012, 2305, 2307.

49 Weichert, Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, NJW 2001, 1463, 1464 ff.

50 Beispiele bei Schwartz (Fn. 7), 126 Harv. L. Rev. 1966, 1974 f. (2013); zum Datenschutz im Gesundheitswesen und den notwendigen Veränderungen angesichts von „Big Data“ Terry, Protecting Patient Privacy in the Age of Big Data, 81 UMKC L. Rev. 385 (2012-2013).

51 Deshalb den scharfen Gegensatz zwischen Würde- und Freiheitsansatz verwerfend Simitis (Fn. 5), 98 Cal. L. Rev. 1989, 1993 (2010).

52 Siehe sogleich unter III. 2.

53 Dies klingt an auch bei Strahilevitz, Towards a Positive Theory of Privacy Law, 126 Harv. L. Rev. 2010, 2034 (2013); auf die EMRK bezogen Diggelmann (Fn. 37 ), VVDStRL 70 (2011), 50, 69 f.

wollte. Denn die Ökonomisierung der Datennutzung bricht sich auch in Deutschland immer mehr Bahn,[54] während die USA sektorspezifisch auch weiterreichenden Schutz gewähren und dazu Marktmechanismen einschränken. In Deutschland nehmen vor allem über das Internet personalisierte Werbung und Leistungsangebote zu, während in den USA bestimmte Differenzierungskriterien (namentlich »*race*« und »*gender*«) auch im Zuge von *Big Data* verbreitet kritisch gesehen werden.[55] Ähnliche Bedenken werden gegenüber den Daten-Analysemöglichkeiten laut, die künftige intelligente Energienetze und -zähler (*Smart Grids* mit *Smart Meters*) ermöglichen sollen.[56] Die dabei im Vergleich zur sonstigen IT-Nutzung erhöhte Sensibilität der US-Amerikaner mag nicht zuletzt dadurch zu erklären sein, dass die Energieverbrauchsdaten Rückschlüsse auf das Verhalten in der besonders geschützten räumlichen Privatsphäre (*home*) zulassen werden.

### 2. *Fundierung in einer umfassenden Werteordnung versus fragmentierter staatsfixierter Abwehrrechte in Anknüpfung an andere Grundrechtsverbürgungen*

Seit dem Lüth-Urteil[57] ist das deutsche Grundrechtsdenken bekanntlich wesentlich von einer objektiven Dimension der Grundrechte als Werteordnung mitgeprägt. Weniger pathetisch lässt sich von objektiv-rechtlichen

---

54 Weichert (Fn. 49), NJW 2001, 1463, 1464 f.; Buchner, Die Einwilligung im Datenschutzrecht – vom Rechtfertigungsgrund zum Kommerzialisierungsinstrument, DuD 2010, 39 ff.; entsprechende Marktmodelle befürwortend Nettesheim, Grundrechtsschutz der Privatheit, VVDStRL 70 (2011), 7, 41 u. 43, unter Verweis auf Zhan/Rajamani, The Economics of Privacy, International Journal of Security and its Applications Vol. 2 (2008), 101.

55 Vgl. Strahilevitz (Fn. 53), 126 Harv. L. Rev. 2010, 2019 (2013).

56 Statt vieler Eisen, Smart Regulation and Federalism for the Smart Grid, 37 Harv. L. Rev. 1, 16 (2013); McNeil, Privacy and the Modern Grid, 25 Harv. J. of L. Tech. 199 (2011); Balough, Privacy Implications of Smart Meters, 86 U. Chi-Kent L. Rev. 161 (2011). Public Utility Commissions mancher Einzelstaaten haben deshalb bereits Datenschutzregelungen getroffen, Eisen (dortige Fn. 93) verweist dazu für Kalifornien auf „Decision Adopting Rules to Protect the Privacy and Security of Electricity Usage Data, Cal. Pub. Util. Comm´n (July 29, 2011)".

57 BVerfGE 7, 198 (205 ff.); dazu kritisch Böckenförde, Grundrechte als Grundsatznormen, Der Staat 29 (1990), 1 ff.

Grundrechtsgehalten sprechen.[58] Für die Menschenwürde macht dies bereits der Verfassungstext in Art. 1 Abs. 1 S. 2 GG deutlich. Dementsprechend folgen aus der informationellen Selbstbestimmung über individuelle Abwehrrechte hinaus staatliche Schutzpflichten und Gewährleistungsaufträge.[59] Diese werden umso bedeutsamer, je mehr der Einzelne die Entscheidungsmacht im Umgang mit seinen Daten in komplexen technischen Systemen faktisch verliert und auf die Integrität dieser Systeme vertrauen muss; auf dieser Einsicht fußt das zur Online-Durchsuchung entwickelte sogenannte »Computer-Grundrecht«.[60] Im Schrifttum sprechen sich viele sogar für eine noch stärkere Abkehr von der abwehrrechtlichen Ausrichtung dieser Grundrechte zugunsten einer objektiv-rechtlichen Verpflichtung des Staates zur »organisations- und verfahrensrechtlichen Strukturierung des Umgangs mit personenbezogenen Daten und Informationen«[61] aus.[62] Staatliche Schutz- und Strukturierungspflichten erfassen nicht zuletzt auch das Privatrecht; es muss so ausgestaltet werden, dass materielle Selbstbestimmung im Umgang mit eigenen Daten selbst in Fällen massiven strukturellen Ungleichgewichts zwischen den Vertragspartnern[63] ge-

58 Kurzüberblick m.w.N. bei Dreier, in ders. (Hrsg.), GG-Kommentar, Bd. 1, 3. Aufl. 2013, Vorbem. Rn. 82; Jarass, Wirkungen der Grundrechte, in: Merten/Papier (Hrsg.) Handbuch der Grundrechte, Bd. II, 2006, § 38 Rn. 5 ff.; kritisch zum Begriff der „objektiv-rechtlichen Funktion der Grundrechte“ z.B. Schwabe, Probleme der Grundrechtsdogmatik, 1977, S. 286 ff.

59 Statt vieler im Überblick Rudolf, Recht auf informationelle Selbstbestimmung, in: Merten/Papier (Hrsg.), Handbuch der Grundrechte, Band IV, § 90 Rn. 25 ff; Britz, in: Hoffmann-Riem (Fn. 18), S. 561, 581 ff.

60 Siehe oben II mit Fn. 17; dazu auch Hoffmann-Riem, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, 1009, 1015 ff.

61 Britz, in: Hoffmann-Riem (Fn. 18), S. 561, 563.

62 Hoffmann-Riem (Fn. 48), AöR 123 (1998), 513, 522 ff., Ladeur, Datenschutz – vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken, DuD 2000, 12, 15 ff.; Albers, Umgang mit personenbezogenen Informationen und Daten, in Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg,), Grundlagen des Verwaltungsrechts, Band 2, 2. Aufl. 2012, § 22 Rn. 68.

63 Insoweit knüpft BVerfG (K), JZ 2007, 576 zu Recht an die – freilich umstrittene (vgl. einerseits Ruffert, Vorrang der Verfassung und Eigenständigkeit des Privatrechts, 2001, S. 342 ff.; andererseits Bumke, Ausgestaltung der Grundrechte, 2009, S. 57 ff.) – Rechtsprechung zur gestörten Vertragsparität (grundlegend BVerfGE 81, 242, 254 ff.; 89, 214, 231 ff.) an.

währleistet bleibt.[64] Dies trifft sich mit dem Gedanken des Verbraucherschutzes im einfachen Recht.[65] Der in die Datenweitergabe einwilligende Bürger ist zumindest dort schutzbedürftig, wo er auf eine bestimmte Vertragsbeziehung ökonomisch oder sozial mehr oder minder angewiesen ist. Nicht umsonst spielt deshalb der Datenschutz in sozialen Netzwerken (etwa Facebook) und gegen übermächtige Internet-Service Providern wie Google auch auf der europäischen Ebene in der Diskussion über die Datenschutz-Grundverordnung eine zentrale Rolle und prägt auch die Kontroverse um die Nachfolge für die vom EuGH aufgehobene *Safe-Harbor*-Vereinbarung mit den USA.[66] Vorhandene gesetzliche Regelungen sind in Deutschland nach der Lehre von der mittelbaren Drittwirkung im Lichte informationeller Selbstbestimmung auszulegen und anzuwenden.[67] Ob auch die Charta-Grundrechte eine solche mittelbare Drittwirkung entfalten sollen, hat man im Grundrechte-Konvent bewusst offen gelassen;[68] jedenfalls Schutzpflichten sind aber auch dem Unionsrecht (vor allem aus der Judikatur zu den Grundfreiheiten, aber auch zu den Grundrechten[69]) vertraut.

---

64 Vgl. Bäcker, Grundrechtlicher Informationsschutz gegen Private, Der Staat 51 (2012), 91, 99 ff., insb. 105 ff; Albers, Informationelle Selbstbestimmung, 2005, S. 562 ff.

65 Dazu näher unten III. 4.

66 Pötters, Primärrechtliche Vorgaben für eine Reform des Datenschutzrechts, RDV 2015, 10 ff.; auch im damaligen Entwurf zur Datenschutz-Grundverordnung ein Schutzdefizit im Hinblick auf Profilbildung durch *Big Data* ausmachend Maas, EU-Datenschutz-Grundverordnung: Datensouveränität in der digitalen Gesellschaft, DuD 2015, 579 f.; vgl. auch Wittmann, Der Schutz der Privatsphäre (Fn. 19), S. 38 f.; Determann (Fn. 8), NVwZ 2016, 561 ff.; zum *Safe-Harbor*-Abkommen s. EuGH v. 6.10.2015, Rs. C-362/14; zur Kontroverse vgl. Borges, Datentransfer in die USA nach Safe Harbor, NJW 2015, 3617, 3619 f.

67 Vgl. Masing (Fn. 28), NJW 2012, 2305, 2308.

68 Borowsky, in: Meyer (Fn. 30), Art. 51 Rn. 31; Hatje, in: Schwarze/Becker/Hatje/Schoo (Hrsg.), EU-Kommentar, 3. Aufl. 2012, Art. 51 GRC Rn. 22.; Perner, Grundfreiheiten, Grundrechte und Privatrecht, 2013, sieht in EuGH v. 1.3.2011, Rs. C-236/09/09 (Tst-Achats) eine implizite Anerkennung der mittelbaren Drittwirkung, doch wird der Begriff dort nicht erwähnt, es ist nur von Schutzpflichten die Rede.

69 Aus deutscher Perspektive Ehlers, Allgemeine Lehren der Grundfreiheiten, in: ders. (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 4. Aufl. 2014, § 7 Rn. 38; für die europäischen Grundrechte etwas zurückhaltender ders., Allgemeine Lehren der Unionsgrundrechte, a.a.O., § 14 Rn. 35.

Solche objektiv-rechtlichen Grundrechtsdimensionen sind dagegen in den USA nahezu[70] unbekannt, es geht ausschließlich um die Abwehr staatlicher Eingriffe.[71] Dementsprechend bleibt auch *Informational Privacy* ausschließlich staatsgerichtet und ist im Übrigen selbst insoweit wie schon beschrieben nicht flächendeckend grundrechtlich garantiert, sondern nur in Anknüpfung an andere rechtsstaatliche und grundrechtliche Garantien.[72] Soweit der *Supreme Court* darüber hinaus ein allgemeineres Grundrecht auf *Informational Privacy* angedacht hat, so würde dies zwar die Regierung auch als Auftrag- oder Arbeitgeber erfassen,[73] trotz gelegentlich angedeuteter Parallelen[74] aber nicht Arbeitsverhältnisse im privaten Sektor. Konzepte eines *Informational Due Process* suchen die allgemeinen staatsgerichteten *Due Process*-Verfahrensgarantien im Hinblick auf besondere Gefahren automatisierten Verwaltungshandelns[75] weiterzuentwickeln, wenn auch gelegentlich darauf hingewiesen wird, dass insoweit eine individualistische Sichtweise nicht ausreicht.[76] Rechtsverhältnisse zwischen Privaten erfassen auch diese Konzepte nicht.

Sofern in den USA ein Schutz gegen den Staat besteht, mögen die Ergebnisse im Einzelfall gar nicht so weit von denen in Deutschland abweichen, wo der Gesetzesvorbehalt durchaus erhebliche Einschränkungen der Freiheit namentlich aus Gründen der inneren Sicherheit zulässt. Die Risiken von Persönlichkeitsprofilen, die das Bundesverfassungsgericht mehrfach betont hat,[77] haben auch schon den *Supreme Court* (anlässlich der

70 Vgl. allerdings Strahilewitz (Fn. 8), 98 Cal. L. Rev. 2007, 2048 (2010), wonach als „zweitbeste Lösung" (primär plädiert er für die Aufgabe des *Constitutional Right to Informational Privacy Experiment*) eine verfassungsrechtliche Lückenfüllung des *Tort Law* zu erwägen sei.

71 Lange, Grundrechtsbindung des Gesetzgebers – Eine rechtsvergleichende Studie zu Deutschland, Frankreich und den USA, 2010, S. 314 ff., 416 ff., 431 f.

72 Namentlich des „*home*" usw. gegen „*search*"; näher oben II. mit insb. Fn. 25.

73 NASA v. Nelson, 562 U.S. 134 (2011), S. 138 u. 148 f.

74 Siehe unten Fn. 90.

75 Dort vor allem die Risiken unterkomplexer und fehlerhafter Programmierung, etwa bei der Administrierung von Sozialleistungen oder dem *„No Flight"*-Programm für terrorverdächtige Personen betreffend; dazu eingehend Citron, Technological Due Process, 85 Wash. U. L. Rev. 1249, 1305 ff. (2008).

76 Cohen, What Privacy Is For, 126 Harv. L. Rev. 1904, 1931 f. (2013).

77 BVerfGE 65, 1, 42 – Volkszählung; E 115, 166, 189 f. und 192 f. – Telekommunikationsüberwachung; E 120, 378, 404 ff. – KfZ-Kennzeichenerkennung; E 125, 260, 319/328 und 333 f. – Vorratsdatenspeicherung.

Auswertung von Smartphones Verhafteter)[78] und US-Instanzgerichte[79] beschäftigt. Und die faktische Erosion des Schutzes im Zeichen (behaupteter) Terror-Prävention ist nicht allein der NSA, sondern (in wohl etwas geringerem Umfang) auch deutschen Geheimdiensten anzulasten.[80] Die konzeptionellen Grundlagen von *Informational Privacy* gegenüber dem Staat bleiben jedoch in wesentlichen Punkten unterschiedlich. Neben der Menschenwürde bildet dabei der demokratische Aspekt das zweite Fundament der grundgesetzlichen Gewährleistungen informationeller Selbstbestimmung und der Integrität informationstechnischer Systeme. Wie bereits im Volkszählungsurteil betont, kann die Angst vor (staatlicher) Überwachung zu gesellschaftlich-politischer Einschüchterung führen.[81] In der US-Rechtsprechung spielt dieser demokratische Aspekt kaum eine Rolle,[82] ebensowenig wie der Menschenwürde-Ansatz. Während bei der Redefreiheit die Argumentation mit einem drohenden *chilling effect* weit verbreitet ist,[83] sucht man Vergleichbares im Kontext von *Informational Privacy* weitgehend vergeblich.

---

78 Riley v. California, No. 13-132 (2014).

79 Besonders United States v. Maynard, 615 F 3 d 544, 562 (D.C. Cir. 2010), dort die vierwöchige lückenlose GPS-Überwachung eines Verdächtigen ohne Durchsuchungsanordnung (*search*) betreffend; dazu näher Strahilewitz (Fn. 8), 98 Cal. L. Rev. 2007, 2038 ff. (2010); unter Hinweis auf die neuen Entwicklungen (*„turmoil"*) in der Rechtsprechung des Supreme Court zur digitalen Überwachung Zweifel an der Verfassungsmäßigkeit des *bulk telephone metadata program* der *NSA* äußernd, doch mangels Entscheidungserheblichkeit darüber nicht abschließend entscheidend U.S. Court of Appeals for the Second Circuit, ACLU v. Clapper, Docket No. 14-42-cv (7. Mai 2015), abrufbar unter: http://www.ca2.uscourts.gov/decisions/isysquery/5c81be63-c2ed-4c0e-9707-6bff831b4aba/1/doc/14-42_complete_opn.pdf (Stand: 25. August 2015), S. 82 ff.

80 Vgl. Bäcker, Erhebung, Bevorratung und Übermittlung von Telekommunikationsdaten des Bundes, Stellungnahme im NSA-Untersuchungsausschuss, 2014, www.bundestag.de/blob/280844/35ec929cf03c4f60bc70c8e404c5cc/mat_a_sv-2-3-pdf-data.pdf (Stand 28.5.2015); ders., Der BND baut sich einen rechtsfreien Raum: Erkenntnisse aus dem NSA-Untersuchungsausschuss, Verfassungsblog v. 19.1.2015, www.verfassungsblog.de (Stand 28.5.2015).

81 Grundlegend BVerfGE 65, 1, 43; für übersteigert hält diese Sorge Bull, Grundsatzentscheidungen zum Datenschutz im Bereich der inneren Sicherheit, in: van Ooyen/Möllers (Hrsg.), Handbuch Bundesverfassungsgericht im politischen Prozess, 2. Aufl. 2015, S. 627, 641 ff.

82 Anders aber in Teilen des Schrifttums, siehe etwa Slobogin (Fn. 24), Die Verwaltung 44 (2011), 465, 482.

83 Dombrowski v. Pfister, 380 U.S. 479, 487 ff. (1965), zuletzt Citizens United v. Federal Election Community, 558 U.S. 310, 326 f. und 329 ff. (2010).

Selbst beim Datenschutz im Internet-Privatrechtsverkehr erscheint es freilich nicht ausgeschlossen, dass sich die Gegensätze in ihren praktischen Auswirkungen künftig ein Stück weit abschwächen werden. Auf europäischer Ebene war es in der Diskussion um die Datenschutz-Grundverordnung umstritten, inwieweit für große Internet-Unternehmen Datenverarbeitungshürden errichtet werden sollen; Freihandel und Wirtschaftsförderung konkurrieren auch hier mit dem Datenschutz.[84] Art. 16 Abs. 2 AEUV macht schon im Wortlaut den engen Zusammenhang zwischen Datenschutz und freiem Datenverkehr deutlich.[85] Das deutsche Konzept der mittelbaren Drittwirkung von Grundrechten ist längst nicht überall in Europa in gleichem Maße verbreitet und ist im Übrigen bei der informationellen Selbstbestimmung bislang nur recht selten und wenig prominent[86] gerichtspraktisch geworden; das Bundesverfassungsgericht hat sich noch nie näher mit einem Fall des (Internet-)Datenschutzes im Privatrechtsverkehr beschäftigt.[87] Auch in Deutschland ist man sich darüber einig, dass wesentliche Elemente des Datenschutzes gegen den Staat wie namentlich der Gesetzesvorbehalt für den Privatrechtsverkehr nicht passen; dort bleibt die freie Entfaltung durch Kommunikation einschließlich Datensammlung und -weitergabe der Normalfall, wobei dem Gesetzgeber allerdings der Ausgleich von Freiheitsphären obliegt.[88] Umgekehrt wird auch in den USA vermehrt erkannt (wenn es auch die Praxis noch nicht erreicht hat), dass sich staatlicher und privater Bereich beim Internet-Datenschutz nicht voll trennen lassen. Denn bekanntermaßen greifen Geheimdienste wie die NSA auch (in freilich ungeklärtem Ausmaß) auf Daten zu, die Firmen wie

84 Schwartz (Fn. 5), 126 Harv. L. Rev. 1966, 1987 ff. (2013).

85 Darauf weist etwa Schneider (Fn. 27), Die Verwaltung 44 (2011), 499, 502 hin.

86 Vgl. aber zur informationellen Selbstbestimmung im Privatrechtsverkehr für die reale Welt (auf den Mietvertrag eines Entmündigten bezogen) BVerfGE 84, 192, 194 ff.; auf eine versicherungsvertragliche Obliegenheit zur Entbindung von der Schweigepflicht bezogen BVerfG (K), JZ 2007, 576, dazu Bäcker (Fn. 64), Der Staat 51 (2012), 91, 107; die Veröffentlichung rechtswidrig erlangter E-Mails durch die Presse betreffend jüngst BGH, JZ 2015, 303, 304 f., freilich ohne zu erwähnen, dass es im Rahmen des behaupteten Unterlassungsanspruchs (§§ 1004, 823 BGB) um eine Drittwirkungskonstellation ging.

87 Albers, in: GVwR II (Fn. 62), § 22 Rn. 67 unter Verweis auf BVerfG (K), NJW 2000, 2413, 2414, obwohl die Vorinstanzen das Recht auf informationelle Selbstbestimmung thematisiert hatten, vgl. BGH JZ 1995, 253 f.; vgl. auch Masing (Fn. 28), NJW 2012, 2305, 2306.

88 Dies betonen zu Recht Masing (Fn. 28), NJW 2012, 2305, 2307; Bäcker (Fn. 64), Der Staat 51 (2012), 91, 100.

Facebook und Microsoft im Privatrechtsverhältnis gespeichert haben.[89] Auf einfachgesetzlicher Ebene erfasst der *Privacy Act* zwar nur (Bundes-)Behörden; in einem neueren Fall, der die Sammlung personenbezogener Informationen bei der Einstellung in den öffentlichen Dienst betraf, hat der *Supreme Court* aber immerhin Parallelen zum privaten Arbeitsverhältnis gezogen – allerdings um die weitreichende Datenerhebung einschließlich der Befragung Dritter zu rechtfertigen.[90] Im Übrigen bleibt abzuwarten, inwieweit die Verhaltensökonomik oder andere Ansätze die ökonomische Analyse des Rechts in den USA revolutionieren und dadurch auch die Notwendigkeit eines Verbraucherschutzes stärker ins Bewusstsein heben können. Darauf ist noch zurückzukommen.[91]

### 3. *Flächendeckende Vorsorge gegen Persönlichkeitsgefährdungen versus bereichsspezifische Schadensvermeidung*

Das deutsche Recht sucht die Persönlichkeitsentfaltung bereits im »Vorfeld konkreter Bedrohungen benennbarer Rechtsgüter«[92] strukturell dadurch zu sichern, dass dem Einzelnen ein umfassender Schutz informationeller Selbstbestimmung zuteilwird. Dieser Vorfeldschutz[93] ist gerade nicht auf besonders sensible Daten beschränkt; das Bundesverfassungsgericht hat betont, dass es in Zeiten automatischer Datenverarbeitung und nahezu unbegrenzter Verknüpfungsmöglichkeiten keine von vornherein »belanglosen« Daten mehr gäbe.[94] Ebenso schützt Art. 8 GrCh alle personenbezogenen Daten unabhängig davon, inwieweit sie prima facie als sen-

89 Dazu ausführlich Greenwald, Die globale Überwachung, 2014, S. 151 ff.; aufgegriffen etwa von Heidebach, Die NSA-Affäre in Deutschland – Stößt der Grundrechtsschutz an seine Grenzen?, DÖV 2015, 592, 593.

90 NASA v. Nelson, 562 U.S. 134 (2011), 149.

91 Siehe dazu unten IV.

92 BVerfGE 118, 168, 184 – Kontostammdaten; E 120, 274, 312 – Online Durchsuchung; E 120, 351, 360 – steuerliche Auslandsbeziehungen; ähnlich E 120, 378, 397 – Kfz-Kennzeichenerfassung.

93 Britz, in: Hoffmann-Riem (Fn. 18), S. 561, 575, ähnlich Bäcker (Fn. 64), Der Staat 51 (2012), 91, 96; kritisch hervorgehoben von Nettesheim (Fn. 54), VVDStRL 70 (2011), 7, 26.

94 So schon BVerfGE 65, 1, 42 f. und 45 – Volkszählung; aufgegriffen etwa von BVerfGE 115, 320, 350 – Rasterfahndung.

sibel erscheinen.[95] Der Personenbezug wird dabei in Deutschland und Europa weit verstanden und schließt, anders als bislang in den USA,[96] auch bloße Telekommunikations-Verbindungsdaten mit ein.[97] Dies führt notwendig zu einem überschießenden Schutzgehalt, doch ist man prinzipiell bereit, dadurch erhöhte Transaktionskosten in Kauf zu nehmen, um ansonsten kaum mehr beherrschbare Persönlichkeitsgefährdungen möglichst schon im Ansatz auszuschließen. Dieses Vorsorgekonzept trifft sich mit dem allgemeinen Erstarken des Vorsorgegedankens, namentlich im Umweltrecht.[98] Im Grundsatz ist deshalb das deutsche wie europäische Datenschutzrecht bewusst allgemein gehalten mit ambitionierten Vorkehrungen wie dem Einwilligungserfordernis (Verbot mit Erlaubnisvorbehalt) und der Zweckbindung. Der Schutz von Vertraulichkeit und Integrität informationstechnischer Systeme wurde zwar zum Schutz vor Online-Durchsuchungen entwickelt, zielt aber darüber hinaus darauf ab, schon im Vorfeld Infiltrationen aller Art durch geeignete – insbesondere technische – Sicherungen zu erschweren.

Eine weitere Ebene der Vorsorge lässt sich schließlich darin erblicken, dass der Persönlichkeitsschutz selbst wiederum auch instrumentell verstanden wird: zum einen zugunsten nichtkonformistischer Formen der Persönlichkeitsentfaltung und damit gesellschaftlicher Pluralität, zum anderen als Demokratie-Voraussetzungsschutz, wenn es darum geht, innere und

---

95 Betont von Bernsdorff, in: Meyer (Fn. 30), Art. 8 Rn. 15; Jarass, Charta der Grundrechte der Europäischen Union, 2. Aufl. 2013, Art. 8 Rn. 6.

96 Grundlegend Smith v. Maryland, 442 U.S. 735, 744 (1979); dazu Wittmann, Der Schutz der Privatsphäre (Fn. 1919), S. 196 ff., vgl. auch S. 798 mit dortiger Fn. 3887; Gärditz/Stuckenberg, Vorratsdatenspeicherung à la americaine, JZ 2014, 209 f.; wohl erstmals anders (unter Bezug auf die „relevance") allerdings nun in Auslegung des Patriot Act U.S. Court of Appeals for the Second Circuit, ACLU v. Clapper, Docket No. 14-42-cv (7. Mai 2015), http://www.ca2.uscourts.gov/decisions/isysquery/5c81be63-c2ed-4c0e-9707-6bff831b4aba/1/doc/14-42_complete_opn.pdf (Stand: 25. August 2015), S. 82 ff.

97 BVerfGE 115, 166, 189 f. – Telekommunikationsüberwachung; E 125, 260, 309 – Vorratsdatenspeicherung; der EuGH hat in seiner Entscheidung zur Vorratsdatenspeicherung dazu nicht ausdrücklich Stellung genommen, vgl. EuGH, Urt. v. 8.4.2014, Rs. 293/12, EuZW 2014, 459, Rn. 26 f. u. 36.

98 Siehe Hoppe, Staatsaufgabe Umweltschutz, VVDStRL 38 (1980), S. 211 ff.; Kloepfer, Umweltrecht, 3. Aufl. 2004, § 4 Rn. 8 ff.; zum Unionsrecht Marti, Das Vorsorgeprinzip im Umweltrecht – Am Beispiel der internationalen, europäischen und schweizerischen Rechtsordnung, 2011, S. 105 ff.; das Vorsorgeprinzip als vom Umweltschutz losgelöstes allgemeines Rechtsprinzip ablehnend Arndt, Das Vorsorgeprinzip im Unionsrecht, 2009, insb. S. 131 ff.

äußere Entscheidungsfreiheit zu sichern, unbefangenes Verhalten zu ermöglichen sowie einem Klima der – dann auch politischen – Einschüchterung vorzubeugen.[99] Die formelle informationelle Selbstbestimmung hat letztlich keinen besonderen Eigenwert, sondern soll materielle Selbstbestimmung des Einzelnen auch in der digitalen Welt möglich machen.

Dagegen stehen die USA auch in anderen Bereichen, namentlich im Umweltrecht, einem Vorsorgeprinzip tendenziell sehr kritisch gegenüber, weil sie in dessen überschießender Tendenz Effizienzverluste erblicken.[100] Dies dürfte ein Grund dafür sein, dass man den Schutz von *Informational Privacy* möglichst passgenau auf besonders sensible Daten und typische abstrakte Gefährdungen, bei denen ein Schaden hinreichend wahrscheinlich erscheint,[101] zu beschränken sucht, sei es im *Tort Law* oder durch Spezialgesetze. Bei der Einschätzung des Gefahrenpotentials von *Privacy*-Verlusten stehen die unmittelbaren Konsequenzen der Datennutzung für den Einzelnen ganz im Vordergrund. Zwar blendet man die gesellschaftlichen und politischen Folgen von *Big Data* keineswegs aus. Doch werden meist eher die Chancen durch verbesserte Informationen betont[102] als etwaige Risiken des »gläsernen Menschen«. Dies mag auch mit größerer Technik-Faszination und mehr Zukunftsoptimismus zusammenhängen, was gemeinhin den US-Amerikanern gegenüber Deutschen nachsagt wird.

Wie alle zuvor beschriebenen (Kultur-)Unterschiede beim Daten- und *Privacy*-Schutz darf freilich auch diese Differenz nicht überzeichnet werden. Teilweise schon bei der Bestimmung der Eingriffsschwelle[103] und spätestens bei Verhältnismäßigkeitsabwägungen müssen auch das deutsche und das europäische Datenschutzrecht nach dem jeweiligen Gefährdungspotential der Datenverarbeitung abstufen und dabei das jeweilige

---

99 Dazu bereits oben III. 2. mit Fn. 81.

100 Besonders prominent Sunstein, Laws of Fear, 2005, insb. S. 13 ff. m.w.N.

101 Vgl. Strahilevitz (Fn. 53), 126 Harv. L. Rev. 2010, 2036 mit dortiger Fn. 117 (2013): „The American approach does have advantages over the European approach in directing government resources at real privacy threats rather than hypothetical ones."

102 Siehe auch schon oben III. 1. sowie unten III. 4. mit Nachweisen in Fn. 112.

103 Nach ständiger Rspr. (erstmals BVerfGE 100, 313, 366, zuletzt E 120, 378, 399, daran anknüpfend zuletzt einen Eingriff durch automatisierte Kennzeichenerfassung verneinend BVerwG, NVwZ 2015, 906, Rn. 27) „begründen Datenerfassungen keinen Gefährdungstatbestand", soweit Daten unmittelbar nach der Erfassung technisch wieder spurenlos, anonym und ohne die Möglichkeit, einen Personenbezug herzustellen, ausgesondert werden."

Gewicht kollidierender Interessen am Informationsfluss berücksichtigen.[104] So sehr informationelle Selbstbestimmung konzeptionell zu einem umfassenden Schutz der informatorischen Voraussetzungen individueller Persönlichkeitsentfaltung tendiert, so sehr muss sie sich letztlich doch in spezifischen Gefährdungslagen bewähren. Dementsprechend hat das Verfassungsgericht in der Grundrechtsprüfung immer viel Wert darauf gelegt herauszuarbeiten, worin die besondere Gefährlichkeit der geprüften Informationsmaßnahmen liegt.[105] Umgekehrt hat kürzlich der *Supreme Court* in seiner Entscheidung über die Auswertung eines Smartphones bei einem Verhafteten auch die potentiellen Gefahren angesprochen, die über den Durchsuchungs-Einzelfall hinaus aus der Ermöglichung von Persönlichkeitsprofilen resultieren können.[106]

### *4. Verbraucherschutz und Grenzen des Homo Oeconomicus versus Informational Capitalism*

In Deutschland herrschte lange Zeit ein eher paternalistisches Verständnis von Verbraucherschutz als sozialstaatliche Aufgabe vor.[107] Zwar gewinnt, ausgehend von der europäischen Ebene, mittlerweile das Leitbild des mündigen Verbrauchers an Boden,[108] der, wird er nur hinreichend informiert, seine Interessen selbst wahren kann. Doch bleibt man mit guten Gründen verbreitet skeptisch gegenüber der Vorstellung eines Homo Oeconomicus, der stets rational seine wirtschaftlichen Eigeninteressen maximieren will und kann. Man sieht im Verhältnis des Kunden zum *Big Business* auch beim Umgang mit den persönlichen Daten oftmals eine mehr oder minder starke Störung der Vertragsparität. Damit verbunden gewinnt Datenschutz politisch oft sogar eine konsumkritische Note; manchem erscheint mediale »Enthaltsamkeit« gar als einziger gangbarer Weg, um die übermäßige Weitergabe persönlicher Daten im Geschäftsverkehr einzu-

104 Gutes Anschauungsmaterial dazu z.B. zuletzt in BVerfGE 133, 277, 322 ff. – Antiterrordatei.

105 Hervorgehoben von Britz, in: Hoffmann-Riem (Fn. 18), S. 561, 578.

106 Riley v. California, No. 13-132 (2014), S. 19 ff.

107 Vgl. Hönn, Kompensation gestörter Vertragsparität, 1982, S. 280 ff., 306 ff.; ferner Ruffert, Vorrang der Verfassung (Fn. 63), S. 272 f.

108 Siehe etwa Pfeiffer, in: Grabitz/Hilf/Nettesheim (Hrsg.), Das Recht der EU, 56. EL 2015, Art. 169 Rn. 21 ff.; Mohr, Der Begriff des Verbrauchers, AcP 204 (2004), 660, 675.

dämmen. Die Bürger sollen, so lautet eine verbreitete Forderung, als Konsumenten die Praktiken der *global player* im Umgang mit ihren Daten kritischer hinterfragen und ihre Daten im Internet nicht auf dem Altar echter oder vermeintlicher besonderer Konsumprivilegien (»goldene Kundenkarte«, »*preferred customer*«) opfern. Verbraucherschutzorientiertes Recht der Datenerhebung und -verarbeitung will ein Stück weit paternalistisch die Menschen davor bewahren, sich zugunsten ihrer kurzfristigen Konsumenteninteressen einer erheblichen Sozialkontrolle zu unterwerfen und sich in Folge des dadurch ausgelösten Konformitätsdrucks langfristig die eigenen Spielräume bei der Persönlichkeitsentfaltung übermäßig zu verengen. Zur Erfüllung entsprechender staatlicher Schutzpflichten kommen technische Vorgaben und vor allem (gegebenenfalls gesetzlich auferlegte) Aufklärungspflichten der Internet-Anbieter in Betracht, der Staat kann sich aber auch edukatorisch an die Nutzer wenden.[109]

Demgegenüber sehen in den USA viele in einem nicht durch Datenschutz behinderten Informationsfluss die Voraussetzung für vertragliche Wohlfahrtsmaximierung im Wege eines *informational capitalism*[110]. Nur wenn die Vertragspartner möglichst viel übereinander wissen, können sie, so heißt es, ihre Präferenzen im Austausch rational bestmöglich verwirklichen. *Strahilevitz*, einer der profiliertesten Autoren in diesem Bereich, sieht unter Verweis auf empirische Untersuchungen *Big Data* und maximale Datenoffenheit gar als einzig wirksames Mittel gegen rassistische Diskriminierung, weil ohne personalisierte Informationen tendenziell immer zuerst bei Schwarzen mangelnde Zahlungsfähigkeit oder gar eine kriminelle Vergangenheit vermutet werde.[111] Aus Sicht der neoklassisch geprägten ökonomischen Analyse des Rechts wirkt Datenschutz daher typischerweise als Hemmschuh und Störfeuer.[112] Gerade wirtschaftlich wich-

---

109 Britz, in: Hoffmann-Riem (Fn. 18), S. 561, 592.

110 Begriff bei Cohen (Fn. 76), 126 Harv. L. Rev. 1904, 1925 (2013).

111 Strahilevitz (Fn. 53), 126 Harv. L. Rev. 2010, 2018 ff. (2013).

112 Posner (Fn. 41), 12 Georgia L. R., 393, 397 ff. (1978); ähnlich Stigler, An introduction to privacy in economics and politics, 9 Journal of Legal Studies, insb. 628-633 (1980); Calzolari/Pavan, On the optimality of privacy in sequential contracting, 130 Journal of Economic Theory, 168 ff. (2006); differenzierter Murphy (Fn. 41), 84 Georgetown L.J., 2381, 2385 ff., der sich Posners Auffassung hinsichtlich der mangelnden Schutzwürdigkeit bloßer Reputationsinteressen anschließt, aber einen gewissen Persönlichkeitsschutz auf der Basis subjektiver individueller Präferenzen für erwägenswert hält; vgl. auch Strahilevitz (Fn. 53), 126 Harv. L. Rev. 2010, 2027 ff. (2013): Datenschutz verhindere optimal auf die

tige Innovationen seien auf ein Maximum an verfügbaren Informationen angewiesen. Angesichts des verbreiteten Konsumverhaltens stufen viele das bloße Sammeln und Speichern von personenbezogenen Daten, vor allem durch Unternehmen, noch als gänzlich ungefährlich und damit unbedenklich ein und wollen Restriktionen erst bei gezielten (staatlichen) Zugriffen auf Daten Einzelner aus diesem Datenpool greifen lassen.[113] *Big Data* erscheint in diesem Licht erneut vor allem als Chance, nicht als Risiko. Dies vernachlässigt allerdings negative externe (also über die jeweilige einzelne Vertragsbeziehung hinausweisende) Effekte für die Gesellschaft. Nur wenige Kritiker[114] weisen in den USA darauf hin, dass Kreativität und damit auch wirtschaftliche Innovationskraft Freiräume zum unbefangenen »Spielen« benötigen und daher in einem Klima der erlebten Überwachung[115] und individuell gefilterten Informationen im Internet schwer wird gedeihen können.

Dennoch griffe eine Gegenüberstellung von »(europäischem) Bürger und (amerikanischen) Bourgeois«[116] viel zu kurz. Im US-amerikanischen (markt)liberalen Menschenbild wird gerade der ungehinderte Informationsfluss als Voraussetzung informierter Entscheidungen selbstbewusster Bürger gesehen, nicht nur in der Wirtschaft, sondern auch in der Politik. Und in Deutschland ist freier Informationsfluss im staatlich-politischen Bereich unter dem Stichwort »Transparenz« ebenfalls mehr und mehr positiv besetzt und wird durch die Informationsfreiheitsgesetze akzentuiert; hier suchen die neuere Gesetzgebung und teilweise auch die Rechtsprechung mittlerweile eher die Ausnahmen vom Informationsanspruch zum Zwecke des Datenschutzes sowie zum Schutz von Betriebs- und Ge-

---

individuelle Zahlungsbereitschaft zugeschnittene Vertragsangebote, kluge Kunden böte ein freier Datenfluss zudem die Möglichkeit, ihr Verhalten strategisch entsprechend auszurichten.

113 Dazu kritisch Geminn/Roßnagel (Fn. ) JZ 2015, 703, 707, unter Verweis auf Rubinfeld, Wahington Post v. 13.1.2014: „Today, most of us allow a great deal of our lives could be monitored or recorded. […] The key question isn´t how to keep information about us getting out into the world; it´s how that information can be used."

114 Cohen (Fn. 76), 126 Harv. L. Rev. 1904, 1918 ff. (2013).

115 Zur Disziplinierung („Internalisierung der Machtverhältnisse") durch Überwachung („Sichtbarkeit") intellektuell einflussreich, Foucault, Überwachen und Strafen, stw 1977, insb. S. 260.

116 In begrifflicher Anlehnung an Smend, Bürger und Bourgeois im deutschen Staatsrecht (1933), in: ders., Staatsrechtliche Abhandlungen, 3. Aufl. 1994, S. 309.

schäftsgeheimnissen mittelbar betroffener Privater enger einzugrenzen.[117] Konflikte zwischen freiem Dokumentenzugang und Datenschutz beschäftigten mehrfach auch schon den Europäischen Gerichtshof, der dabei betonte, dass ein verhältnismäßiger Ausgleich anzustreben sei.[118] Geht es um die Aufklärung politischer Missstände durch die Medien, kann auch unter dem Grundgesetz die Medienfreiheit das Recht auf informationelle Selbstbestimmung und das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme überwiegen.[119] Für die Datennutzung lassen sich auf europäischer Ebene und in Deutschland vermehrt Tendenzen beobachten, den im Ausgangspunkt strengen Zweckbindungsgrundsatz zu bloßer Zweckvereinbarkeit abzuschwächen; ein risikobasierter Ansatz will stärker danach abstufen, welches konkrete (Schadens-)Risiko der jeweilige Datenverarbeitungsvorgang in sich birgt.[120] Damit würde auch der Grundsatz der Datensparsamkeit, in dem sich das Vorsorgeprinzip besonders deutlich widerspiegelt, zugunsten von mehr *Big Data*-Freiräumen aufge-

---

117 Vgl. Gurlitt, Das Informationsverwaltungsrecht im Spiegel der Rechtsprechung, Die Verwaltung 44 (2011), 75 (95 ff.); allgemein zur Abwägung zwischen Informationszugangsinteressen und Datenschutzbelangen (§ 5 IFG) und zum im Bundesrecht sehr weitgehenden Schutz von Geschäftsgeheimnissen (§ 6 IFG) Schoch, IFG, Kommentar, 2009, Vorbem. §§ 3 bis 6 Rn. 14 ff., § 5 Rn. 7, 28 ff. und § 6 Rn. 11, 40, wobei er immerhin dafür plädiert, rechtswidriges Verhalten nicht als durch Betriebs- oder Geschäftsgeheimnis geschützt anzuerkennen; zum demgegenüber deutlich weiterreichenden Hamburger Informationszugangsrecht Schnabel, Das neue Hamburger Transparenzgesetz – Informationsregister, Datenschutz und Betriebs- und Geschäftsgeheimnisse, NordÖR 2012, 431, 434 f.; vgl. auch VG Hamburg v. 5.8.2015, 17 K 3203/13, Rn. 38 ff. (juris); zum Gebot einer restriktiven Auslegung der Ausnahmen vom Informationszugangsanspruch auch im Bundesrecht BVerwGE 150, 383, Rn. 24; BVerwG v. 15.11.2012 – 7 C 1.12 – Buchholz 404 IFG Nr. 10 Rn. 39.

118 Besonders EuGH, Rs. C-92/09 u.a. (Schecke), EuZW 2010, 929, Rn. 85; vgl. EuGH, Rs. C-28/08 (Bavarian Lager), EuZW 2010, 617, Rn. 59 ff; zum Ganzen Schneider (Fn. 27), Die Verwaltung 44 (2011), 499, 513 ff.

119 Zuletzt BGH, JZ 2015, 303, 304 ff. mit kritischer Anm. Ladeur.

120 Besonders deutlich Veil, DS-GVO: Risikobasierter Ansatz statt rigidem Verbotsprinzip – Eine erste Bestandsaufnahme, ZD 2015, 347 ff.; mit Recht kritisch aber etwa Article 29 Data Protection Working Group, Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EI, 14/EN WP 221, adopted on 16 September 2014,
http://ec.europa.eu/justice/data-protection/index_en.htm (Stand 21.9.2015).

geben.[121] Beim Verbraucherschutz sind ebenfalls Annäherungen zu beobachten. Denn im Wirtschaftsverkehr wenden sich Europa und Deutschland stärker dem Leitbild eines mündigen Verbrauchers zu, während in den USA ein libertärer Paternalismus[122] an Einfluss gewinnt. Wie schon erwähnt darf schließlich informationelle Selbstbestimmung auch in Deutschland nicht mit Abschottung des Individuums gleichgesetzt werden, sondern zielt gerade umgekehrt auf selbstbestimmte Teilhabe an Kommunikationsprozessen auch beim (Internet-)Konsum.[123]

### *IV. Auf der Suche nach pragmatischen Schnittstellen*

Bei allen Unterschieden zwischen den *Privacy*-Kulturen diesseits und jenseits des Atlantiks finden sich immerhin gewisse Überschneidungen, an die künftige Übereinkommen zur Ermöglichung des Datenflusses anknüpfen könnten. Dass über konzeptionelle Grundlagen Dissens besteht, schließt nicht von vornherein aus, in Teilbereichen pragmatische Verständigungen zu erzielen.[124]

Vor allem das Erfordernis von Information über und Einwilligung in die Datennutzung oder jedenfalls deren widerspruchslose Hinnahme spielt im Privatrechtsverkehr sowohl in Deutschland[125] und Europa als auch in den USA eine wichtige Rolle. Trotz unterschiedlicher Grundmodelle – Verbot mit Erlaubnisvorbehalt versus Widerspruchsoption – wird um die

---

121 Demgegenüber zu Recht stärker auf die anerkannten Lösungen durch Einwilligung und Transparenz und vor allem Anonymisierung des Datenaufkommens hinweisend Ohrtmann/Schwiering, Big Data und Datenschutz – Rechtliche Herausforderungen und Lösungsansätze, NJW 2014, 3984 ff.

122 Im Sinne von Sunstein/Thaler, Libertarian Paternalism is not an Oxymoron, 70 U. Chi. L. Rev. 1159 ff. (2003); teilweise ähnlich Camerer et al., Regulation for Conservatives: Behavioral Economics and the Case for „Asymmetric Paternalism", 151 U. Pa. L. Rev. (2003), S. 1211 ff.; vgl. auch Sunstein/Thaler, Nudge: Wie man kluge Entscheidungen anstößt, 2009, S. 14 ff.

123 Dies haben die Kritiker eines eigentumsähnlichen (Miss-)Verständnisses des Datenschutz-Grundrechts immer wieder betont; siehe oben III. 1. mit Fn. 45, vgl. auch Fn. 48.

124 Wie dies rechtlich umgesetzt werden könnte – etwa wie bisher in *Safe Harbour Rules*, *Model Contractual Clauses, Bind Corporate Rules* –, ist nicht Gegenstand dieses Beitrags; dazu im Überblick aus amerikanischer Perspektive Schwartz (Fn. 7), 126 Harv. L. Rev. 1966, 1980 ff. (2013). Zum *Safe-Harbor* Urteil s. Fn. 66.

125 Statt vieler Masing (Fn. 28), NJW 2012, 2305, 2308 f.

richtigen technischen Privatheits-Standardeinstellungen (*default rule)* im Internet (*opting-in* oder *opting-out*[126]) auf beiden Seiten des Atlantiks gestritten.[127] Gerade hier könnte die Verhaltensökonomik, welche die Grenzen rational-informierter Entscheidungen allgemein und speziell auch im Umgang mit den eigenen Daten im Internet aufzeigt, als Brücke dienen. Sie vermag zum einen auch in den USA das Bewusstsein dafür zu schärfen, welch großen Unterschied ein substanzielles – d.h. kein mangels Alternativen rein formales[128] – Einwilligungserfordernis gegenüber einem bloßen Widerspruchsrecht macht. Zum anderen bietet die Verhaltensökonomik mit ihrer Betonung der Kontext-Abhängigkeit menschlichen Verhaltens (*framing effects*[129]) zumindest gewisse Erklärungen – wenngleich keine Lösungen – für die Tatsache, dass der Schutz der Privatsphäre zwar von vielen abstrakt als wichtig bezeichnet wird, aber daraus kaum Konsequenzen beim realen Verhalten resultieren, selbst wenn ausnahmsweise die Transaktionskosten des Schutzes[130] (etwa vor *Cookies*) gering bleiben.[131]

---

126 Beispielsweise wurde in den USA im „Driver´s Privacy Protection Act" die Offenlegung entsprechender Informationen durch Public Law 106-69, 113 Stat. 986 von einer Widerspruchs- auf eine Einwilligungslösung umgestellt, dazu aus der Föderalismusperspektive Reno v. Condon 528 U.S. 141 (2000); für Deutschland vgl. etwa BGHZ 177, 253 ff.; BGH NJW 2010, 864; Wiesener, Datenschutzrechtliche Einwilligung zur Werbung: Opt Out ausreichend?, DuD 2007, 604 ff.; Buchner (Fn. 54), DuD 2010, 39, 41 ff.

127 Vgl. Determann (Fn. 8), NVwZ 2016, 561, 562 f. mit Hinweis auch auf deutliche Vollzugsdefizite. Bezeichnenderweise befürworten einflussreiche US-Wissenschaftler auch insoweit wiederum eine auf *Big Data*-Analysen gestützte personalisierte *Default Rule*, siehe Sunstein, Deciding By Default, 162 U. Pa. L. Rev. 1, 13 ff. u. 48 ff. (2013); vgl. auch Porat/Strahilevitz, Personalizing Default Rules and Disclosure of Data, 112 Mich. L. Rev. 1417 ff. (2014).

128 Wie oftmals im Internet; dazu aus den USA besonders klar Schwarz/Solove, Reworking Information Privacy Law (Fn. 7), S. 31 ff.

129 John/Acquisti/Loewenstein, Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information, 37 J. of Consumer Research. 858, 859 f. (2011).

130 Zu Möglichkeiten und Grenzen, die Transaktionskosten der Einwilligung durch technische Lösungen zu senken, siehe Roßnagel, Datenschutz in einem informatisierten Alltag, 2007, S. 161 ff.; Kühling, Datenschutz in einer künftigen Welt allgegenwärtiger Datenverarbeitungen – Aufgabe des Rechts?, Die Verwaltung 40 (2007), 153, 162 ff.

131 Siehe z.B. John/Acquisti/Loewenstein (Fn. 128), 37 J. of Consumer Research. 858, 868 (2011); vgl. auch Tene/Polonetsky, To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising,

Soweit Big Data-Anwendungen allein auf einer statistischen Auswertung eines großen Datenvolumens beruhen, lassen sich datenschutzrechtliche Bedenken auch aus deutscher und europäischer Sicht durch eine konsequente Anonymisierung zerstreuen.[132] Bei der Frage, ob eine Wiederherstellung des Personenbezugs mit vertretbarem Aufwand möglich bleibt, wäre an eine ökonomische Analyse zu denken.

Bei der unterschiedlichen Einstellung zum Vorsorgedenken könnte eventuell eine modifizierte Kosten-Nutzen-Abwägung[133] eine Brücke schlagen. Einerseits schärft dieser analytische Ansatz das Bewusstsein für die Transaktionskosten eines im Ausgangspunkt sehr weit zugeschnittenen Datenschutzes, der wohl gerade deshalb von den meisten Internet-Nutzern als zu umständlich vernachlässigt wird. Andererseits zeigt gerade die jüngere Kosten-Nutzen-Diskussion zum Klimawandel in der US-amerikanischen Literatur,[134] dass dieser ökonomische Ansatz bei den Kosten durchaus auch die langfristigen Gefahren der Kumulation vieler scheinbar kleiner Ursachenbeiträge abzubilden und in das Bewusstsein zu rücken vermag. Es läge nahe, dies etwa auf die Risiken zu übertragen, die aus der Ermöglichung der Erstellung von Persönlichkeitsprofilen aus dem Internet-Nutzungsverhalten resultieren. Ergänzend sollte der Blickwinkel bei der Messung des Nutzens von der neoklassisch verstandenen ökonomischen Effizienz (in Form aggregierter individueller Präferenzen für ein bestimmtes Datenschutzniveau) stärker auf die Optimierung der individuellen Persönlichkeits-Verwirklichungschancen im Internet verschoben werden. In diesem – allerdings bislang wohl weder in Deutschland noch in den USA mehrheitsfähigen – *Capability Approach*[135] ließe sich das doppelte Anliegen in der digitalen Welt, nämlich sowohl ein selbstgewähltes

---

13 Minnesota J. of Law, Science and Technology, 281, 333 (2012); eingehend nun Hermstrüwer, Informationelle Selbstgefährdung, 2016.

132 Siehe nur Ohrtmann/Schwiering (Fn. 121), NJW 2014, 2984, 2988.

133 Dazu allgemein Fehling, Ökonomische Analyse im Öffentlichen Recht als Methode zur Reformulierung und Operationalisierung von Gerechtigkeitsfragen, in: Die Fakultät der Bucerius Law School (Hrsg.), Begegnungen im Recht, 2011, S. 39.

134 Vgl. Posner, Catastrophe: Risk and Response, 2004, insb. S. 43 ff. u. 155 ff.

135 Entwickelt vom Ökonomie-Nobelpreisträger Amartya Sen, z.B.: Ökonomie für den Menschen, 4. Aufl. 2007, S. 94 ff.; ders., Die Idee der Gerechtigkeit, 2010, S. 258 ff.; ders., Commodities and Capabilities, 1985; zur Abgrenzung von und Kritik an herkömmlichen Kosten-Nutzen-Analysen ders., The Discipline of Cost-Benefit Analysis, 29 J. of Legal Studies 931 ff. (2000).

Niveau von Privatheitsschutz als auch selbstbestimmtes Teilen von Information mit anderen, besonders gut abbilden.[136] Selbstverständlich lässt sich mit einem solchermaßen modifizierten Kosten-Nutzen-Ansatz kein optimales Niveau des Datenschutzes ausrechnen. Aber dieses analytische Raster kann helfen, die Grundfragen und auch Lösungsoptionen klarer zu identifizieren.

Allerdings deutet wiederum die Verhaltensökonomik auf Grenzen der transatlantischen Verständigung über Datenschutz und Informationsfluss im Internet hin. Abwägungen und Prioritätensetzungen sind danach nämlich nur begrenzt rational möglich angesichts der unterschiedlichen Verfügbarkeit von Erfahrungen (*information bias*) und darauf basierender Entscheidungsheuristiken.[137] Die NS- und DDR-Vergangenheit einerseits[138] und die Erfahrung des 11. Septembers andererseits bleiben für unterschiedliche Gewichtungen von Freiheit und Sicherheit im Internet wirkmächtig. Im Verhältnis zwischen Privaten sind es sozialstaatliche bzw. marktliberale Traditionen, die auch die digitale Welt prägen. Besonders die letztgenannte Kluft dürfte schwer überwindbar sein.

## *V. Fazit*

Zieht man Bilanz, so zeigt sich: Die konzeptionellen Unterschiede beim Umgang mit Informationen und Daten in der digitalen Welt zwischen Deutschland bzw. Europa und den USA lassen sich mittels griffiger Schlagwörter und Gegenüberstellungen kennzeichnen. In dieser Diktion steht einer würdebasierten umfassenden Schutzkonzeption, die dem Einzelnen im Verhältnis zum Staat wie auch unter Privaten eine selbstbestimmte Teilhabe am Kommunikationsprozess sichern soll, ein bloßer punktueller abwehrrechtlicher Schutz allein gegen den Staat gegenüber, wobei der Akzent im Übrigen weit stärker auf der wohlfahrtssteigernden Wirkung des freien Informationsflusses liegt. Bei genauerer Analyse fin-

136 Dazu näher Fehling, in: Eger/Oeter/Voigt (Fn. 2), S. 99, 102 f.; Andeutungen in diese Richtung finden sich auch bei Cohen (Fn. 76), 126 Harv. L. Rev. 1904, 1911 mit dortiger Fn. 20 (2013).

137 Eindrucksvoll geschildert von Kahneman, Schnelles Denken, langsames Denken, 2011, insb. S. 139 ff.

138 Als Grundlage des Datenschutzes besonders hervorgehoben etwa von Masing (Fn. 28), NJW 2012, 2305.

den sich allerdings durchaus gewisse Annäherungen und Überschneidungen. Pragmatische Verständigungen, die vor allem am Einwilligungserfordernis und an Risikoanalysen auf Kosten-Nutzen-Basis ansetzen könnten, erschienen auch im Zuge der jüngeren Entwicklungen nicht ausgeschlossen. Dennoch bleiben im Ausgangspunkt gravierende rechtskulturelle Unterschiede sichtbar. Zusammen mit den politischen und ökonomischen Machtverhältnissen bleiben diese Unterschiede für die Verantwortungsstrukturen in der digitalen Welt prägend.

Vor diesem Hintergrund liegt zumindest ein steiniger transatlantischer Verhandlungsweg vor uns auf der Suche nach der »einen (westlichen) Welt« im Internet. Immerhin wäre es bereits ein Gewinn, die Unterschiede klar zu benennen. Die schlechteste Lösung – und diese erscheint leider keineswegs unrealistisch – wäre ein auf dem Papier äußerst ambitioniertes europäisches Datenschutzrecht, das aber im transatlantischen Geschäftsverkehr – von der Geheimdienstzusammenarbeit ganz zu schweigen – nicht ernst genommen und »heimlich, still und leise« bis zur Unkenntlichkeit verwässert wird.